الجمهورية الجزائرية الديمقراطية الشعبية

RépubliqueAlgérienneDémocratique et populair

Ministère de l'Enseignement Supérieur et
de la Recherche Scientifique.
Université de Ghardaïa

Faculté de Droit et des Sciences Politiques
Département de Droit

وزارة التعليم العالي و البحث العلمي
جامعة غرداية
كلية الحقوق والعلوم السياسية
قسم الحقوق

شهادة تصحيح

يشهد الأستاذ د/ أولاد النوي مراد ..... بصفته(ها) رئيس لجنة مناقشة

مذكرة ماستر ل:

الطالب(ة): طسرا د أيمان ..... رقم التسجيل: 190890729874

الطالب(ة): حليفي الزهرة ..... رقم التسجيل: 191939082895

تخصص :ماستر قانون جنائي وعلوم جنائية ..... دفعة : 2024 لنظام (ل م د).

للمذكرة المعنونة بـ: السرقة الرقمية .....

.....

.....

قد تم تصحيحها من طرف الطالب / الطالبين وهي صالحة للإيداع.

غرداية في: 7 جويلية 2024

إمضاء الأستاذ رئيس اللجنة المكلف بمتابعة التصحيح

د/ أولاد النوي مراد

رئيس القسم

ملاحظة: تترك هذه الشهادة لدى القسم .

جامعة غرداية

كلية الحقوق والعلوم السياسية

قسم الحقوق

السرقة الرقمية

مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي حقوق تخصص قانون جنائي والعلوم الجنائية.

اعداد الطالبتين:

- طراد أسماء
- خليفي زهرة

إشراف أستاذ:

- ماشوش مراد

لجنة المناقشة:

لقب واسم الاستاذ	الرتبة	الجامعة	الصفة
أولاد النوي مراد	**أستاذ محاضر "أ"**	**جامعة غرداية**	**رئيسا**
ماشوش مراد	**أستاذ مساعد "ب"**	**جامعة غرداية**	**مشرفا مقررا**
زروقي أسيا	**أستاذ محاضر "أ"**	**جامعة غرداية**	**عضوا مناقشا**

نوقشت بتاريخ: 06/11 /2024

السنة الجامعية:

1445-2020هـ/ 2024-2025

الشكر والإهداء

شــكر وعـــرفان

الحمد لله الذي ساعدني على انجاز هذه المذكرة وانار لي دربي ووفقني في مسيرتي العلمية.

أتقدم بخالص الشكر والتقدير والاحترام:

الى الأستاذ الدكتور ماشوش مراد الذي لم يبخل على بكل ما لديه من معلومات ومراجع، وعلى كل ما قدمه لنا من نصائح.

الى كل اساتذتي الافاضل، الذين كان لهم الفضل في سلوكي هذا الدرب أساتذة كلية الحقوق والعلوم الإنسانية بجامعة غرداية.

الى أعضاء لجنة المناقشة الموقرة الأستاذ أولاد النوي مراد رئيسا ، الأستاذة زروقي أسيا و الأستاذ ماشوش مراد مشرفا ومقررا .

كما لا ننسى في الأخير ان نتقدم بشكر الجزيل لكل من ساعدنا بمعلومة ، نصيحة ، توجيه ، او بكلمة طيبة في أي مكان .

إهـــــــــــداء

بسم الله الرحمان الرحيم

وقضى رَبُّكَ أَلا تَعْبُدُوا إِلَّا إِيَّاهُ وَبِالْوَالِدَيْنِ إِحْسَانًا الإسراء :23

أهدي ثمرة جهدي:

إلى امي التي أعطتني رحيق حياتي وكياني، إلى التي سفتني حيا وأحاطتني حنانا عطفا وأعطتني زاد التقوى فكانت مصباح دربي إلى التي غمرني دعاتها في الليل والنهار فكانت عونا لي في مسيرة حياتي.

إلى من علمني الصعود وحذرني من التوقف في أول الصعاب. إلى من أنار بصيرتي بنور العلم وجعله مفتاحا وطريقا بالإيمان.

ابي – رحمه الله واسكنه فسيح جناته الله –

إلى أخواتي و نور عيني: امنية و نورة و رميسة .

والى كل من يعرفني من بعيد أو قريب.

طراد اسماء

إهـــــــــــداء

بسم الله الرحمان الرحيم

وقضى رَبُّكَ أَلا تَعْبُدُوا إِلَّا إِيَّاهُ وَبِالْوَالِدَيْنِ إِحْسَانًا الإسراء :23

أهدي ثمرة جهدي:

إلى امي التي أعطتني رحيق حياتي وكياني، إلى التي سفتني حيا وأحاطتني حنانا عطفا وأعطتني زاد التقوى فكانت مصباح دربي إلى التي غمرني دعاتها في الليل والنهار فكانت عونا لي في مسيرة حياتي.

إلى من علمني السعود وحذرني من التوقف في أول الصعاب. إلى من أنار بصيرتي بنور العلم وجعله مفتاحا وطريقا بالإيمان.

ابي – رحمه الله –

إلى جميع إخوتي وأخواتي وأقاربي وإلى كل اساتذتي ومن أشرفوا عليا طيلة مشواري والى كل من يعرفني من بعيد أو قريب.

خليفي زهرة

مقدمة

مقدمـــة

من المعروف أن جريمة السرقة تعد من أقدم الجرائم التي عرفها الإنسان، وأنها تطورت مع تطور أساليبه ومعارفه في الحياة. فجريمة السرقة و إن كانت معروفة في العصور القديمة ، خاصة عند الرومان، إلا أنها لم تختلف عن جرائم الاعتداء على المال، سواء شكلت هذه الجرائم فعلا من أفعال الاحتيال أو خيانة الأمانة، والاستعمال غير المشروع لأموال الغير ، إلا أن الأمر لم يعد كذلك بعد ظهور الإسلام وظهور المذاهب الفقهية الإسلامية التي تناولته بدراسة وتحليل، مما أدى إلى تمييزها من حيث عنصرها المادي عن جريمة الاختلاس ، ومن ناحية أخرى، فقد بقيت جريمة السرقة لفترة طويلة في أوروبا لا تختلف عن جرائم اغتيال الأموال، إلا بعد صدور قانون العقوبات الفرنسي عام 1811، حيث أصبحت تعرف على انها : "**اختلاس شيء مملوك للغير**".

وهكذا ضلت جريمة السرقة في تباين مستمر وصولا الى وقتنا الراهن أين يعيش العالم اليوم تطوراً علمياً وتقنياً كبيرا في مختلف جوانب الحياة، ومن اهم هذه المستجدات التطور التكنولوجي في مجال الاعلام والاتصال او ما يعرف بالشبكة المعلوماتية، بحيث تتسارع الوتيرة التكنولوجية والتقنية الهائلة بشكل غير معالمه، وبالإضافة الى ظهور الفضاء الالكتروني ووسائل الاتصال الحديثة كالفاكس والإنترنت، وكل هذا بفضل الاختراعات الهائلة على المستوى التقني.

كما يوصف العصر الذي نعيش فيه بأنه عصر تكنولوجيا المعلومات والاتصالات، وظهور الاستخدام الواسع النطاق لأجهزة الكمبيوتر وتطور شبكات المعلومات، فنجد العلماء والصالحين يحاولون الاستفادة منها وفي المقابل نجد أن المجرمين يحاولون أيضًا الاستفادة من التقدم التكنولوجي من أجل استغلال مرتكبي الجرائم الإلكترونية في تنفيذ جرائمهم التي لم تعد تقتصر على اقليم الدولة واحدة، بل باتت جرائم عابرة لحدود الدول وهي بذلك تمثل ضرب من ضروب الذكاء الاجرامي.

وعلى الرغم من المزايا العديدة الناجمة عن التطور المعلوماتي الهائل، إلا أنه ترتب على اثره مخاطر عدة ناجمة عن سوء استخدام شبكة المعلومات الدولية لصالح المجرمين للقيام بأنشطتهم الإجرامية، كما ساهم في ظهور فئة جديدة من المجرمين و الجرائم المستحدثة، بما في ذلك جريمة السرقة الرقمية وهي الصورة التقنية لجريمة السرقة التقليدية التي عرفتها للمجتمعات عبر العصور كما سبق بيانها أعلاه ، وعليه فإن جريمة السرقة الرقمية ترتبط ارتباطاً وثيقاً بمدى اعتماد المجتمع ومؤسساته المختلفة على الأنظمة المعلوماتية في جميع قطاعاته، ولهذا زادت فرصة ارتكاب جرائم المعلوماتية و لقد أبدعوا في ارتكاب ممارسات غير مشروعة مثل هذه الجريمة، من خلال تطوير أساليب مبتكرة لتنفيذ جرائمهم في هذا المجال مستغلين قدراتهم ومعارفهم من أجل تنفيذ أنشطتهم الإجرامية.

وعليه كلما زاد استخدام الإنترنت في الحياة الشخصية أو المهنية ازدادت مخارطها ونتيجة لارتفاع الخطورة الإجرامية لجريمة للسرقة الرقمية، وضعت تحديات صعبة على عاتق المشرع، من اجل التدخل لمعالجتها ووضع أسس قانونية متكاملة لمواجهتها قبل أن تصبح عائقاً في طريق تقدم المجتمع وتطوره.

تعتبر جريمة السرقة الرقمية من المواضيع المهمة والجديدة التي لا تزال محل دراسة وتدقيق على المستوى الفقهي والقانوني، وباعتبار أن هذه الجريمة من الجرائم المعلوماتية الحديثة التي تفرض نفسها على الصعيدين الدولي والوطني فإن أهمية البحث في هذا الموضوع تتجلى فيما يلي:

– محاولة سد الفجوة الناتجة عن قلة الأبحاث ودراسات المتخصصة حول موضوع البحث نظرا لحداثته وجعله بداية لدراسات اخرى.

– البحث في الأثار السلبية الخطيرة لهذه الجريمة حيث تكمن خطورتها كونها ظاهرة عالمية تهدد الأفراد والدول وتهدد الأنشطة الفردية والدولية وذلك من اجل التوصل الى طرق للوقاية منها ومكافحتها.

– تتيح لنا هذه الدراسة تسليط الضوء على هذا النوع من الجرائم والتعرف على أهم صور الاعتداءات الواقعة على الأموال والمعلومات الرقمية.

– معرفة مدى إمكانية التوافق بين القواعد التقليدية المتعلقة بجرائم الأموال التي تناولها المشرع الجزائري في قانون العقوبات والقواعد المتعلقة بجرائم الأموال في شكلها الرقمي وكذا التعرف على الطبيعة القانونية لمحل السرقة الرقمية.

إن اختيار موضوع جريمة السرقة الرقمية جاء لعدة أسباب منها ذاتية واخرى موضوعية، نفصلها كالاتي:

– الرغبة الشخصية في الكتابة عن موضوع حديث ومعاصر يشهده الواقع المعاش.

– الميل الى دراسة الجرائم المعلوماتية بعناية والاطلاع واكتساب المعرفة اللازمة في هذا المجال وحب الاستزادة من العلوم القانونية بشأنها.

– التطور المستمر لأساليب ارتكاب جريمة السرقة الرقمية إضافة الى التطور التكنولوجي الحاصل في مجال تكنولوجيا المعلومات هذه الخصائص تجذب اهتمام الباحثين للدراسة والبحث في هذه الجريمة

– إن حيوية الموضوع الدراسة وامتداد تأثيره على مختلف الاصعدة، وارتباطه بالتطور التكنولوجي الذي أصبحنا نعتمد عليه في حياتنا اليومية، بالإضافة إلى الإشكالات القانونية التي يثيرها، تجبرنا على التركيز عليه والتعرف على جميع جوانبه.

– الانتشار الواسع للجرائم الاعتداء على الاموال عبر الوسائط الإلكترونية ونتيجة الصبغة التقنية التي تكتسيها هذه الجريمة حيث صعبت على رجال القانون مهمة قمعها وبذلك نحاول معرفه ما توصل اليه تشريع الجزائري في مواجهه جريمة السرقة الرقمية.

تهدف هذه الدراسة في الأساس الى:

– دراسة هذه الجريمة بما يواكب تلك الطفرة الهائلة الحاصلة في مجال الجرائم المعلوماتية، والتي يعتمد فيها المجرم اساسا على الوسائط الإلكترونية المختلفة لارتكاب جريمة السرقة الرقمية.

– ازالة الغموض الذي يكتنف جوانب جريمة السرقة الرقمية وملامسه اهم الاشكالات التي تطرحها.

– استعراض الانماط والسلوكيات التي أتت بها جريمة السرقة الرقمية ومطابقتها مع الانماط وسلوكيات جريمة السرقة التقليدية.

– بيان موقف الفقه ونظم القانونية المقارنة من جريمة السرقة الرقمية بالأخص موقف النظام القانوني الجزائري وكيف نظمها في ظل قوانين الخاصة.

– إبراز خصوصية هذه الجريمة من حيث خصوصية إثباتها، واساليب البحث والتحري، والهياكل الخاصة المكلفة بالمنع والوقاية هذا النوع من الجرائم.

من خلال هذه الدراسة واثناء جمعنا للمادة العلمية التي بنينا عليها هيكلة بحثنا هذا فإننا لم نتعرض الى دراسة سابقة تحمل نفس عنوان موضوعنا " السرقة الرقمية " غير أننا اعتمدنا على دراسات وأن كانت تحمل عناوين مختلفة عنه إلا أنها ذات صلة مباشرة بالموضوع ولو بشكل جزئي، نذكر منها:

– **الدراسة الاولى:** كتاب بعنوان السرقة الإلكترونية وحكمها في الاسلام، لمؤلفه أحمد عبد الرؤوف المينيفي الطبعة الثانية، دار النشر E-kutubltd لندن سنة 2017.

ولعل اهم نقاط الالتقاء بين هذا المؤلف ودراستنا هو الإطار الموضوعي لجريمة السرقة الرقمية بينما يزيد عنها في تحليل احكامها الفقهية الاسلامية.

– **الدراسة الثانية:** بعنوان جريمة السرقة الالكترونية، مقالة بمجلة جامعة بابل العلوم الانسانية، المجلد 27، العدد 5، سنة 2019، تناولت هذه المقالة جريمة السرقة الرقمية ولكن بمصطلح مغاير وهو السرقة الالكترونية من خلال التطرق الى جانبها الموضوعي والقانوني.

– **الدراسة الثالثة:** بعنوان السرقة الالكترونية تكييفها الشرعي وطرق إثباتها، مقالة نشرت في مجلة الاحياء، جامعة حسيبة بن بو علي، شلف، مجلد 19 ال عدد22 سنة.

ما يميز هذه الدراسة هو تطرقها للتكييف الشرعي لجريمة السرقة الالكترونية او الرقمية على خلاف باقي الدراسات التي اهتمت فقط بتكييفها القانوني، زيادة الى تناولها أحد اهم جوانبها الإجرائية هو كيفية الاثبات الجنائي فيها.

-**الدراسة الرابعة:** بعنوان الجرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق والعلوم السياسية، جامعة ابو بكر بالقايد تلمسان ،2010 -2011.
اشارت هذه الدراسة الى جريمة السرقة الرقمية بشكل غير مباشر او كجزيئة، وذلك باعتبارها صورة من صور الجرائم المعلوماتية ذات الأهمية البالغة من حيث خطورتها الإجرامية.

مما لا شك فيه أن الدراسات مهما كان نوعها أو مجالها لا تخلو من الصعوبات، ولعل أهم عائق واجهنا خلال بحثنا هذا المتعلق بجريمة السرقة الرقمية هو نقص المراجع المتخصصة في الموضوع، ويرجع ذلك اساسا كونه موضوعاً حديثا لم ينل حظه من البحث والتحليل على مستوى الفقه الجزائي والتطبيق القضائي ، وبخلاف ذلك تتوافر المراجع العامة المتعلقة بالجرائم المعلوماتية لكنها تقتصر فقط على الإشارة إلى جريمة السرقة الرقمية دون تفصيل ، إضافة إلى غموض الذي يحيط بهذه الجريمة في ظل غياب التشريعات التي تحدد إطارها القانوني وعدم تبني المشرع الجزائري لموقف صريح اتجاهها.

على ضوء أهمية موضوع البحث وتأسيسا لما سبق ذكره في هذه الدراسة المتخصصة ارتأينا طرح الإشكالية التالية: **كيف نظم المشرع الجزائري جريمة السرقة الرقمية بإعتبارها جريمة ذات خصوصية فقهية وإجرائية لتحقيق المواجهة القانونية الجنائية المنشودة لها؟**

وتندرج تحت هذه الاشكالية الرئيسية، جملة من التساؤلات الفرعية، والتي نعرضها على النحو التالي:

- فيما تتمثل الاحكام العامة لجريمه السرقة الرقمية؟
- ما هي الاحكام الخاصة لجريمة السرقة الرقمية؟
- ما موقف الأنظمة القانونية المتباينة والنظام الجزائري خاصة من جريمة السرقة الرقمية؟
- ما وجه الخصوصية الاجرائية في جريمة سرقه الرقمية؟

من خلال دراستنا لهذا النوع من الجرائم ونظراً لطبيعة الموضوع، ارتأينا معالجة الإشكالية المطروحة وفق المنهج الوصفي التحليلي اي الوصف الذي يتخلله بعض التحليل فحاولنا بموجب:

-**المنهج الوصفي:** وصف جريمة السرقة الرقمية بتسليط الضوء على اهم التعريفات الفقهية والقانونية لها وابراز خصائصها والوقوف على اركانها العامة والخاصة، ايضا وصف الصور الناتجة عنها وطرق ومراحل ارتكابها.

- **المنهج التحليلي:** وباعتباره المنهج الأنسب لمعالجة الدراسات القانونية، اعتمدنا في هذه الدراسة على أدوات هذا المنهج في تحليل النصوص القانونية المتعلقة بجريمة السرقة الرقمية، وتحديد العقوبات المقررة لها، بالإضافة إلى الكشف عن الجانب الإجرائي والتنظيمي والمتعلق بهذه الجريمة.

وللإجابة على الإشكالية المطروحة تناولنا الموضوع وفق خطة ثنائيه مكونة من فصلين رئيسيين خصص الفصل الاول منها لدراسة الإطار الموضوعي لجريمة السرقة الرقمية من خلال التطرق للأحكام العامة لجريمة السرقة الرقمية في المبحث الأول والمتضمن مطلبين الأول بعنوان أساسيات حول جريمة السرقة الرقمية ،اما الثاني فتحدثنا فيه عن خصائص هذه الجريمة، وجاء المبحث الثاني متعلقا بالأحكام الخاصة لجريمة السرقة الرقمية مبينين فيه تطبيقات هذه الجريمة في المطلب الاول و تقنياتها في المطلب الثاني، بينما بحثنا في الفصل الثاني عن التنظيم القانوني لجريمة السرقة الرقمية الذي جاء بدوره مقسما الى مبحثين ، بداية بالتكييف القانوني لجريمة السرقة الرقمية في المبحث الاول من خلال ابراز أركان الجريمة في المطلب الاول ، و استعراض موقف الانظمة القانونية في المطلب الثاني وصولا أخيرا في المبحث الثاني بعنوان المواجهة القانونية لجريمة السرقة الرقمية في المبحث الثاني، المتفرع الى المطلب الاول الخاص بالإثبات في جريمة السرقة الرقمية اما بالنسبة للثاني فقد كان بعنوان مكافحة جريمة السرقة الرقمية .

الفصل الأول:

الإطار الموضوعي لجريمة السرقة الرقمية.

تمهـــيـد

تعتبر الجريمة السرقة الرقمية من اهم جرائم الاموال واكثرها انتشارا، كما وأنها من أقدم الجرائم التي عرفتها البشرية فاستهجنتها كل تشريعات على مر الأزمان، وبظهور التكنولوجيا الحديثة التي لا ننكر فضلها في المساهمة بالنهوض قدما وتطوير مجتمعاتنا لكن في المقابل نجد ان لها انعكاسات سلبية سببها سوء استخدام تقنياتها والتي اثرت بصوره مباشره على هذه الجريمة فتعدى مفهومها التقليدي الى انها اصبحت جريمة سرقة رقمية ترتكب في الفضاءات الافتراضية محلها الأموال والبيانات الإلكترونية.

وبالتالي نجد أنفسنا امام مسؤولية جديدة تملي علينا تمحيص وتفكيك أجزاء هذه الجريمة المستحدثة بمعرفه سبل مواجهتها والحد منها وهذا ما سنتعرض له بالدراسة في هذا الفصل وذلك بالتطرق الى الجانب الموضوعي لجريمة السرقة الرقمية من خلال المبحثين الاول يتضمن الاحكام العامة لجريمه السرقة الرقمية اما الثاني يختص بأحكامها الخاصة.

المبحث الاول الاحكام العامة لجريمه السرقة الرقمية

تعتبر جريمة السرقة الرقمية او الاعتداء على الأموال والبيانات عبر الوسائط الرقمية أحد أنواع الجرائم الإلكترونية التي تقع على الأصول المالية للأشخاص وتتميز بمجموعة من الخصائص والمميزات التي تفرقها عن جريمة السرقة التقليدية ولذلك سوف نحاول من خلال هذا المبحث التطرق الى مضمون هذه الجريمة من تعاريف واهم خصائصها وكذا تميزها عن السرقة التقليدية.

المطلب الأول: أساسيات حول جريمة السرقة الرقمية.

سنتناول في هذا المطلب مضمون جريمة السرقة الرقمية وذلك في الفرع الأول، حيث نشير فيه الى أهم تعريفات هذه الجريمة وطبيعتها القانونية، بينما نتطرق الى أبرز خصائصها في الفرع الثاني.

الفرع الأول: مضمون جريمة السرقة الرقمية.

ان بيان مفهوم شيء يتطلب بيان تعريفه لغة وكذا اصطلاحا وكما نعلم ان الجريمة السرقة الرقمية من حيث التكوين تنقسم الى مفردين هما السرقة والرقمية وعلى ذلك كان لابد من الإحاطة بالمعنى العام لكل منهما.

أولا: المقصود بالمصطلح السرقة.

1-تعريف السرقة لغة:

السرقة بفتح السين وكسر الراء من سرق يسرق من اخذ شيئا من الغير على وجه الخفيه والسارق هو من جاء مستترا الى حرز فاخذ مال غيره[1]، ايضا استرق السمع مستخفيا ويقال لمن يسارق النظر اليه إذا اهتبل غفلته لينظر اليه.[2]

2-تعريف سرقه اصطلاحا:

اختلفت المذاهب الفقهية في تعريفها تبع الاختلاف شروط هذه الجريمة وآرائهم

1.2-تعريف الحنفية: القول بان السرقة من اخذ العاقل البالغ نصابا محررا او ما قيمته نصاب ملكا للغير لا شبهة فيه على وجه الخفية. [3]

2.2-تعريف المالكية: هي اخذ المال للغير مستترا من غير ان يؤتمن عليه. 3.2-

3.2-تعريف الشافعية: السرقة هي اخذ المال خفيه ظلما من حرز مثله بشروط[4]

---

[1] محمد الطيب عمور، **السرقة الإلكترونية تكييفها الشرعي وطرق أثبتها**، مجلة الاحياء، جامعة حسيبة بن بوعلي شلف، المجلد 19 العدد 22، ص 405.

[2] جمال الدين بن فضل الافغاني، محمد بن كرم بن منظور الانصاري، **لسان العرب، ط** 3، **دار** صادر، بيروت ،1996، ص 155.

[3] محمد الطيب عمور، مرجع سابق، ص 460.

[4] ابراهيم رمضان ابراهيم، **الجريمة الإلكترونية وسبل موجهتها في الشريعة الإسلامية والأنظمة الدولة**، مجله كليه الشريعة والقانون، بطنطا، المجلد 30، العدد 2، ص 387.

4.2-تعريف حنابلة: أخذ مال خفيه محترما لغيره واخراجه من حرز لا شبهة فيه على وجه الاختفاء[1]

انطلاق من هذه التعريفات الفقهية المختلفة يمكن التوصل الى تعريف لمفرد السرقة على انها كل فعل يقوم به الشخص بغية اخذ او امتلاك مال غير مملوك له خفية عن صاحبه دون وجه حق.

3-تعريف السرقة قانونا:

ان المشرع الجزائري لم يضع تعريفا محددا لجريمة السرقة، انما اكتفى بالوصف القانوني للفعل الذي يأتيه الجاني حتى يعتبر قد ارتكب جريمة السرقة، وذلك في نص المادة **350** ق ع ج حيث جاء فيها "**كل من اختلس شيئا غير مملوكا له يعد سارقا**" [2]على هذا الاساس فأن القانون الجزائري صنف جريمة السرقة في ظل قانون العقوبات على انها جنحة.

ثانيا-المقصود بمصطلح الرقمية

1-تعريف الرقمية لغة:

اسم منسوب على رقم ونقول الشبكة الرقمية بمعنى شبكه الاتصالات الرقمية العالمية المتطورة او لغة رقمية وهي لغة تعد خصيصا طبقا لقواعد معينة تستخدم في حسابات الإلكترونية كوسيلة للعمل بها. [3]

2-تعريف الرقمية اصطلاحا:

لقد عرفت على انها كل نتيجة مبدئية او نهائية مترتبة[4] عن تشغيل البيانات وتحليلها واستقراء دلالاتها واستنتاج، ما يمكن استنتاجه منها وحدها او متداخله مع غيرها او تفسيرها على نحو يثري معرفة متخذي القرار ومساعدتهم على حكم الصواب. [5]

تعرف ايضا على انها معالجة عقلية للمعلومات باستخدام آلات تعمل ذاتيا حيث ان هذا التعريف هو راجح لدى الفقه لتضمنه جميع المعلومات التي يتم تجميعها بمعرفة الانسان والتي تتمتع بتجديد والابتكار والسرية.[6]

3-تعريف السرقة الرقمية:

---

[1] دحمان صبيحه خديجة، **جرائم السرقة والاغتيال عبر الانترنت دراسة مقارنه بين الفقه الاسلامي والقانون الجزائري**، مذكره لنيل شهادة الماجيستير، كلية العلوم الإسلامية، قسم العلوم الإسلامية وقانون، جامعة الجزائر يوسف بن خدة، 2013-2014، ص 8.

[2] الامر رقم 66-156مؤرخ في 8 يونيو 1966، المتضمن قانون العقوبات، الصادر في الجريدة الرسمية رقم 49، مؤرخة في 11-06-1966، ص 255.

[3] معاني المعاجم، المقال منشور على الموقع: https://www.almaany.com تم نظر اليها يوم 22 ماي 2023 على الساعة 20:23 مساءا

[4] احمد خليفة ملط، **جرائم المعلوماتية**، طبعه 2، دار الفكر الجامعي، الإسكندرية،2006، ص 81.

[5] سوير سفيان، **الجرائم المعلوماتية**، مذكره لنيل شهادة الماجستير في العلوم الجنائية وعلم الاجرام، كلية الحقوق والعلوم السياسية جامعه ابو بكر بالقايد، تلمسان، 2010-2011، ص 11.

[6] احمد عبد الرؤوف المنيفي، **السرقة الإلكترونية وحكمها في الاسلام**، الطبعة الثانية، E-kutultd،لندن ،2017 ،ص 40.

هي نوع من أنواع الجرائم المعلوماتية التي ترتكب بواسطة الكمبيوتر تقع على النظام المعلوماتي وتقع السرقة الرقمية على المعلومات والبرامج التي لها قيمة مالية والتي تتجسد في شكل أصول مالية داخل هذا النظام وهي تنطوي بوجه عام ذات الصفات والخصائص التي تتمتع بها الجرائم المعلوماتية. [1]

وتعرف بانها: "عباره عن افعال غير مشروعه يكون الحاسب الالي محلا لها او وسيلة لارتكابها."[2]كما تعرف بوجه عام على انها "اخذ المعلومات والبرامج المخزنة في الحاسوب الالي او المنقول عبر وسائل الاتصال، باستخدام الادوات التقنية المعلومات". [3]

ومن خلال مما سبق من تعريفات لجريمة السرقة الرقمية نستخلص بانها: انعكاس سلبي للتطور التكنولوجي الحديث الذي نشهده، وهي تعد سطو واختلاس على البرامج المخزنة في الكمبيوتر اي كان نوعها سواء مالا بنكي او بيانات شخصية فالفعل غير المشروع الذي يقوم به الجاني والمتمثل في السرقة من مكان بعيد عن مكان الجريمة يكون صعب الاثبات عكس السرقة التقليدية التي تلزم الجاني بالتواجد في مسرح الجريمة.

رابعا –الطبيعة القانونية لجريمة السرقة الرقمية.

انقسمت الآراء الفقهية الى تيارين فهناك من رأى بان جريمة السرقة الرقمية ذات طابع خاص بينما هناك من يدعو الى انها ذات وصف عام.

1–جريمة ذات الطبيعة خاصة:

يرى الفقه التقليدي ان مجال الحماية القانونية في جريمة السرقة الرقمية، هو المعلومات في حد ذاتها وانطلاقا من فكرة ان اخفاء وصف القيمة يكون على الاشياء المادية القابلة للاستحواذ، وبالنظر الى الطبيعة الخاصة التي تتميز بها المعلومات كونها ذات طبيعة معنوية فانه من غير المعقول ان تكون قابلة للإستئثار، وعلى ذلك فان المعلومات المخزنة لا تعتبر مالا كالمواد الأدبية او الفنية او الصناعية وذلك كونها لا تندرج ضمن مجموعة القيم المحمية.

لكن استبعاد المعلومات من مجموعة القيم المالية لم يمنع الفقه والقضاء من الاعتراف بوجود اعتداء يتطلب الحماية القانونية في حالة الإستيلاء غير مشروع عليها.[4]

2– جريمة ذات وصف عام.

يرى الفقه الحديث ان المعلومات ما هي الا مجموعة مستحدثه من القيم القابلة للاستحواذ مستقله عن دعمتها المادية وذلك ان المعلومات لها قيمة اقتصادية قابلة لأنها تحاز حيازة غير مشروعة

---

[1] انسام سمير طاهر، **جريمة السرقة الإلكترونية**، مجلة جامعة بابل للعلوم الانسانية، مجلد 27، العدد 5، 2019، ص 134.
[2] احمد محمد عبد الرؤوف المنيفي، مرجع سابق، ص 40.
[3] احمد خليفه ملط، مرجع سابق، ص 104.
[4] سلامه محمد عبد الله، **موسوعة جرائم المعلوماتية جرائم الكمبيوتر والانترنت**، ط 2، منشأة المعارف، الإسكندرية، 2006، ص 44-43.

انها ترتبط كما يقولان vivant and catala بمؤلفهما عن طريق علاقة التبني التي تقوم بينهما كالعلاقة القانونية التي تتمثل في علاقة المالك بالشيء الذي يملكه بمعنى ان المعلومات مال قابل للتملك والاستغلال، على اساس قيمته الاقتصادية وليس على اساس كيانه المادي لذلك فهو يستحق الحماية القانونية ومعاملته معاملة المال. [1]

خامسا-التمييز بين جريمة السرقة الرقمية وسرقه التقليدية.

1-اوجه الاتفاق بين السرقة الرقمية والسرقة التقليدية:

1.1-من حيث أطراف الجريمة: مجرم يقوم بالاعتداء ومجنى عليه يكون الضحية سواء كان شخصيه طبيعية او شخصيه اعتباريه.

2.1-من حيث اركان الجريمة: الركن المادي والمعنوي شرطان أساسيان لقيام جريمة التقليدية والرقمية شأنهما شأن الجرائم الأخرى.

3.1-من حيث شروط السرقة: بناء على القياس الذي عقده الباحثون من بين السرقة العادية والرقمية فان موضوع السرقة هو المال المنقول والمقوم البالغ النصاب المأخوذ من حرز شريطه ان يخرج السارق الشيء.

4.1-من حيث عناصر الجريمة: توفر ثلاثة عناصر (النشاط الاجرامي، النتيجة، العلاقة السببية) في الجرائم كافة وبالنسبة الى جميع المساهمين فيها. [2]

2-اوجه الاختلاف بين السرقة الرقمية والسرقة التقليدية.

لعل الاختلاف الناجم عن مفهوم السرقة التقليدية، فمفهوم السرقة يضمن نقل من حيازة الى حيازة، اي نزع المال من حيازة صاحبه وادخاله في حيازة السارق ومن يقوم بسرقة المعلومات والبيانات وان يكون قد اخذ نسخة من المعلومات وادخلها في حيازته الا انه لم يخرج المعلومات من حيازة صاحبها بل أبقاها في حيازته هذا ما جعل البعض ينفي ان تتم السرقة على برامج والمعلومات وبالتالي يعارض هذا الاتجاه إمكانية ان تكون البرامج محلا للسرقة لأنها اشياء غير محسوسة وغير مادية. [3]

1.2-من حيث تحديد الركن المادي: في الجرائم المعلوماتية تثير جملة من الصعوبات التي تفرضها طبيعة الوسط التي تتم فيه الجريمة والمتمثل في الجانب التقني بمعنى انها يتم من خلال المعالجة الألية للبيانات او عن طريق شبكة الأنترنت.

---

[1] تركي بن عبد العزيز بن تركي ال سعود، **السرقة الإلكترونية بين الحذر والتعزير**، مذكره لنيل شهادة الماجستير في العلوم الجنائية، أكاديمية نايف العربية للعلوم الأمنية، قسم الحقوق، الرياض، 2011، ص 77.

[2] سالم بن حمزة المدني، **مدى إمكانيه تطبيق الحدود على الجرائم الإلكترونية**، مجلة الحجار العالمية المحكمة للدراسات الإسلامية والعربية، مجلد 6، العدد 1، 2014، ص73.

[3] تركي بن عبد العزيز بن تركي ال سعود، مرجع سابق، ص 90.

2.2-من حيث السلوك الاجرامي: لابد ان تتم من خلال استخدام أجهزه الحاسوب الآلي وشبكة الانترنت وعلى ذلك فإن العلاقة السببية تستوجب ان يكون السلوك المادي يتم من خلال أجهزة الحساب الآلي وينتج عنه ضرر بالمصلحة المحمية.

3.2-من حيث العلاقة السببية: في مجال الحاسوب والانترنت تعد من المسائل الصعبة والمعقدة بالنظر الى تعقيدات صناعتها والتطور امكانياتها، اضافة الى تعدد اساليب الاتصال بين الأجهزة الإلكترونية، وتعد المراحل التي تمر بها الأوامر المدخلة حتى تخرج وتنفذ النتيجة المراد الحصول عليها كل ذلك سيؤدي حتما الى صعوبة تحديد الاسباب الحقيقية للإساءة المرتكبة في هذه المسؤولية.[1]

الفرع الثاني خصائص جريمة السرقة الرقمية.

نبرز من خلال هذا الفرع أهم مميزات جريمة السرقة الرقمية التي تمنحها الطابع الخاص وهي في الحقيقة نتائج ذلك التطور الهائل في تقنية المعلومات والاتصالات وبالتالي نذكرها كما يلي:

أولا_ جريمة السرقة الرقمية تنفذ عن بعد:

تتميز جريمة السرقة الرقمية بأن تنفيذها يتم عن بعد، أي يكون الجاني في مكان بعيد عن مكان الجريمة وعن مكان المسروق ذلك انه بفعل تقنية المعلومات فان الجاني لا يحتاج لتنفيذ الجريمة الى تواجد في مكان الجريمة وموضع المال المسروق بل يمكنه الوصول الى المعلومات باستخدام تقنية الاتصال عن بعد غير شبكة الوسائل والاتصال التي بعد ان يصل الى المعلومات عن طريق هذه التقنيات يمكنه ان يقوم بنسخها والاستيلاء عليها.[2]

ثانيا_ جريمة السرقة الرقمية جريمة عالمية.

بعد ظهور شبكة المعلومات لم يكن هناك حدود مرئية او ملموسة تقف امام نقل المعلومات عبر الدول المختلفة، فالمقدرة التي يتمتع بها الحواسيب وشبكاتها في نقل كميات من المعلومات وتبادلها بين الأنظمة يفصل بينها ألاف الأميال قد أدت نتيجة مؤداها ان أماكن متعددة في الدول مختلفة تتأثر بالجريمة الإلكترونية الواحدة في أن واحد، فالسهولة في حركة المعلومات عبر الأنظمة التقنية الحديثة مما جعل بالإمكان إرتكاب الجريمة عن طريق حاسوب موجود في دولة معينة بينما يتحقق فعل الاجرامي في دوله أخرى.[3]

ثالثا-خاصية جريمة السرقة الرقمية صعبة الاثبات.

تتميز بصفة عامه الجرائم الرقمية او الإلكترونية بصعوبة اكتشافها المتابعة فيها بحيث لا تترك أثرا فهي مجرد أرقام تتغير في السجلات، فمعظم الجرائم الإلكترونية تم اكتشافها بالصدفة وبعد

---

[1] احمد محمد عبد الرؤوف المنيفي، مرجع سابق، ص 41.
[2] نهله عبد القادر المومني، **جرائم المعلوماتية**، الطبعة 2، دار الثقافة للنشر والتوزيع، عمان، 2010، ص 55.
[3] هشام محمد رستم، **الجرائم المعلوماتية اصول التحقيق الفني، مجلة الامن والقانون**، دبي، المجلد 5، العدد 2، 1999، ص 240.

وقت طويل من ارتكابها ،ويلاحظ ان الجرائم التي لم تكتشف هي اكثر بكثير من تلك التي كشف عنها على أساس أنها تفتقر الدليل المادي التقليدي كالبصمات ،كما يصعب الاحتفاظ الفني بأثارها وإن وجدت تحتاج لخبرة فنية خاصة يتعذر على المحقق التقليدي منالها او التعامل معها لأنها تعتمد غالبا على قصة الذكاء المصحوب بالخداع التضليل بدس البرامج او وضع كلمات سرية ورموز تعوق الوصول الى دليل وقد يلجا مرتكبيها لتشفير التعليمات لمنع ايجاد اي دليل يدينه. [1]

رابعا: جريمة السرقة الرقمية جريمة خفية.

فجريمه السرقة الرقمية في أكثر صورها خفية لا يلاحظها المجني عليه ولا يدري بوقوعها والامعان في حجب السلوك المكون لها واخفائه عن طريق التلاعب غير المرئي في النبضات والذبذبات الإلكترونية التي تسجل البيانات عن طريقها امر ليس فيه الكثير من الاحوال بحكم توافر المعرفة والخبرة في مجال حسابات غالبا لدى مرتكبيها.[2]

خامسا: جريمة السرقة الرقمية جريمة مستحدثة.

الجريمة الإلكترونية أو الرقمية تعد أبرز الجرائم الجديدة، التي يمكن ان تشكل أخطارا جسيمة فلا غرابة ان تعتبر الجريمة الإلكترونية من جرائم المستحدثة بحيث ان تقدم التكنولوجي الذي تحقق في سنوات القليلة الماضية جعل العالم بمثابة قرية صغيرة، ونجد ان هذا التقدم بقدراته وامكانياته قد تجاوز وفاق أجهزه الدولة الرقابية، وأكثر من ذلك فانه قد أضعف من قدرات أجهزة الدولة في تطبيق قوانينها التي اصبحت لا تواكب هذا التطور وبالتالي هذا الضعف والعجز أصبح يهدد أمن الدولة ومواطنيها. [3]

سادسا: جريمة السرقة الرقمية جريمة لا تتطلب الأدلة.

ذلك ان الجاني في الجريمة الرقمية لا يقوم بنقل أصل المعلومات المسروقة من مكانها والاستيلاء عليها بل يقوم بنسخها في حين يبقى الاصل لدى الملك وهذا يساعد على جعل المجني عليه لا يشعر بارتكاب الجريمة.[4]

سابعا: جريمة السرقة الرقمية جريمة تقنية.

تتميز جريمة السرقة الرقمية بأن مرتكبها هو مجرم من نوع خاص تتوفر فيه المعرفة التقنية العالية بالحاسب الآلي ونظام الاتصالات والشبكات ومع ان جميع الجرائم المعلوماتية تتطلب معرفه تقنية مرتكبها الا ان جريمة سرقة الرقمية بالذات تتطلب لارتكابها مهارات تقنيه عالية أكثر عمقا في مجالات الوصول عن بعد واختراق الانظمة لحماية الامن المعلوماتي.[5]

---

[1] تركي بن عبد الرحمن الموشير، **بناء نموذج أمني لمكافحه الجرائم المعلوماتية وقياس فعاليته**، الطبعة الأولى، دار الجامعة نايف للنشر، الرياض 2012، ص 20.

[2] خالد ممدوح ابراهيم، **أمن الجريمة الإلكترونية**، ط1، الدار الجامعية، الإسكندرية، 2008 ص 51.

[3] احمد عبد الرؤوف المنيفي، مرجع سابق، ص 42.

[4] احمد عبد الرؤوف المنيفي، مرجع سابق، ص 43.

[5] فؤاد حسين العزيري، **جرائم المعلوماتية**، ط 1، دار الفكر الجامعي، الإسكندرية، ص 41.

المطلب الثاني: العوامل الشخصية لجريمه السرقة الرقمية

سنتناول في هذا المطلب مختلف فئات مرتكبي جريمة السرقة الرقمية وذلك في الفرع الاول دوافعهم الرئيسية لارتكابها في الفرع الثاني على التوالي.

الفرع الأول: فئات مرتكبي جريمة السرقة الرقمية.

هذه الجريمة تطلب قدره العقلية والذهنية العميقة لدى مرتكبيها حيث يحقق اهدافه من خلال استخدام هذه القدرات ويكون ذلك بكل هدوء دون اللجوء الى العنف والشغب وعليه يصنف مجرومها الى فئات التالية:

اولا: طائفة صغار مجرمي المعلومات:

يسميهم البعض صغار نوابغ المعلوماتي وهم مجموعه شباب صغار الذين لديهم الخبرة الكافية لاستخدام الحاسوب الالي ويمارسون هوايتهم بالدخول في النظم والبرامج المعلوماتية من اجل التسلية واللعب والاستطلاع. [1]

ثانيا: طائفة القراصنة.

تضم الاشخاص الذين يهدفون الى الدخول الى أنظمة الحسابات الألية الغير مصرح لهم بالدخول إليها وكسر الحواجز الأمنية الموضوعة لهذا الغرض وهذا بهدف إكتساب الخبرة او بدافع الفضول او لمجرد إثبات القدرة على إختراق هذه الأنظمة [2]يصنفون الى:

1-قراصنة محترفون: وهم الأخطر لأنهم يعلمون جيدا ما يريدون وهم ذوي ميول إجراميه تهدف بالأضرار بالغير ويتوصلون الى اهدافهم باستخدام ما لديهم من مهارات يطورونها باستمرار في لغة البرمجة وتشغيل وتصميم وتحليل البرامج وتشغيلها بسرعة ويستهدفون المصارف بغرض سحب الأموال من حساباتها واختراع واختراق المواقع المحكمة والحساسة بغرض التلاعب ببنيتها وتدميرها.

2-القراصنة الهواة: يعتمد المنتمون لهذه الفئة في القيام بعملياتهم على البرامج الجاهزة سواء عن طريق شراء او التحميل من المواقع الانترنت ويقومون بزرع هذه البرامج في الحسابات الضحايا عن طريق البريد الالكتروني او ثغرات الوندوز ويقومون كذلك بسرقه الحسابات والتلاعب بإعدادات الحواسيب ويهدفون من خلال ذلك الى ظهور واثبات قدراتهم عن طريق ترك ما يثبت انهم قاموا بهذه الافعال بغرض انضمامهم فيما بعد لفئه الهاكرز. [3]

ثالثا: طائفة الموظفون العاملون في مجال الأنظمة المعلوماتية.

---

[1] نائلة عادل محمد فريد قوره، مرجع سابق، ص 61.

[2] عمر عبد القادر، **تحديات القانونية لأثبات الجريمة المعلوماتية**، ط 2، دار النشر الجامعي الجديد، تلمسان، الجزائر، 2021، ص47.

[3] نهله عبد القادر مؤمني، مرجع سابق، ص 85.

بحكم طبيعة العمل هؤلاء الموظفين ونظر لان النظام المعلوماتي في مجال عملهم اساسي ونضرا للمهارات والمعرفة التقنية التي يتمتعون بها فانهم يقترفون بعض الجرائم المعلوماتية التي من الممكن ان تحقق اهدافهم الشخصية واهمها كسب المادي، فالعلاقة الوظيفية التي تربط بين موظف والمجني عليه تجعل عملية ارتكابه الجريمة المعلوماتية أسهل نظرا للثقة الذي يتمتع بها وقد يكون هدفهم الربح المادي او الانتقام من اصحاب عملهم[1].

رابعا: طائفة المبرمجون.

هم أشخاص يتمتعون بقدرات عالية بصفتهم اختصاصيين في المعلوماتية مما يمكنهم من إخفاء دليل الجريمة المعلوماتية وتنصب معظم جرائمهم على شبكات تحويل الاموال ويقومون بالتلاعب بحسابات مصارف وفواتير الكهرباء والهاتف وتزوير البطاقات البنكية وهم من أخطر انواع الهاكرز لأنهم يضعون الادوات الخاصة بهم ويتحكمون بالشفرات وكيفية التعامل معها.

خامسا: طائفة المديرون.

هم اشخاص امكانياتهم اقل من المبرمجين يستندون في ارتكاب عملية الاختراق على ادوات غيرهم والتي قد تكون ملغمة او سليمة ولا يمكنهم صناعة ادوات الاختراق .[2]

سادسا: طائفة مجرمي المعلوماتية في إطار جريمة المنظمة.

تعتبر هذه الطائفة الاكثر شيوعا بين مجرمي المعلوماتية فهم يرتكبون جرائم المعلوماتية بحيث يترتب عليها في الكثير من الاحيان خسائر كبيرة تلحق بالمجني عليه حيث تتبنى هذه الجماعات اصحاب الكفاءات والخبرة والموهبين في مجال تقنية المعلومات ذلك بإغوائهم بالمال لينظموا الى صفوفهم وتقوم بتدريبهم وزيادة مهاراتهم في هذا المجال لخلق مجرمين متخصصين في جرائم معلوماتية في إطار هذه المنظمات ويمارسون نشاطات يمكن ان تدر ارباحا عليهم.[3]

الفرع الثاني: دوافع ارتكاب جريمة السرقة الرقمية.

المقصود بالدافع هو الغرض او السبب كلها متغيرات لها اهمية في القانون الجنائي وعليه هناك أسباب او دوافع مختلفة تدفع المجرم الى إرتكاب جريمة سرقه الرقمية نتطرق اليها على النحو التالي:

اولا –الدوافع الشخصية.

وهي تنقسم بدورها الى قسمين

1–الدوافع المالية.

[1] عمر عبد القادر، مرجع سابق، ص 48.
[2] نهله عبد القادر مومني، مرجع سابق، ص 88.
[3] نهله عبد القادر مومني، المرجع نفسه ص 90.

تعتبر اهم البواعث على ارتكاب الجرائم الإلكترونية لما تحققه من ثراء فاحش فالرغبة في تحقيق مكاسب مادية هائلة أحيانا بزمن قياسي قد يكون من أكثر البواعث التي تؤدي الى إقدام مجرمي المعلوماتية إما عن طريق المساومة على البرامج أو المعلومات أو عن طريق استعمال بطاقة سحب مزوره ومنتهية الصلاحية وغير ذلك[1] ،من امثله ذلك ما حدث في فرنسا عام 1986 كان العائد من ارتكاب جناية السرقة من محل السلاح 7000 فرنك فرنسي في حين ان جريمة الغش في مجال المعالجة الالية للمعلومات حصل منها الجاني على 670000 فرنك فرنسي [2].

2-الدوافع الذهنية.

يكون المجرم المعلوماتي هنا هدفه الرغبة في اثبات الذات وتحقيق إنتصار على تقنية الأنظمة المعلوماتية دون ان يكون لها نوايا اثمة ويرجع ذلك الى وجود عجز في التقنية التي تترك فرصة لمشيدي برامج النظام المعلوماتي لارتكاب تلك الجرائم.[3]

نذكر أمثله مواقع في فرنسا حيث نشرت "جريدة الاكسبريس" الفرنسية في سبتمبر عام 1983 عنوان ميلاد النزعة قام عامل يدعى **دولاند** بجريمة السطو تتلخص وقائعها في انه توجه الى أحد البنوك لإيداع شيك فشاهد في تلك اللحظة الموزع الآلي للنقود عند قيام مستخدمي الصيانة باستخراج نقود البنك في الألة عند الطلب عن طريق بطاقة خاصة فقام بالتدرب على الحاسب الآلي وقام بعملية السطو. [4]

ثانيا: الدوافع الخارجية

إذا يتأثر الانسان في بعض المواقف ويستسلم للمؤثرات والدوافع الخارجية بارتكابه بعض الجرائم المعلوماتية نتيجة لوجوده في بيئة المعالجة الألية للمعلومات وتعدد المؤثرات التي تدفع المجرم المعلوماتي اقتراف مثل هذه السلوك من بينها:

1-دافع الانتقام

قد يكون الانتقام مؤثرا في ارتكاب الجرائم المعلوماتية اذ قد لوحظ ان عاملين في قطاع التقنية أو مستخدمين لها في نطاق قطاعات العمل الأخرى يتعرضون على نحو كبير لضغوطات نفسيه ناجمة عن ضغط العمل والمشكلات المالية ومن طبيعة علاقات العمل المنفردة في حالات كثيرة مثلت قوه محركة لبعض العاملين لارتكاب جرائم المعلوماتية باعثها الانتقام من المنشأة[5]

2- دوافع التعاون وتواطئ على الاضرار.

---

[1] سوير سفيان، مرجع سابق، ص 26.
[2] معز خليل العمر، **جرائم مستحدثه**، الطبعة الاولى، دار وائل للنشر والتوزيع، عمان 2012، ص 218.
[3] معز خليل العمر، المرجع نفسه، ص 219.
[4] سوبر سفيان، مرجع سابق، ص 28.
[5] معز خليل عمر، مرجع سابق، ص 219.

يعتبر هذا النوع كثير التكرار في الجرائم المعلوماتية، وغالبا ما يحدث من المتخصصين في الأنظمة المعلوماتية حيث يقوم الاول بالجانب الفني او المشروع الاجرامي والاخر من المحيط او خارج المؤسسة المجني عليها لتغطية عمليات التلاعب وتمويل المكاسب المادية، وعادة ما يمارسون التلصص على الأنظمة وتبادل المعلومات بصفه منتظمة حول انشطتهم. [1]

ثالثا: دوافع من نوع اخر.

التنافس سياسي والاقتصادي قد يكون دافعا الى ارتكاب هذه الافعال، فقد قام بعض القراصنة المتواجدين في الارضي الروسية بإختراق نظم حسابات حكومية في الولايات المتحدة الأمريكية مدة عام كامل، حيث قاموا بسرقة معلومات غير سريه لكنها حساسة من اجهزه الحواسيب العسكرية الأمريكية.

اما دافع الايذاء وتهديد ينتشر نتيجة الوقوع تحت التهديد والضغط من الغير في مجالات الاعمال التجارية والخاصة بالتجسس والمنافسة [2]

المبحث الثاني: الأحكام الخاصة لجريمة السرقة الرقمية.

تعتبر جريمة السرقة الرقمية من بين الجرائم الواقعة على النظام المعلوماتي بحيث انها ترتكب بالاعتماد على العديد من الأساليب وتمر بالعديد من مراحل ومن هذا المنطلق قمنا بتقسيم المبحث الى المطلبين بحيث تتطرق بتفصيل إلى تطبيقات جريمة السرقة الرقمية حيث نستعرض في المطلب الاول تطبيقات جريمة السرقة الرقمية والتي تشمل تعريف المصنفات الرقمية وبيان أنواعها وصور استغلالها وفي المطلب الثاني نستعرض فيه تقنيات جريمة السرقة الرقمية والتي تشمل اساليب جريمة السرقة الرقمية وبيان المراحل الوصول الى ارتكابها.

المطلب الأول: تطبيقات جريمة السرقة الرقمية

قمنا بالتقسيم المطلب الى فرعين بحث تتناول في الفرع الاول سرقة المصنفات الرقمية من حيث تعريف المصنفات الرقمية وانواعها إضافة الى الاستغلال المالي في حين نتطرق في الفرع الثاني الى سرقة أرقام بطاقة الوفاء عبر الانترنت من خلال تعريف بطاقة الوفاء واليات السرقة التقنية لبطاقة الوفاء.

الفرع الأول: سرقة المصنفات الرقمية

مع انفتاح العالم على شبكة الانترنت وتزامنها مع حرية انسياب المعلومات دون تقييد او مراقبة لانسياب هذه المعلومة من أي جهة محددة سواء كانت مركزية او دولية تطورت صور التعدي لتطال حتى الملكية الفكرية للمؤلف من استغلال للمنصفات الرقمية ماليا.

[1] نهله عبد القادر مومني، مرجع سابق، ص 93.
[2] نهله عبد القادر مومني، المرجع نفسه، ص 94.

اولا: تعريف المصنفات الرقمية

تعتبر المصنفات الأدبية والفنية من المصنفات التي تقع عليها الحماية بموجب حق المؤلف والحقوق المجاورة والتي نص المشرع الجزائري على حمايتها في الأمر رقم 05/03 [1] ، والمصنف هو كل إنتاج ذهني ينطوي على شيء من الابتكار مفرغ في صورة مادية يبرز فيها إلى الوجود ، ويكون معدا للنشر وإعادة النشر، لكن لم يعرف القانون الجزائري في الأمر نفسه المصنف الأدبي والفني ولكن ذكر ما يمثله في المادة الرابعة من القانون نفسه والتي تنص في مجملها على انه "تعتبر على الخصوص كمصنفات أدبية أو فنية محمية كل من المصنفات الأدبية المكتوبة ، مصنفات المسرح والمصنفات الدرامية، مصنفات الموسيقى ، مصنفات الفنون والرسوم والمصنفات التصويرية وحتى مبتكرات الألبسة للأزياء والوشاح "، وتشترط المصنفات مجموعة من الشروط وهي كالاتي:

1-شرط الابتكار: ويقصد به أن يكون هناك بصمة شخصية للمؤلف في مصنفه أي يكفي أن يقدم المصنف شيئا يعبر عن مجهود ذهني للمؤلف في صورة جديدة تظهر ذاتية وشخصية.

2-التعبير على الأفكار: وذلك لان الحماية لا تنصب على طريقة التعبير الفكرة إما الفكرة بحد ذاتها فإنها تخضع للقوانين الخاصة بالملكية الصناعية

3-إفراغ المصنف في صورة مادية يبرز فيها إلى الوجود: يعني إفراز المصنف في صورة مادية أي لا يكون مجرد فكرة ويجب أن تكون أخذت وضعها النهائي وأصبحت معدة للطبع والنشر وإفراغه في صورة مادية يمكن التعبير عنه كما تختلف صوره من مكتوبة موسيقية، فتوغرا فيا[2]

ثانيا: انواع المصنفات

إن أهم صور المصنفات التي يمكن الاعتداء عليها تتمثل في:

1-المصنفات المكتوبة: ويدخل في ذلك الكتب والكتيبات والمقالات والنشرات وغيرها من المصنفات المكتوبة مثل البريد الالكتروني وملحقاته

2-المصنفات الموسيقية المسموعة: وكل ما هو مقترن بالألفاظ أو غير ما قترن بها، والمصنفات السمعية البصرية كالأفلام والأغاني والمقطوعات الموسيقية المادة بالأنترنت أو المودعة عليه.

3-الصور التي تمر عبر الانترنت: ومن ثم فان نشر الصور الكترونيا يمثل تعديا على حق المؤلف ويدخل في مصنفات الرسم بالخطوط أو بالألوان والنحت والطباعة على الحجر وعلى الأقمشة وأية مصنفات مماثلة في مجال الفنون الجميلة والمصنفات الفوتوغرافية وما يمثلها ومصنفات الفن التشكيلي والتطبيقي.

---

[1] الأمر 05/03 **المتعلق بحقوق المؤلف والحقوق المجاورة**. الصادر بتاريخ 23/7/2003 الموافق ل 23 جمادى الأولى عام 1424 هجري الموافق عليه بالقانون 03/17 الجريدة الرسمية رقم 44. ص 4.

[2] ياسين بن عمر، **جرائم تقليد المصنفات الأدبية والفنية واليات مكافحتها**. مذكرة مقدمة لنيل درجة الماجيستر، تخصص قانون جنائي. كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة ورقلة قاصدي مرباح، السنة الجامعية 2010/2011، ص14.

4-الصور التوضيحية والخرائط الجغرافية والرسوم التخطيطية وكل ما يتعلق بالمصنفات الثلاثية الأبعاد المتعلقة بالجغرافيا أو الطبوغرافيا أو التصميم المعمارية.

5-المصنفات المشتقة: وهي التي تستمد أصلا من مصنف سابق الوجود كالترجمات والتوزيعات الموسيقية وتجمعات المصنفات بما في ذلك قواعد البيانات المقروءة سواء من الحاسب أو غيرة وحتى مجموعات التعبير الفلكلوري مادامت مبتكرة من حيث ترتب أو اختيار محتوياتها[1].

6-المصنفات الرقمية الحديثة: من أهم المصنفات الحديثة التي أضافها المشرع الجزائري في الأمر 05/03 وهي:

1.6-برامج الحاسب الآلي: وهي مجموعة من التعليمات التي تستطيع الآلة قراءتها والقيام بإنجاز وظيفة أو أداء مهمة بواسطة المعالجة الآلية للمعطيات وهي نوعيين برامج التشغيل وبرامج التطبيق

2.6-قواعد البيانات: وهي عبارة عن معطيات ومعلومات مجمعة تتعلق بموضوع ما يتم تخزينها على دعامات مادية متصلة بالحاسب الآلي تتميز بكونها مرتبة ترتيبا منطقيا ومصممة بحيث يسهل البحث والرجوع لما ورد فيها من معلومات، كما يجب توفير طابع الابتكاري المستند أساسا من طبيعة البيانات نفسها أو من طريقة ترتيبها أو إخراجها وتجميعها واسترجاعها.[2]

ثالثا: صور الاستغلال المالي للمصنفات.

إن الحق المالي هو إعطاء لكل صاحب إنتاج ذهني حق الاستغلال بما يعود عليه بالمنفعة أو الربح أي هو القيمة المادية لابتكاره وإبداعه، وهو حق استئثاري مقرر للمؤلف وحده كما لا يجوز إن يستعمله إلا بإذن منه كما يجب أن تتوفر شرطيين لإجراء أي تصرف على الحق المالي وهما:

الشرط الأول: أن يتم إفراغ التصرف على الحقوق المالية في شكل مكتوب وتعتبر الكتابة هنا شرط للانعقاد وليس للإثبات.

الشرط الثاني: تحديد مضمون التصرف صراحة وبوضوح تام، أي بيان مداه ومدة الاستغلال والغرض منه، ولقد تباينت صور استغلال المصنفات من خلال قوانين حق المؤلف والاتفاقيات الدولية الخاصة بحق المؤلف صورا رئيسية لاستغلال المصنف ماليا وللاستغلال نوعان استغلال مباشر واستغلال غير مباشر.

1-الاستغلال المباشر :ويتم عن طريق نقل المصنف إلى الجمهور بشكل علني وعام أي عرضه على الجمهور عرضا مباشرا من قبل المؤلف أو الغير ممن قد يكون قد تلقى هذا الحق من المؤلف كما يسمى هذا الحق بالأداء العلني وما يهم ليس كيفية نقل المصنف إلى الجمهور وإنما العلنية في ذلك فلا يشترط النشر في مكان معين أو بشروط معينة بشكل معين فالمهم هو أن يحصل

[1] محمد حسين منصور، **المسؤولية الالكترونية**، دار الجامعة الجديدة، الاسكندرية – مصر، 2009، ص 264.
[2] ياسين بن عمر. مرجع السابق، ص 15-16.

الإعلام للجمهور، فحق الاستغلال قاصر على المؤلف وحده وليس للغير مباشرة هذا الحق إلا بعد الحصول على إذن مكتوب منه أو من خلفائه.[1]

2-الاستغلال غير المباشر: يحصل الاستغلال غير المباشر من خلال نقل المصنف إلى الجمهور بطريق النسخ وليس من خلال النسخة الأصلية، فان لم ينشر المؤلف مصنفه بنفسه فقد يختار نشره بواسطة نسخ نماذج أو صور للمصنف يكون في متناول الجمهور إذ يملك أي فرد أن يحصل على نسخة منه. [2]

الفرع الثاني: سرقة ارقام بطاقات الوفاء عبر الانترنت

وتعد بطاقة نظام جديد في البيئة التجارية انشأته الأعراف المصرفية وساعدت في انتشاره التكنولوجية الحديثة، وبتطور وسائل الحماية ظهرت حالات من الاستعمال غير مشروع للبطاقة من عملية السرقة التي أصبحت تمس أرقام بطاقات الوفاء عبر مواقع الانترنت.

أولا: تعريف بطاقة الوفاء

تعد بطاقة الوفاء وسيلة تستخدم من قبل حاملها الوفاء بالتزاماته المالية بدلا من الدفع الفوري بالنقد كما يمكن إصدارها للعميل وفقا لسقف ائتماني معين متفق عليه وفقا لشروط استخدامها التي تكون معدة سلفا من قبل المصدر كما لها عدة أشكال مختلفة فمنها المحلية والدولية وهناك أيضا البطاقات الذهبية والتي تمنح حاملها سقف ائتماني عالي جدا، وهي بطاقة بلاستيكية الصنع مستطيلة الشكل تسمح لحاملها وفاء ثمن السلع والخدمة التي يحصل عليها من بعض المحلات التجارية التي تقبلها بموجب اتفاق دائما من الجهة المصدرة لها وذلك ثمن البضائع والخدمات من حساب العميل المشتري أي حاملها إلى حساب مقدم الخدمة أو السلعة ويتم ذلك بإحدى الطريقتين وهما: [3]

1-الطريق المباشرة: والتي يتم فيها خصم قيمة العملية المنفذة بواسطة البطاقة أو حساب حاملها بنفس لحضت تمرير البطاقة في الجهاز المخصص لها ويتم في نفس الوقت تحويل القيمة إلى حساب التاجر ويوقع الحامل على نسخة الفاتورة وبذلك تكون البطاقة بمثابة دفع فوري.

2-الطريق غير المباشر: وهذا يقوم عميل البنك بتقديم بطاقته إلى نحو تحتوي على اسم المؤسسة المصدرة لها وشعارها واسمه وتوقيعه ورقم البطاقة وتاريخ انتهاء العمل بها إلى التاجر الذي يقوم بتدوين تفصيلات عن حامل البطاقة ومعلومات عن بطاقه على عدة نسخ يوقعها حامل البطاقة و ارسال نسخة من هذه البيانات إلى الجهة المصدرة للبطاقة ليتم تسديدها كما يمكن أن تحل بطاقة

---

[1] عمر علي نايت، **الملكية الفكرية في إطار التجارة الالكترونية**، مذكرة مقدمة لنيل درجة الماجيستر، في العلوم الجنائية وعلم الاجرام، كلية الحقوق والعلوم السياسية ، جامعة مولود معمري، تيزي وزوو، 2014 ، ص 102.

[2] عمر علي نايت، نفس المرجع السابق، ص 103.

[3] وسام فيصل محمود الشواورة، **المسؤولية القانونية عن استخدام غير المشروع لبطاقات الوفاء**، الطبعة الأولى، دار-وائل-للنشر، عمان, 2013، ص 13-14.

الوفاء محل الشبك وتسمح لحاملها بتنفيذ مشترياته من السلع والخدمات لدى التجار المنضمين النظام الوفاء بدون وفاء ينوي من جانبه وإنما يكفي تقديم بطاقته . [1]

لم يتناول المشرع العربي نظام بطاقة الوفاء بالتقنين التشريعي وبيان ذلك أنها لم ترد في قوانين التجارة العربية على عكس التشريعات الغربية التي كرست أمس ومبادئ التنظيم القانوني للوفاء بالبطاقات منذ 1974 حيث واكبت هذه التشريعات التطور التجاري السريع الذي يحدث على ساحة وسائل الدفع، ولذلك عرفت بطاقة الوفاء من جانب الفقه العربي على أنها البطاقة التي ينحصر دورها في كونها أداة للوفاء يثمن السلع والخدمات التي يحصل عليها حاملها من بعض التجار المقبولين لدى الجهة المصدرة للبطاقة "، كما عرفها التشريع الفرنسي على أنها: أداء تصدر من إحدى المؤسسات الائتمان أو إحدى الجهات الخاصة بنشاط رقابة مؤسسات الائتمان كما تسمح لحاملها سحب أو تحويل تفرد من حسابه " [2]. أما المشرع الجزائري تناولها بالتعريف فقط وذلك من خلال المادة 543 مكرر 23 من قانون 05/02 دون أن تدخل في تنظيمها نصوص قانونية أمرة لأنها حديثة المولد وبذلك يكون سهل على البنوك أن تصدر هذه البطاقات بما يتماشى مع البيئة التجارية وان لا يؤدي وضعها في قوالب القانونية إلى حموضها. [3]

ثانيا: مكونات بطاقة الوفاء.

تبين هذه المكونات على أساس أنها أهم العناصر التي تتم عليها السرقة المعلوماتية البطاقة الوفاء وهي كالاتي.

1-المكونات الشكلية: وهي أن تحمل البطاقة ميزة المنظمة، كما تكون مقسمة إلى جزئيين (اسم المنظمة والعلامة المانية بشرط توفر عليها شعار الفيروس والعلامة المائية التي تتمثل في طائر يحرك جناحيه[4].

2-المكونات المادية:يتم وضع الغلاف وجسم البطاقة عادة من مادة يطلق عليها الدائن البولي فينيل كلورد) وهي الأكثر شيوعا في صناعة هذه البطاقة، ويتم تغليف البطاقة بمواد كيمائية أخرى تشكل غطاء للبطاقة وذلك تمهيدا الصياغة البيانات والمعلومات عليها وكلمة لدائن تعني مركبات لينة وقابلة التشكل عند تكوينها ثم تصبح صلبة بعد ذلك موأهم خصائص هذه اللدائن المرونة والقابلية للتشكل والشفافية و القابلية الألوان متعددة عدم التأثير بالعوامل الجوية أو الأوكسجين عدم الصدأ، الثبات ضد المواد العضوية والكيماوية توافرها بكثرة رخصة الثمن القابلية للحام والالصاق، وانخفاض توصيلها للحرارة والكهرباء . [5]

---

[1] وسام فيصل محمود الشواورة، المرجع السابق، ص14-15.
[2] وسام فيصل محمود الشواورة، المرجع نفسه، ص 15.
[3] عماد علي الخليل، **الحماية الجزائية لبطاقة الوفاء دراسة تحليلية مقارنة**، طبعة الأولى، دار-وائل-للنشر، عمان, 2000، ص 7-8-9.
[4] وسام فيصل محمود الشواورة، مرجع سابق. ص 21.
[5] وسلم فيصل محمود الشواورة المرجع نفسه، ص 23- 24.

3-المكونات المعلوماتية البطاقة الوفاء

ويقصد بذلك البيانات التي تحتويها بطاقة الوفاء مثل:

1.3-اسم صاحب البطاقة وعادة ما يكون مطبوعا على الوجه الأمامي للبطاقة وبالحروف البارزة.

2.3-سعدة صلاحية تاريخ انتهاء العمل بها حيث لا يمكن تداولها بعد انتهاء هذا التاريخ.

3.3-التوقيع ويوجد بظهر البطاقة شريط يوقع عليه حاملها الشرعي المتعاكس مع مصدرها وفائدة هذا التوقيع هي أن المتعامل مع بطاقة الوفاء والقابل لها يستطيع أن يتأكد من توقيع صاحبها.

4.3-صورة صاحب البطاقة أدخلت مؤخرا تقنية وضع الصورة وذلك لتأكيد من شخصيته ولمنع استخدامها من قبل الغير

5.3-رقم البطاقة وتستخدم الطابعة الممغنطة لبطاقة هذا الرقم فيظهر بشكل بارز على البطاقة وهذا الرقم يختلف عن الرقم السري لصاحب البطاقة

6.3-الشريط الممغنط أو المغناطيسي وهو موجود بخلفية البطاقة ويحمل جميع البيانات الخادم وغالبا ما تستعمل كل هذه المعلومات للسطر على أرقام بطاقات الوفاء وسرقتها.[1]

ثالثا: آليات السرقة التقنية لبطاقة الوفاء.

تعتمد آلية الشراء بواسطة بطاقات الوفاء عبر مواقع شبكة الانترنت العالمية على تزويد التاجر برقم البطاقة الخاص بالعميل وعنوانه البريدي وبضع معلومات أخرى لتصله بذلك السلعة المطلوبة خلال الفترة الزمنية التي يتم الاتفاق عليها وفي الوقت التي تظهر فيه شبكات البنوك العالمية وشركات الوساطة المالية إجراء عمليات التقاطي بين الحاسبات وقيد الفوائد والعمولات إلا أن ميزة استخدام شبكة الانترنت العالمية قابلتها استغلال غير مشروع المواطن الضعف التي أكتفت آلية العمل بها في النظام بحيث يتمكن أي محرم يستند إلى مبادئ بسيطة في علم برمجة الحاسوب واستخدام الانترنت يهدف الاعتداءات على الدمة المالية لصاحب البطاقة، كما يعتمد نشاط هذه الفئة من المجرمين على استخدام طرق وأساليب متعددة لا تقع تحت حصر لكن أشهرها يتمثل في أسلوبيتين هما: [2]

1-لاحتراق غير المشروع المنظومة خطوط الاتصال العالمية التي تربط جهاز الحاسوب الخاص بالمشتري بذلك الخاص بالتاجر.

2_تقنية تفجير الموقع والهدف بقصد كشف البيانات والمعلومات الخاصة بالبطاقة والتي قد تكون مركزة في موقع التاجر أو موقع العميل المشتري بحيث يهدف المجرم من خلال ذلك الحصول

[1] وسام فيصل محمود الشواورة، المرجع السابق، ص 20.
[2] عماد على الخليل، مرجع سابق، ص 101.

على أرقام وبيانات المتعلقة ببطاقة العملاء ليقوم باستخدامها في تحقيق الإثراء أو التحويل غير المشروع على حساب أصحاب البطاقات.[1]

المطلب الثاني: تقنيات جريمة السرقة الرقمية.

تعتبر جريمة السرقة الرقمية أحد اهم الجرائم المعلوماتية المستحدثة نظرا لتطورها السريع وذلك تماشيا والتطور التكنولوجي الواقع والذي على أثره تطورت أساليب ارتكابها وتعددت مراحلها ومن هذا المنطلق قمنا بتقسيم هذا المطلب الى فرعين بحيث نتناول في الفرع الأول أساليب الجريمة الرقمية والتي نستعرض فيه أساليب التلاعب في بطاقات الوفاء بالإضافة بالإضافة الى البرامج الخبيثة اما بالنسبة للفرع الثاني نتناول من خلاله مراحل جريمة السرقة الرقمية.

الفرع الأول: أساليب جريمة السرقة الرقمية.

ان الاستخدام غير مشروع لأرقام بطاقات الوفاء لا يقتصر فقط على الغير، وقد يستخدمها حاملها الشرعي بطريقة غير مشروعة عبر الأنترانت، ولهذا فان التلاعب في ارقام بطاقات الوفاء قد يقع من الغير اومن قبل حاملها الشرعي، وفيما يلي نفصل الأساليب والطرق التي يتم من خلالها الاعتداء على ارقام بطاقات الوفاء.

أولا: أساليب التلاعب في بطاقة الوفاء.

يقصد بالغير في هذه النقطة كل الأشخاص الذين لا صلة لهم بأطراف بطاقة الوفاء أي هم قراصنة المعلوماتية وهناك أساليب وطرق مختلفة ومتعددة لا تقع تحت الحصر يستخدمها هؤلاء في الحصول على أرقام وبيانات بطاقات الائتمان عن طريق الإنترنت لاستخدامها بطريقة غير مشروعة في الحصول على السلع والخدمات عبر تلك الشبكات، يتمثل أشهرها في الأساليب التالية:

1-الاختراق: غير المشروع لمنظومة خطوط الاتصالات العالمية أو ما يعرف باسم illegal access أو التجسس وبعد هذا الأسلوب من أخطر الأساليب التي تهدد فكرة التجارة عبر الإنترنت، إذ يربط جهاز الحاسوب الخاص بالمشتري بذلك الخاص بالتاجر حيث يستخدم قراصنة المعلوماتية برامج تتيح لهم الاطلاع على البيانات والمعلومات الخاصة بالشركات التجارية والكبرى والأفراد على شبكة الإنترنت.

وعلى ذلك يتمكنون من الحصول على بيانات بطاقة الائتمان المستخدمة في التجارة الإلكترونية عبر تلك الشبكة ولعل الدافع الأساسي وراء اللجوء إليه يتمثل في الرغبة الكامنة في نفوس محترفي إجرام التقنية في قهر نظام التقنية والتفوق على الحماية وتعقيلها. [2]

[1] عماد على الخليل، المرجع السابق، ص 102.
[2] عماد على خليل، المرجع نفسه، ص 3.

2-أسلوب الخداع: ويتحقق هذا الأسلوب بإنشاء مواقع وهمية على شبكة الإنترنت المشابهة تماما المواقع الشركات والمؤسسات التجارية الأصلية الموجودة على هذه الشبكة بحيث يظهر بأنه الموقع الأصلي المقدم لتلك الخدمة.[1]

وإنشاء هذا الموقع يقوم القراصنة بالحصول على كافة بيانات الموقع الأصلي من خلال شبكة الإنترنت ،مع تعديل بياناته السابقة بالشبكة، بحيث لا يكون هناك غير موقع واحد بنفس العنوان و هو الموقع الوهمي والذي يصبح يستقبل كافة المعاملات المالية و التجارية التي يقدمها الموقع الأصلي لأغراض التجارة الإلكترونية و من بينها البيانات الخاصة ببطاقات الائتمان والرسائل الإلكترونية الخاصة بالموقع الأصلي الاطلاع عليها،ومن ثم الاستفادة غير المشروعة من المعلومات المتضمنة فيها، وذلك على نحو يضر بالشركات والمؤسسات صاحبة الموقع الأصلي ويدمر ثقة المستخدمين في التجارة الإلكترونية.[2]

3-تقنية تفجير الموقع المستهدف: ويوجه هذا الأسلوب عادة إلى الحواسب المركزية للبنوك والمؤسسات المالية والمطاعم والفنادق ووكالات السفر بهدف تحصيل أكبر عدد ممكن من أرقام بطاقات الائتمان. ويستند هذا الأسلوب أساسا على مئات آلاف من الرسائل الإلكترونية من جهاز الحاسوب الخاص إلى الجهاز المستهدف بهدف التأثير على سعته التخزينية بحيث يؤدي شكل هذا الكم الهائل من الرسائل الإلكترونية في نهاية المطاف إلى إغراق الموقع العامل على الشبكة وتفجيره وتشتيت المعلومات والبيانات المخزنة فيه، لتنقل بعد ذلك للجهاز الخاص بالمجرم أو تمكنه من حرية التجول في الموقع المستهدف بسهولة ويسر، فيستولي بذلك على ما يشاء من أرقام وبيانات خاصة ببطاقات ائتمانية مملوكة لغيره. [3]

4-تخليق أرقام البطاقات: ويعرف هذا الأسلوب باسم Card Math وهو يعتمد بالدرجة الأولى على إجراء معادلات رياضية وإحصائية بهدف تحصيل أو تخليق أرقام بطاقات ائتمانية مملوكة للغير، وهي كل ما يلزم للشراء عبر شبكة الإنترنت[4] حيث يتوافر في الأسواق برامج تشغيل باسطة وخاصة تتيح امكانية تخليق أرقام بطاقات بنك معينة من خلال تزويد الحاسوب بالرقم الخاص بالبنك المصدر للبطاقات.[5] وعادة ما يقوم مجرمو البطاقات ينشر هذه المعادلات وبيان الكيفية

---

[1] جميل عبد الباقي الصغيرة, **الحماية الجنائية والمدنية البطاقات الائتمان الممغنطة**، الطبعة الأولى ،دار النهضة العربية، القاهرة,1999، ص37.

[2] نائلة عادل محمد فريد قوره، مرجع سابق، ص 562.

[3] عصام عبد الفتاح مطر، **التجارة الالكترونية في التشريعات العربية والأجنبية**، ط 2، دار الجامعة الجديدة، الإسكندرية, 2009، ص 359.

[4] على حسن عباس، **مخاطر استخدام بطاقات الدفع الالكتروني عبر شبكة الإنترنت (المشاكل والحلول، ورقة عمل مقدمة إلى ندوة الصور المستحدثة لجرائم بطاقات الدفع الالكتروني التي نظمها مركز بحوث الشرطة)** بأكاديمية الشرطة القاهرة، 1998، ص 17.

[5] سليمان أحمد فضل، **المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية**، ط 2، دار النهضة العربية، القاهرة, 2007، ص 171.

التي يمكن من خلال اتباعها خطوة بخطوة الحصول على أرقام البطاقات الائتمانية المملوكة للغير عبر مواقعهم المنتشرة على شبكة الانترنت.

ثانيا: البرامج الخبيثة

1-**فيروس الحاسب:** هي محتوى معلوماتي ضار وهي عبارة عن مجموعة من التعليمات التي تتكاثر بمعدل سريع، لدرجة تصيب النظام المعلوماتي بالشكل التام [1] فهي عبارة عن برنامج يتم تسجيله أو زرعه على الاسطوانات الخاصة بالحاسوب الآلي، ويظل خاملا لفترة محددة، ثم ينشط فجأة في توقيت معين ليدمر البرنامج أو المعلومات المخزنة أو يتلفها جزئيا وذلك بالخرق أو تعديل [2] إضافة إلى ذلك يعتبر الفيروس هو برنامج مكتوب بإحدى لغات البرمجة بواسطة أحد المخربين بهدف إحداث الضرر بنظام الحاسوب، ويمثل نوعا من أنواع جرائم التعدي على نظم الحاسبات[3] يستخدم فيروس الحاسب الآلي العديد من التقنيات المعروفة لأداء مهامه التخريبية، ومع ذلك فان تقنية نسخ الفيروس نفسه ذاتيا هي المعيار الشائع الذي يميز الفيروس عن الأنواع الأخرى من برامج الكمبيوتر.[4]

وتتميز هذه الفيروسات بقدرتها على التكاثر والانتقال من جهاز إلى آخر عن طريق الملفات المتبادلة بين المستخدمين. [5] وهناك أنواع عديدة من الفيروسات ومنها ما يلي:

2-حصان طروادة: وهي نوع من الفيروسات يدخل الحاسب الآلي عن طريق البرامج، ويقوم بتخريب الحاسب الآلي[6]وهي برامج خبيثة تختفي بداخل برامج مهمة وغرضه هو جمع المعلومات وإرسالها ويسمح للهاكرز، بتصفح جهازك والتحكم بملفاتك.[7]

3-فيروسات خفية: هذه الفيروسات تفلت من الرقابة بواسطة قدرتها على التنكر، مما يجعل اكتشافها صعب [8]

4-فيروسات المقيمة: فهي كلما تم تشغيل البرنامج المصاب بواسطة المستخدم، يتم تنشيط الفيروس، ويقوم بتحميل وحدة النسخ التماثل الخاصة به في الذاكرة ثم ينقل التحكم مرة أخرى إلى

---

1 أيمن عبد الله فكري، **الجرائم المعلوماتية دراسة مقارنة في التشريعات العربية والأجنبية**، الطبعة الأولى، معهد الإدارة العامة، الرياض، ص 45.

2 عبد الرحمان عبد الله سند، **الاحكام الفقهية للتعاملات الالكترونية (الحاسب الالي وشبكة المعلومات الانترنت)**، الطبعة الأولى, دار الوراق، عمان –الأردن، 2004، ص 345.

3 أسامة فتحي، **فيروسات الحاسوب**،دط ، دون بلد النشر، دون سنة النشر، ص 3.

4 احمد محمد عبد الرؤوف المنيفي، **فيروسات الحاسب الآلي**، اليمن، 2019، ص 4

5 عبد الله دعش العجمي، **المشكلات العملية والقانونية للجرائم الالكترونية دراسة مقارنة**، مذكرة لنيل شهادة الماجستير في القانون العام، جامعة الشرق الأوسط، 2014، ص 7.

6 انظر موقع الكتروني: **https://www.mlzamty.com/virus-damage** يوم الاطلاع 23/4/2021على الساعة22:48 مساءا

7 إبراهيم السنوسي نصر، **مقدمة للإنترنت البرنامج التمهيدي للتدريب على استخدام الحاسوب والانترنت**، جامعة سبها مكتب التدريب 2015، ص 20

8 نسيم دردور، **جرائم المعلوماتية على ضوء القانون الجزائري والمقارن**، مذكرة لنيل شهادة الماجستير في القانون العام، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة منتوري، قسنطينة، 2013، ص 45.

البرنامج الرئيسي، فهو لا يزال الفيروس نشطا في الذاكرة في انتظار فرصة للعثور على ملفات الأخرى وتصيبها حتى بعد الرئيسية تم إنهاء البرنامج (المضيف)[1]. وانطلاقا مما تقدم نلاحظ بان فيروس الحاسوب أو ما يسمى البرامج الخبيثة هي تقوم بتخريب النظام المعلوماتي، والتي صنعت عمدا بغرض تغير الملفات التي تصيبها الفيروس بتنفيذ الأوامر إما بالإزالة أو التخريب أو التعديل، وما شبهها من العمليات، والتي تهدف إلى إلحاق الضرر بها أو السيطرة عليها. فهي تتكاثر بتوليد نفسها نسخ شفرتها المصدرية وإعادة توليدها بحيث لها القدرة على التخفي والخداع عن طريق الارتباط ببرامج أخرى، كما أن الفيروس يتميز بسرعة الانتشار، فلها قدرة تدمير تظهر عندما يجد الفيروس المفجر الذي يبعثه على العمل.

الفرع الثاني: مراحل إرتكاب جريمة السرقة الرقمية.

إن جريمة السرقة الالكترونية تتم وفق مراحل وخطوات التي يقوم بها المجرم من اجل الوصول الى هدفه وهي نفسها الخطوات التي يتبعها القراصنة بوجه عام لدخول الى نظام الحاسب الالي وتتكون من ثلاث مراحل:

أولا: مرحلة الاستطلاع وجمع المراجع.

يقصد بمرحلة الاستطلاع جمع المعلومات عن المنظمة الهدف أو بالتحديد شبكة المنظمة، سواء كان هذه المنظمة بنك أو شركة ... الخ [2]،فقبل أن يقوم الجاني باختراق نظام المعلومات في منظمة أو مؤسسة ما فانه يقوم أولا: بالتحضير والإعداد لهذا الاختراق من خلال جمع المعلومات الممكنة والمتوافرة عن شبكة المنظمة التي يريد اختراقها ويمكن تشبيه هذه المرحلة التحضير للسطو على بنك معين [3] **ولقد أدرج المشرع نص المادة 394 مكرر2 في الفقرة الأولى التي يعاقب فيها على كل شخص يقوم عمدا وعن طريق الغش تصميم أو بحث أو تجميع أو توفير لو نشر لو الاتجار في المعطيات المخزنة أو المعالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم).**

بواسطة استعمال منهج جمع المعلومات يمكن للمتسلل تنفيذ هجمات محتملة مثل اقتحام الشركة، قاعدة البيانات، اختراق موقعها على شبكة الانترنت، ويمكن للقراصنة جمع المعلومات قبل القيام في الواقع هجوم كالحصول على معلومات اسم المجال معلومات أساسية حول موقع الويب الهدف (اسم المجال)، مثل خوادم الأسماء المرتبطة، تفاصيل الاتصال المرتبطة به كالبريد الالكتروني، الهاتف. [4]

---

[1] محمد سعد، **عالم القرصنة**، حقوق الطبع والنشر, 2020، ص 75

[2] احمد محمد عبد الرؤوف المينيفي، **فيروسات الحاسب الآلي**، مرجع سابق، ص 37.

[3] احمد محمد عبد الرؤوف المنيفي، **فيروسات الحاسب الآلي**، المرجع نفسه، ص 37.

[4] محمد سعد، مرجع سابق، ص 34.

من خلال ما سبق نستنتج بان مرحلة الاستطلاع هي مرحلة بدائية، نشير في هذا الصدد بان مرحلة الاستطلاع تلعب دورا كبيرا في جمع بعض المعلومات والبيانات عن شركة أو بنك أو مؤسسة ما، بحيث نجد أن المشرع يعاقب على كل من يقوم بتجميع البيانات والمعطيات أو البحث فيها في المنظومة المعلوماتية، كما أن الجاني (السارق) يقوم أولا بجمع المعلومات المنظمة التي يريد سرقتها، ويمكن القول بأنه يقوم باستكشاف كل ما يخص الأموال أو المعلومات المتواجدة في الكمبيوتر أو ما يخص الحراسة وغيرها. وكل هذا يقوم به الجاني قبل قيام باختراق المنظومة المعلوماتية.

وتجدر بنا الإشارة أن المشرع الجزائري انه تطرق في قانون العقوبات إلى بعض المواد التي تنص فيما يخص المساس بأنظمة المعالجة الآلية للمعطيات ومن خلال الخطوات التي يتبعها الجاني، يعتبر عمل خطير بحيث يقوم بالتحضير لاختراق للسطو من خلال جمع المعلومات.

المادة 394 مكرر 5 قانون العقوبات بأنه إذا كان هذا التحضير مجسدا بفعل أو عدة أفعال مادية فيعاقب بعقوبات المقررة للجريمة ذاتها المشرع الجزائري أكد على تجريم الاشتراك سواء كان شخص طبيعي أو كان شخص معنوي في مجموعة أو اتفاق بغرض الإعداد الجريمة من الجرائم الماسة بالأنظمة المعلوماتية.[1]

ويتم جمع المعلومات في هذه المرحلة بواسطة بعض أدوات القرصنة المخصصة للبحث، بحيث يتم ذلك بجمع المعلومات بشكل عام إلى التطبيقات، وإلى المواقع ويب، وعمل كل هذه الأدوات هو القيام بعمليات بحث مفتوحة في مصادر عامة على شبكة الانترنت مثل الإخبار المقالات، وشركات التسجيل وخوادم أسماء النطاقات ... الخ.[2]

وبما أن هذه المرحلة هي بدائية التي تتمثل الشروع في جمع المعلومات والبيانات، نجد المشرع لم يغفل عليها حيث نص **على المادة 394 مكرر 7 يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها.** يتضح من خلال هذه المادة بان المشرع يعاقب على الشروع في الجرائم المعلوماتية، إذن جريمة السرقة الالكترونية يعاقب فيها في مرحلة الشروع.

ثانيا:مرحلة المسح.

تهدف مرحلة المسح إلى التعرف على الحواسيب المتصلة التي تعمل على الشبكة والخدمات التطبيقات والبرامج التي تشغلها هذه الحواسب. والتي تعد منافذ يمكن الدخول من خلالها إلى النظام وهذه المرحلة ضرورية لان الجاني مهما جمع من المعلومات فانه لا يستطيع الوصول إلى حاسب

---

[1] يوسف صغير، **الجريمة المرتكبة عبر الانترنت**، مذكرة لنيل شهادة الماجيستر في القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة مولود معمري، تيزي وزوو، ص 111.

[2] احمد محمد عبد الرؤوف المنيفي، **فيروسات الحاسب الآلي**، مرجع سابق، ص 38.

إلى بعيد واختراقه إلا إذا كان الحاسب متصلا بالإنترنت، أو شبكة المؤسسة أو الشركة التي ينتمي إليها.

ويتم التعرف على الأنظمة المتصلة والقابلة للوصول عبر الانترنت من خلال إرسال إشارة اتصال عنوان. إلى للحاسب الهدف، وفي حالة إذا استجاب الحاسب الهدف لهذه الرسالة فإننا نعرف أن هذا الحاسب متصل وفعال.[1]

ويعتبر برنامج الماسح هو برنامج احتمالات بحيث يقوم فكرة تغير التركيب أو تبديل احتمالات المعلومة، وعندما تستخدم قائمة الاحتمالات لتغير رقم الهاتف، يقوم بمسح قائمة أرقام كبيرة للوصول إلى أحدهما الذي يستخدم موزع للاتصال بالإنترنت، أو إجراء لاحتمالات عديدة لكلمة السر من اجل الوصول إلى الكلمة الصحيحة التي تمكن المخترق من الدخول للنظام ومن جديد، بحيث يعتبر هذا الأسلوب تقني يعتمد واسطة تقنية هي برنامج الماسح بدلا من اعتماد على التخمين البشري. [2]

وفيما يخص مسح المنافذ فيقوم أولا بإتمام التحقيق بان الحاسب الآلي الهدف متصل بالإنترنت، وعليه يقوم الجاني بعملية مسح المنافذ من اجل التعرف على الخدمات أو البرامج العاملة في الحاسب الآلي. [3]

المسح يعتبر الخطوة الثانية في الاستخبارات عملية جمع المتسللين حيث معلومات حول عناوين IP محددة. ويمكن الحصول على بنيتها والخدمات التي تعمل على أجهزة الكمبيوتر مختلف البصمة التي تجمع المعلومات بشكل سلبي من مصادرة خارجية مختلفة ينطوي المسح الضوئي على المشاركة لنشاطه مع الهدف للحصول على المعلومات، وأما يتعلق الأمر بإتلاف البرامج والمعلومات بمعناها الفكري أي المحتوى المسجل على دعامة ما أيا كان نوعها ماديا أو الكترونيا، بحيث يتخذ صورتين:

الصورة الأولى والتي يتم فيها محو المعلومات كليا وتدميرها الكترونيا، وأما الصورة الثانية فهي أن يتم فيها تشويه المعلومة أو البرنامج على نحو فيه إتلاف بحيث يجعلها غير صالحة للاستعمال[4] ،وعلى سبيل المثال قيام المجرم الالكتروني بتغيير أو تزوير البيانات مثل التسلل الالكتروني إلى البيانات المتعلقة بفاتورة الهاتف قبل طبعها في شكلها النهائي بحيث يتمكن من حذف بعض

---

[1] احمد محمد عبد الرؤوف المنيفي، **فيروسات الحاسب الآلي**، المرجع السابق، ص 51.

[2] رابحي عزيزة، **الاسرار المعلوماتية وحمايتها الجزائية**، أطروحة لنيل شهادة الدكتورة قانون خاص، كليه الحقوق والعلوم السياسية، قسم الحقوق، جامعة ابوبكر بلقايد، تلمسان,2018، ص 115 و116.

[3] احمد محمد عبد الرؤوف المنيفي، **فيروسات الحاسب الآلي**، مرجع سابق، من 54.

[4] محمد نصير محمد، **مشكلات الحماية الجنائية لبرامج الحاسب الآلي (دراسة مقارنة)**، مجلة قضائية، المجلد 5، العدد الثامن، محرم 1425ه، ص227.

المكالمات من الفاتورة قبل طبعتها وإرسالها، ومثل قيام أحد الطلاب بتغيير درجاته المسجلة على الكمبيوتر في مادة معينة أو تغيير معدلة الفصلي أو العام.[1]

ويتضح مما تقدم تعتبر مرحلة المسح مرحلة ضرورية للجاني، لا بد أن يكون الحاسوب متصلا بالإنترنت أو الشركة التي ينتمي إليها أو شبكة مؤسسة بهدف مسح المعطيات من منظومة يؤدي ذلك تلقائيا إلى إضرار معالجة الآلية للمعطيات. **كما أن المشرع الجزائري نص في المادة 394 مكرر 1 من قانون العقوبات بأنها تعاقب كل من يدخل بطريق الغش معطيات في نظام معالجة الآلية. أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها.** بحيث نلاحظ في هذه المادة بأن المشرع ذكر كلمة "أزال" والتي تعنى إتلاف البرامج والتطبيقات الموجودة في الكمبيوتر وتدميرها، وعليه أقر المشرع بتضاعف العقوبة إذا ترتب ذلك الحذف أو تغير المعطيات المنظومة أو تخريب في المادة 394 مكرر»

ثالثا: مرحلة الدخول.

تقع هذه الجريمة من طرف أي شخص، ويكون عادة من بين أولئك الذين لهم حق الدخول إلى النظام، وهذه الجريمة تقع متى كان الدخول مخالفا لإرادة صاحب النظام أو من له الحق السيطرة عليه كالأنظمة المتعلقة بأمن الدولة أو أنظمة تتعلق بالحياة الخاصة التي لا يجوز الاطلاع عليها. يقصد بتدمير المواقع الدخول غير المشروع على نقطة ارتباط أساسية أو فرعية متصلة بالإنترنت من خلال نظام ألي أو مجموعة نظم مرتبطة شبكيا بهدف تخريب نقطة أو النظام). [2]

فللولوج أو الدخول إلى النظام المعلوماتي يكفي معرفة الطريقة الواجب إتباعها، مما يفسح المجال للمتدخل الحصول على كل ما يريد من معلومات مخزونة في هذا النظام، وأكثر من ذلك فان عملية الدخول تسمح له بالوصول إلى شبكات أخرى تكون مرتبطة، ويضم الولوج غير المصرح به الاختراق الذي يحدث للنظام بأكمله أو جزء منه [3]

إن الدخول إلى النظام الضحية يتم إما عن طريق كسر كلمة المرور في إحدى خدمات الاتصال عن بعيد، أو عن طريق استغلال ثغرة أو منظمة ضعف برمجية في جدار النظام الهدف الطريقة الأولى لا صعوبة فيها ويمكن تشبيهها بكسر الأبواب والنوافذ وأما فيما يخص الطريقة الثانية الخاصة باستغلال الثغرات البرمجية فهي أصعب في التحديد، لأنها أحيانا تبدوا كأنها منطقة ضعيفة في جدار النظام يقوم الجاني بخرقها والدخول منها، واختيار هذا التكيف أو ذاك يترتب عليه بلا شك أثار خطيرة بالاعتبار الشرعي بشأن توافر شرط هتك الحرز. [4]

---

[1] فاطمة الزهراء خبازي، **جرائم الدفع الالكتروني وسبل مكافحتها**، أعمال الملتقى الوطني اليات مكافحة الجرائم الالكترونية في التشريع الجزائري الجزائر 29 مارس 2017 جامعة الجيلالي بونعامة، خميس مليانة، ص 33.

[2] عبد الرحمن عبد الله السند **الأحكام الفقهية للتعاملات الالكترونية الحاسب الآلي وشبكة المعلومات الانترنت**، دار الورق، الطبعة الأولى 1424هـ، 2004، ص 283

[3] رابحي عزيزة، مرجع سابق، ص 157.

[4] احمد محمد عبد الرؤوف المنيفي، **فيروسات الحاسب الآلي**، مرجع سابق، ص 61.

من خلال ما تقدم نستنتج بأنه تتم هذه المرحلة الدخول إلى الحاسب الآلي باستعمال طريقتين، الطريقة الأولى المتمثلة في كسر كلمة المرور فهذه الطريقة ليست صعبة بالنسبة للجاني. وأما الطريقة الثانية والمتمثلة في استغلال الثغرات البرمجية وهذه الطريقة أصعب. ولكن إتباع الطريقة الأولى أو الطريقة الثانية فهي طبعا تؤدي إلى آثار خطيرة. والملاحظ على النصوص في قانون العقوبات أن المشرع أدرج بتجريم وعقاب في نص المادة 394 مكرر كل شخص يدخل أو يبقى عن طريق الغش يعاقب على ذلك.

فالدخول هو الولوج إلى نظام معالجة للمعطيات بطريقة الغش. يعاقب الجاني من اجل الوقاية من السرقة الالكترونية. تقوم الجريمة بمجرد القيام بالدخول الغير المصرح به إلى المنظومة المعلوماتية عن طريق الغش أو البقاء فيها في كل أو جزء منها أو من يحاول ذلك. يعتبر الدخول الغير المصرح به جريمة، بحيث تقوم الجريمة بمجرد ما يتم الدخول غير المرخص به وعن طريق الغش إلى المنظومة. [1]

وكما نصت المادة 2 من الاتفاقية الدولية للإجرام المعلوماتي الصورة البسيطة للجريمة تتمثل في مجرد الدخول أو البقاء غير المشروع بينما الصورة الشديدة، تتحقق بتوافر الظرف المشدد لها، ويكون في حالة التي ينتج فيها عن الدخول أو البقاء غير المشروع إما محو أو تغيير في المعطيات الموجودة في النظام أو التخريب نظام أشغال المنظومة.[2]

وأما المساس بسلامة البرمجية للمؤلف فوحده له الحق في تعديل أو تغير أو تحويل أو حذف أو إضافة في برنامجه، ولا يمكن اعتراض الغير على ذلك، فمؤلف البرنامج له الحق التعديل دون التغيير، في نوع المصنف وإدخال ما يراه ملائما إثناء عملية صنع الدعامة وفقا للمادة 89 الأمر (03-05)[3]، نلاحظ بان المشرع أعط الحق للمؤلف بقيام تعديل أو إدخال طبقا لما نص في المادة 89 من قانون (03-05)[4].

[1] صغير يوسف، مرجع سابق، ص 108.
[2] بدري فيصل، **مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي**، أطروحة لنيل شهادة الدكتوراه في قانون عام، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة الجزائر1، بن يوسف بن خدة، الجزائر ، 2018، ص 161.
[3] بدري فيصل، المرجع نفسه، ص 144.
[4] الأمر رقم 03-05 مؤرخ في 19 جمادي الأولى عام 1412 الموافق 19 يوليو سنة 2003 متعلق بحقوق المؤلف والحقوق المجاورة،

خلاصـــــة

نخلص في نهاية هذا الفصل المتعلق بالاطار الموضوعي لجريمة السرقة الرقمية اين تطرقنا الى مختلف الآراء الفقهية فيما يخص تعريف هذه الجريمة حيث انتهينا بأنها نوع من انواع الجرائم المعلوماتية التي يرتكبها الجاني عن بعد بواسطة جهاز الكمبيوتر، داخل الأنظمة المعلوماتية كما وانها تنطوي بوجه عام على ذات الخصائص التي تتمتع بها تلك الجرائم السابقة الذكر وكذا تبيان تمييز هذه السرقة الرقمية عن مفهوم السرقة التقليدية بأن الاولى تقع على البيانات الرقمية ذات القيمة المالية وهذا ما جعل منها جريمة ذات طابع خاص وعليه فهي تعتبر من الجرائم المستحدثة سريعة التطور ونظرا لأهمية العامل الشخصي في هذه الجريمة المتمثل ،في الجاني مرتكب الجرم فقد تم تناوله بالتفصيل من خلال شرح كافه المجرمين الالكترونيين وابراز الدوافع الرئيسية التي تدفع به الى ارتكاب هذه الجريمة الخطيرة.

إضافة الى كل ذلك فقد تم التركيز على مختلف تطبيقات والاساليب والتقنيات التي يستخدمها الجنات للولوج الى الأنظمة المعلوماتية وتحقيق جريمة سرقه الرقمية فيها.

وأخيرا تم تسليط الضوء على المراحل التي تمر بها هذه الجريمة ومن ثم ننتقل الى تفاصيل الفصل الثاني من بحثنا والذي كان بعنوان التنظيم القانوني لجريمة السرقة الرقمية والذي سنتناول من خلاله كافة الأثار القانونية المترتبة على جريمة السرقة الرقمية.

الفصل الثانـي:

التنظيم القانونـي لجريمة السرقة الرقمية.

تمهيـــد:

نظرا لطبيعة جريمة السرقة الرقمية الخاصة، وكونها جريمة مستحدثة ذات صبغه تقنية تمس بالحقوق المالية للأفراد، حيث تشكل خطرا وضررا على المجتمع كان لابد من مكافحتها وايجاد سبل الوقاية منها وامام الموقف غير الصريح والمبهم للمشرع الجزائري بخصوصها نجد أنه أصبح ملزما للوقوف امام السلوكيات الإجرامية لمرتكبي هذه الجريمة لتقيمها وادراجها ضمن دائرة التجريم من اجل مكافحتها والوقاية منها. وذلك بتحديد اركانها وتقرير عقوبات رادعة لها ، وكذا دراسة مدى امكانية تطبيق النصوص الموضوعية لجريمة السرقة التقليدية عليها ،اضافة الى بيان خصوصية اجراءات الاثبات و طرق التحري الخاصة بها، وصولا الى كيفية مكافحتها على الصعيدين الوطني والدولي من خلال استحداث هياكل مهمتها الاساسية البحث في هذه الجريمة و المنع و الوقاية منها ،وعليه ادرجنا هذا الفصل تحت عنوان التنظيم القانوني لجريمة السرقة الرقمية حيث فيه حاولنا الإلمام بكل ما سبق ذكر اعلاه ،من خلال تقسيمه الى مبحثين الاول بعنوان التكييف القانوني لجريمة السرقة الرقمية ،و الثاني المواجهة القانونية لجريمة السرقة الرقمية .

المبحث الأول: التكييف القانوني لجريمة السرقة الرقمية

قمنا بتقسـيم هذا المبحث الى مطلبين بحيث نتطرق بالتفصـيل في المطلب الاول الى اركان جريمة السـرقة الرقمية بداية من حيث اركانها العامة والمتمثلة في الركن المادي والركن المعنوي نهاية بالركن المفترض لها وهو محل جريمة السرقة الرقمية الذي يضفي عليها طابع الخصوصية اما فيما يخص المطلب الثاني فتناولنا فيه موقف الأنظمة القانونية المقارنة وصـولا الى موقف المشرع الجزائري من هذه الجريمة واهم العقوبات التي قررها لها في ظل القوانين الخاصة.

المطلب الاول: أركان جريمة السرقة الرقمية

من الثابت ان أركان الجريمة تنقسم الى أركان عامة، واخرى خاصـه او مفترضـة، وان الاولى ما توجد في كل جريمة مهما كان نوعها، والثانية هي ما يشـترط توافره في كل جريمة موصـوفه تضـاف الى اركانها العامة لإعطائها اسـما قانونيا يميزها عن غيرها من الجرائم، وقد اختلف الفقهاء في تعريف أركان الجريمة العامة الى مذاهب ونحن نتفق مع من قال إن الجريمة لها ركنان، ومن هنا يتبين لنا أن جريمة السـرقة الرقمية هي من الجرائم التي تتطلب الركن المادي والركن المعنوي إضافة الى محل الجريمة الذي يمنحها طابع الخصوصية.

الفرع الاول: الاركان العامة لجريمة السرقة الرقمية.

نتناول في هذا الفرع الاركان العامة لجريمة السـرقة الرقمية والمتمثلة في الركن المادي وكذا الركن المعنوي محاولين بذلك شرحها بإقتضاب.

اولا: الركن المادي لجريمة السرقة الرقمية.

1-مضمون الركن المادي لجريمة السرقة الرقمية.

الركن المادي هو ما يدخل في كيان الجريمة وله طبيعة مادية وهو الوجه الظاهر للجريمة وبه يتحقق الاعتداء على المصـلحة المحمية فلابد من فعل او امتناع يمكن اثباته والركن المادي هنا يختلف من حال لأخر حسـب التصـنيف الذي يقع على الفعل وعليه لا يمكن حصـر الجريمة المعلوماتية تحت تكييف واحد فقد تشـكل الواقعة المرتكبة والتي تحمل وصـفا الجريمة المعلوماتية شـكل مطابق لما نص عليه قانون العقوبات ولقد اتخذت اشـكال لا يمكن ان تطبق عليها النصوص التقليدية وهو ما دعي للتدخل التشريعي[1].

تتمثل عناصر الركن المادي في السلوك المجرم والنتيجة لعلاقه الشبيهة حيث يعد السلوك المجرم في هذا الصنف من الجرائم هو السرقة السلوك يوجد بصورتين فقط يكون بفعل ايجابي اذ يفترض في هذه الصورة قيام الجانب بفعل ارادي بغيه احداث نتيجة معينه كما يمكن ان يكون

[1] بوضياف اسمهان، مرجع سابق، ص 353 -354

بفعل سلبي يأخذ وصف الامتناع عن اتيان الامر يوجبه المشرع وفي وقت الجريمة الإلكترونية يمكن ان نجده بنوعين الايجابي والسلبي.

والنتيجة يقصد بها التغيير الذي يحدث في العالم الخارجي كأثر للفعل الجرمي والنتيجة لا تعتبر من العناصر الأساسية في كل جريمة انما هي لازمة في بعض الجرائم دون اخرى تصنف جريمة السرقة على انها من جرائم الاعتداء على الاموال والعلة من وراء تجريم السرقة على انها من جرائم الاعتداء على ملكيه هذا المال والملكية هي أحد الحقوق التي أولاها المشرع [1]

2_السلوك الإجرامي لجريمة السرقة الرقمية.

هو فعل الاختلاس ويعرف على انه:" **نقل الشيء او نزعه من المجني عليه بغير علمه أو بغير رضاه وادخاله الى حيازة الجاني**"، ويعرف الاختلاس ايضا بانه: "**سيطرة "الجاني على الشيء المسروق وظهور والظهور عليه بمظهر مالك**"[2]،ويقوم الاختلاس على عنصرين: عنصر مادي ويتمثل في الاستيلاء على الحيازة، وعنصر معنوي وهو عدم رضا مالك الشيء او حائزه عن الفعل، ويقتضي الاختلاس ان يقوم الجاني بحركة ماديه يتم بها نقل الشيء الى حيازته مهما كانت الطريقة ،سواء النزع او السلب او الخطف او النقل او اي طريقه اخرى ، وكل ما يشترط هو ان يقع الاستيلاء على الشيء بفعل الجاني وذلك ليس من الضروري ان يكون بيده فيعد السارق الشخص الذي يدرب الكلب على السرقة او الذي يستعمل الة الارتكاب السرقة، ويترتب على تحديد الاختلاس نتيجتان هما : لا يتحقق الاختلاس اذا كان الشيء موجودا اصلا في حوزة المتصرف فاذا كان الشيء في حوزة الجاني من قبل وامتنع عن رده الى مالكه الاصلي او حائزه او تصرف فيه تصرفا ضارا فلا يعتبر سارقا لأنه لا ينقل الشيء برفضه او بتصرفه انما يستبقيه والاستبقاء لا يحقق الاختلاس الذي يتحقق بالنقل فقط [3].

ايضا لا يعتبر مختلسا البائع الذي يحبس المبيع بين يديه بعد ان يستلم ثمنه وكذلك من يعثر على شيء ملك للغير فيأخذه دون سوء نية ثم يمسك يمسكه بنيه التملك، بالنسبة للنشاط الاجرامي المكون لجريمه السرقة وهو الاختلاس وبتطبيقه على البرامج الحاسب الالي او المعلومات المعالجة بصفه عامه نلاحظ ان الجاني وان كان يدخل ذمته ما استولى عليه من البرامج الا انه في نفس الوقت لم يخرج هذه البرامج من تحت السيطرة هذا الاخير دون انتقاص من محتواها.[4]

---

[1] اسامة أحمد المنارة، جلال محمد الزغبي، **جرائم تقنية نظام المعلومات الالكترونية**، الطبعة الثالثة، دار الثقافة النشر والتوزيع، عمان، 2014، ص 53.

[2] محمد نجيب حسني، **شرح قانون العقوبات**، القسم الخاص، ط 6، دار النهضة العربية القاهرة، د.س.ن.، ص 838.

[3] أحسن بوسقيعة، **الوجيز في القانون الجزائي الخاص**، الجزء الاول، الطبعة الثالثة، دار هومة للطباعة والنشر، الجزائر، 2005، ص 248.

[4] رحال بومدين، سعداني نورة، **الحماية الجنائية الواقعة على اموال التجارة الالكترونية**، **جريمة السرقة والنصب**، مجلة الواحات للبحوث والدراسات، المجلد 9، العدد 2، 2016، ص 99.

ما يثير الاشكال في هذه المسألة هو الكيان المعنوي للمال المعلوماتي الذي انقسم الفقه حول مدى انطباق فعل الاختلاس عليه كالتالي:

-الراي الرافض لكون فعل الاختلاس يقع على المعلومات: ذهب هذا الجانب من الفقه الى القول بعدم امكانيه وقوع فعل الاختلاس على المعلومات واعتراضهم تمحور حول مدى انطباق صفه المنقول على المعلومات والمعروف ان المنقول كل مال يمكن تغيير موضعه ونقله من مكان الى اخر لكن لا تخرج من مكان التي تكون فيه فالأصل لم ينقل ولم ينقص منه شيئا وما تزال المعلومات على الرغم من حصول الجاني عليها بين يدي مالكها وتحت سيطرته.

-الرأي المؤيد لكون فعل الاختلاس يقع على المعلومات: يرى هذا الجانب من الفقه ان المبادئ العامة لعناصر الركن المادي للسرقة المتمثل في السلوك الاجرامي والنتيجة الاجرامية والعلاقة السببية تتحقق في اختلاس المال المعلومات اثر قيام الجاني بتشغيل الحاسب الألي والحصول على البيانات والمعلومات او حيازتها وهو ليس في حاجه الى استعمال العنف لكي ينقل المعلومات ومن الممكن تطبيق نصوص الجريمة السرقة العادية على سرقه الشيء الالكتروني او التلاعب به حيث ان اختلاس الشيء المتمثل في البيانات والمعلومات يتحقق بالنشاط المادي الذي يصدر عن الجاني ذلك بتشغيل الحاسوب للحصول على المعلومة التي يرغب بها او التلاعب بها للحصول على مردود مادي فيحقق النتيجة بحصوله عليها.[1]

ثانيا: الركن المعنوي في جريمة السرقة الرقمية .

يقصد بالركن المعنوي في اي جريمة بالقصد الجنائي واغلب التشريعات الجنائية بما فيها التشريع الجزائري، لم تضع تعريفا للقصد الجنائي، ولذلك فانه لمعرفة الجرائم العمدية نرجع الى النصوص الجنائية التي تعرف الجرائم المختلفة وتبين عناصرها ومن ضمنها الركن والمعنوي،[2]بالرجوع الى نص المادة 350 من قانون العقوبات الجزائري نجد ان المشرع اشترط توافر القصد الجنائي في جريمة السرقة. [3]

1-القصد العام: لقيام جريمة السرقة يجب ان يعلم الجاني بأن البرامج والبيانات مملوكه للغير ، واذا تحصل على المعلومات والبيانات بدون قصد اي "خطاء "بالبرامج، فلا يكون مرتكبا لجريمة السرقة لانتفاء عنصر العلم[4] ، ان المجرم المعلوماتي مرتكب لجريمه سرقه المعلومات، يسعى بإرادته الى الاستحواذ عليها بتشغيله ويعلم انها مملوكه للغير في قيامه باختلاسها او بنسخها ويعتبر قد توفر لديه عنصر القصد العام [5]، بالإضافة الى العلم يجب ان تتجه إرادة السارق الى

[1] رحال بومدين، سعداني نورة، المرجع نفسه، ص 97.
[2] محمود مصطفى، **شرح قانون العقوبات**، قسم الخاص، ط 8، دار جامعة القاهرة، 1994، ص 471.
[3] أحسن بوسقيعة، مرجع سابق، ص 276.
[4] دحمان صبايحية خديجة، مرجع سابق، ص56.
[5] رابحي عزيزة، مرجع سابق، ص 197.

اخراج الشيء محل السرقة من حيازة المجني عليه وادخاله في حيازته وتكون ارادته حرة بحيث اذا اكرهه شخص اخر لاستخراج المال من حيازة صاحبه تخلفت لديه اراده ارتكاب الاستيلاء وامتنع قيام السرقة ،[1] وعليه القصد العام يقتضي توافر العلم والإرادة وسنبين مدى توافر كل منهما في جريمة السرقة الرقمية.

1.1-العلم: يقصد بالعلم توفر اليقين لدى الجاني بأن الفعل الذي ارتكبته يؤدي الى إحداث نتيجة جرمية يعاقب عليها القانون وعليه كذلك بجميع العناصر القانونية للجريمة[2].

ومحل العلم بشكل العلم بالقانون والعلم بالوقائع، فمن المبادئ الاساسية أن يكون الجاني على دراية بالقانون الذي يعاقب على كل الجرائم مهما كان نوعها، وان يكون عالما بكل الوقائع [3]

2.1-الارادة: هي قوة نفسية او نشاط نفسي يوجب كل أعضاء الجسم أو هو نشاط نفسي يصدر عن وعي وأدراك يهدف الى بلوغ هدف معين.

محل الارادة في الجرائم العمدية هو ارادة السلوك من جهة والنتيجة من جهة اخرى، اتجاه الارادة الى السلوك يفترض علم الجاني بماهية سلوكه وخطورته على الحق الذي يحميه القانون ثم دفعه اعضاء جسمه الى اتبان الحركة التي يطلبها ذلك السلوك. [4]

2-القصد الخاص: القصد الخاص الى جانب عنصر القصد العام والذي يتمثل في العلم والإرادة يضاف عنصر القصد الخاص والذي يتمثل في نية الاستحواذ على الشيء.

يجب لقيام جريمة السرقة ان تتجه لدى الجاني نيته الى تملك الشيء المختلس فاذا لم تتجه نيته الى تملكه فلا تقوم الجريمة في هذه الحالة، وعندما ينتهك الجاني النظام المعلوماتي الخاص، الذي له كلمه السر والنظام الأمني خاص يدل على وجود قصد وسوء النية من مرتكب الفعل، ويتوفر فيها القصد العام والخاص ويظهر القصد الخاص في فتره البقاء غير المشروع الا ان المشكلة التي تعترض ذلك هي كيفية اثبات سوء النية[5].

الفرع الثاني: الركن المفترض لجريمة السرقة الرقمية.

لقد بينا سابقا الاركان العامة لجريمة السرقة الرقمية، بينما نبرز في هذا الفرع الركن المفترض لها وهو محل السرقة الرقمية ونحاول بيان مدى انطباقه على وصف المال مهما كانت صفته محل جريمة السرقة المالية المعلوماتية يجب بداية توضيح مفهوم الشيء أو المال المعلوماتي و الذي يقصد به هنا الحاسب الآلي أو الكمبيوتر بكل مكوناته المادية والمعنوية ، فالجزء المادي فيه يتكون

---

[1] سالم محمد بن سلام بني مصطفى، مرجع سابق، ص46.
[2] ابراهيم بلعيات، **أركان الجريمة وطرق اثباتها في القانون الجزائري**، د.ط، دار الخلدونية للنشر والتوزيع، الجزائر، ص 121.
[3] غازي حنون خاف الدراجي، **استظهار القصد الجنائي في جريمة القتل العمد**، ط1، منشورات الحلبي الحقوقية، لبنان ،2012، ص 24.
[4] غازي حنون خاف الدراجي، المرجع نفسه، ص 33.
[5] دحمان صبايحية خديجة، مرجع سابق، ص56.

من جهاز الإدخال والإخراج و وحدات التشغيل المركزية[1]، أما الجزء المعنوي فيشمل البرامج بالإضافة إلى المعلومات المطلوب معالجتها أو التي تمت معالجتها بالفعل، مع الأخذ بعين الاعتبار المعطيات أو المعلومات منذ دخولها ومعالجتها إلكترونيا وتخزينها واسترجاعها لا تنفصل عن البرامج التي تنظمها ، و لذلك فإنها لا تختلف في الطبيعة و في كونها شيئا معنويا و تكون لها نفس الحماية المقررة للبرامج . من خلال تعريف المال المعلوماتي فإن الجزء الخاص بالكيان المادي للكمبيوتر لا يثير أي مشكلة باعتباره مال منقول كشاشة الكمبيوتر وجهاز المعالج والطابعات وغيرها، لكن الإشكال يثور حول مدى قابلية المعلومات لتكون محلا للاختلاس حيث اختلف الفقهاء في ذلك تبعا لطبيعة المعلومات، فهناك المعلومات المعالجة آليا والمخزنة بالنظام المعلوماتي والمعلومات المخزنة على الدعامة.

أولا–المعلومات المعالجة آليا.

اختلف الفقه حول مدى صلاحية المعلومات المعالجة آليا كمحل لفعل الاختلاس فنتج عن ذلك اتجاهين[2]:

1_ ذهب الاتجاه الأول إلى التفريق بين عدة حالات في سرقة البرامج والمعلومات فإذا وقعت السرقة على CD أو ديسك مسجل عليه معلومات أو برامج يشكل هذا الفعل جريمة السرقة وتخضع لأحكام قانون العقوبات، أما إذا وقعت السرقة على برامج في ديسك أو CD وذلك عن طريق نسخه فهذا الفعل يشكل تقليد للمصنف أو نقله لدى الجاني بنية التملك دون رضى المجني عليه.

تعرضت هذه النظرية إلى العديد من الانتقادات من بينها أن الجاني لا يحتاج للقيام بأي حركة مادية مما يصعب إثبات الجريمة وأنها ضيقت إلى حد كبير من نطاق الاختلاس المعاقب عليه، فجاءت نظرية التسليم الاضطراري للحد من العيوب التي شابت هذه النظرية،مضمون نظرية التسليم الاضطراري لا ينفي الاختلاس إذا كانت تتطلب ضرورات المعاملات والأخذ والعطاء بين الأفراد وتطبيقا لهذه الفكرة فإن من يستلم شيئا من طرف البائع ويتظاهر بشرائه أو حتى بفحصه ويفر به دون أن يدفع ثمنه بعد سارقا لأن التسليم هنا هو تسليم اضطراري الذي اقتضته ضرورة التعامل بين الناس، ولقد وجهت لهذه النظرية العديد من الانتقادات أهمها أن التسليم الحاصل في الفرضيات السابقة ليس اضطراريا، وهذه الفكرة واسعة وغير محددة والأخذ بهذه الفكرة يؤدي إلى نتائج غير منطقية.[3]

2–يختلف أنصار الاتجاه الثاني مع الأول بحيث يرون أن المعلومات المخزنة داخل جهاز الكمبيوتر يشكل محل السرقة فإذا قام الشخص بالدخول إلى جهاز الحاسب الآلي واطلع على

---

[1] رجال بومدين ومحاني نورة، مرجع سابق، ص 10.

[2] عمر أبو الفتوح عبد العظيم الحمامي، **العمالية الجنائية للمعلومات المسجلة الكترونيا**، د ط، دار النهضة العربية، عمان، 2010، ص 560.

[3] عمر أبو الفتوح عبد العظيم الحمامي، المرجع نفسه، ص 549.

البرامج أو المعلومات الموجودة بداخله أو حتى لو قام بعملية النسخ لهذه البرامج أو المعلومات فهذا الفعل يشكل جريمة السرقة، لأنه يمثل الاعتداء على حق الملكية.

من بين أهم الأسانيد التي اعتمد عليها هذا الاتجاه أن البرامج أو المعلومات لها كيان مادي يمكن رؤيته مترجم على الشاشة ويمكن الاستحواذ على برامج ومعلومات عن طريق نسخها والقول بعدم قابليتها للاستحواذ يجردها من الحماية القانونية[1]. يتحقق اختلاس المعلومات بالنشاط المادي الصادر من الجاني سواء بتشغيله للجهاز للحصول على معلومات أو برامج أو الاستحواذ عليها، كما أنه ليس بحاجة إلى استعمال العنف لانتزاع الشيء، فبمجرد تشغيله للجهاز للقيام بعملية اختلاس المعلومات تتحقق النتيجة بحصوله عليها لأن الرابطة السببية متوفرة بين نشاطه المادي والنتيجة الإجرامية.

ثانيا-المعلومات المخزنة بالنظام المعلوماتي.

اختلف الفقهاء حول صلاحية نسخ ونقل المعلومات من النظام المعلوماتي لفعل الاختلاس فظهر اتجاهين هما:

1-الاتجاه الأول: أقر هذا الاتجاه عدم صلاحية نقل المعلومات ونسخها من النظام المعلوماتي محل الاختلاس حيث استندوا على مجموعة من الحجج أهمها أن المعلومات المخزنة بالنظام المعلوماتي ولو أنها لا تعتبر أشياء مادية فلا يمكن تصور انتزاع حيازتها، أي لا تكون محلا للسرقة إلا في حالة تفريغها وتثبيتها داخل إطار دعامة، والصعوبة التي تثار في عدم اعتبار نسخ ونقل صورة منها لا ينطبق عليها وصف سرقة. [2]

2-الاتجاه الثاني: يرى أصحاب هذا الاتجاه بصلاحية نقل ونسخ المعلومات من النظام المعلوماتي لأن تكون محل الاختلاس واستندوا إلى العديد من الحجج أهمها أنه فعل الاختلاس يقع على المعلوماتية وذلك راجع لوجود المعلومات حقيقية بكل فوائدها ومزاياها الاقتصادية التي تمثلها البيانات في الذمة المالية للمجني عليه بعد هذا الاختلاس ويتمثل في بيع المعلوماتية أو وضعها موضع التنفيذ. [3]

ثالثا-المعلومات المخزنة على الدعامة.

كذلك الأمر بالنسبة لصلاحية المعلومات المخزنة على الدعامة كمحل للاختلاس، فانقسم الفقهاء إلى اتجاهين فيرى الأول عدم صلاحية المعلومات المسجلة الكترونيا والمخزنة على دعامات وكذلك البرامج، حيث يرون أن الاختلاس يقع على سرقة الدعامات نفسها ومن الحجج التي استندوا

---

[1] حسين محمود الشيلي، مهد فايز الدويكات، **التزوير والاحتيال البطاقة الائتمان**، الطبعة الأولى، دار مجدلاوي للنشر والتوزيع، عمان، 2009، ص 46-45.

[2] عمر أبو الفتوح عبد العظيم الحمامي، مرجع سابق، من 567.

[3] عمر أبو الفتوح عبد العظيم الحمامي، المرجع نفسه، من 567.

عليها أن ما يترتب على سرقة المعلومات أضرار تفوق القيمة الحقيقية للدعامة ذاتها ويرجع ذلك إلى أن اختفاء المعلومات يعقبه إفشاء الأسرار والتي كانت المتوقع بقائها في نطاق السرية. ويتمثل سرقة الدعامة في ضياع عمل على قدر كبير من الأهمية.[1]

إذا كانت القواعد العامة لجريمة السرقة لا تدخل الأموال المعنوية ضمن الاعتداء في نصوص جريمة السرقة لما تتطلب تلك النصوص من كون المال يقع على كيان مادي، وعلى الرغم من ذلك إلا أنه أمكن حيازته داخل إطار معين للاستئثار به فإنه يقع تحت طائلة السرقة و إن كانت طبيعة المعلومات والبيانات المخزنة و المتبادلة عبر شبكة الانترنت مما يصعب حيازته ما لم تثبت على وسيلة لنقل أو نسخ المعلومات بحيث تصبح محلا للسرقة [2]لأن كيانها المادي يتمثل بالشريك الممغنط أو الملف الذي يحفظ تلك المعلومات ، و الذي يعد عندها اختلاس محتوى المعلومة ، تأسيسا على أن سرقة المعلومات والبيانات تختفي خلف سرقة الشريط الممغنط أو الملف و أن سرقة هذا الأخير دليل على سرقة الأول من معلومات و بيانات [3]

المطلب الثاني: موقف الانظمة القانونية من جريمة السرقة الرقمية.

سنتناول خلال هذا المطلب مواقف الأنظمة القانونية المتباينة من جريمة السرقة الرقمية حيث نشير في الفرع الاول منه الى موقف الأنظمة القانونية المقارنة من جريمة السرقة الرقمية بينما اختص الفرع الثاني منه بموقف المشرع الجزائري من هذه الجريمة.

الفرع الاول: موقف الانظمة القانونية المقارنة من جريمة السرقة الرقمية

نحاول من خلال هذا الفرع التعرف على مختلف مواقف الانظمة القانونية المقارنة من جريمة السرقة الرقمية على الصعيد الغربي والعربي.

أولا: موقف التشريع الفرنسي والانجليزي الموقف الصريح الذي أخذه كلا من الفقه والقضاء الفرنسي من جريمة السرقة المعلوماتية.

فان المشرع الفرنسي صمت ولم يتناولها صراحة بل اكتفى بالنص على جريمة السرقة التقليدية دون المعلوماتية ومنها الواقعة عبر الانترنت في المادة 311-1 من قانون العقوبات الفرنسي الجديد على أنها اختلاس الشيء المملوك للغير وفي المادة 311-2 إذ اعتبر أن اختلاس الطاقة أضرارا بالغير بعد سرقة.[4]فالتشريع الفرنسي نص قانون العقوبات الجديد على تجريم سرقة المال المعلوماتي متمثلا في المعلومات والبرامج، وذلك بموجب الفقرة الأولى من المادة 307، إذ تقرر

---

[1] عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، من 568.
[2] عمر أبو الفتوح عبد العظيم الحمامي، المرجع نفسه، من 569.
[3] عمر أبو الفتوح عبد العظيم الحمامي، المرجع نفسه، من 570.
[44] هروال هبة نبيلة، **جرائم الانترنت دراسة مقارنة**، أطروحة لنيل شهادة دكتورة في القانون العام، كلية الحقوق و العلوم السياسية، قسم الحقوق، جامعة ابي بكر بلقايد، تلمسان, 2014، ص 187.

المادة أن كل من النقط بطريق الاختلاس والتحايل برامج أو معلومات أو أي عنصر من عناصر نظام المعالجة الآلية للبيانات تعاقب بالحبس مدة ثلاث سنوات وبغرامة مقدارها مليون فرنك)[1]. وعلى الصعيد القانون الانجليزي لم يعترف بجريمة السرقة للمال المعلوماتي عبر الانترنت، لأنه لا يعتبر المعلومات من قبيل المال الذي تصلح حيازته للانتقال من صاحبه إلى السارق وهذا ما أقره الفقه والقضاء الانجليزي في الكثير من القضايا[2]

ثانيا: موقف التشريعات العربية.

بالنسبة للمشرع الليبي فنص على جريمة السرقة في المادة 444 من قانون العقوبات الليبي بأنه كل من اختلس منقولا مملوكا للغير يعاقب بالحبس وبعد من الأموال المنقولة في حكم قانون العقوبات الطاقة الكهربائية وجمع أنواع الطاقة ذات القيمة الاقتصادية[3] ولا يختلف الأمر كثيرا في التشريع المصري عن التشريع الأردني، فقد نص المشرع المصري في المادة 311 من قانون عقوباته على أن السرقة هي كل من اختلس منقولا مملوكا للغير وحتى تكون أمام الجريمة فلابد أن يكون الاعتداء واقعا على منقول له صفة المال بالإضافة إلى حيازة الغير له[4] فهي اكتفت بتطبيق قوانينها العقابية التقليدية الخاصة بجريمة السرقة[5] . كما صدرت تشريعات عربية تتعلق بتطبيق استخدام الحاسب الآلي وتجريم الاعتداء على المعلومات، وذلك من مشروع قانون مكافحة جرائم تقنية المعلومات الاتحادي في دولة الإمارات العربية المتحدة في المادة 10 من قانونها، كما نصت المادة 4 من قانون مكافحة جرائم المعلوماتية السعودي(**على انه يعاقب بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني** ريال، **أو بإحدى هاتين العقوبتين كل شخص يرتكب أي من الجرائم المعلوماتية الآتية: الاستيلاء لنفسه، أو لغيره على مال منقول أو على سند أو توقيع هذا السند ...)**[6] ومن خلال ما سبق نلاحظ بأن مواقف التشريعات هناك من استحدث نصوص التجريم جرائم التي ترتكب على الحاسب الآلي وهناك بعض التشريعات اكتفت بالقوانين التقليدية

الفرع الثاني: موقف النظام القانوني الجزائري من جريمة السرقة الرقمية

نحاول من خلال هذا الفرع التطرق الي موقف المشرع الجزائري من هذه الجريمة من خلال بيان مدى تطبيق النصوص الموضوعية لجريمة السرقة التقليدية على الجريمة السرقة الرقمية بالإضافة إلى تبيان العقوبات التي شرعها النظام القانوني الجزائري في إطار القوانين الخاصة.

---

[1] أنسام سمير طاهر، مرجع سابق، ص 146.
[2] هروال هبة نبيلة، مرجع سابق، ص 188.
[3] هروال هبة نبيلة، مرجع نفسه ، ص 189.
[4] عبد الله ماجد عبد المطلب العكايلة، **سرقة البيانات والمعلومات الإلكترونية**، دراسة مقارنة، كلية العلوم والإنسانيات، جامعة الأمير سطام بن عبد العزيز، ص 163.
[5] هروال هبة نبيلة، مرجع السابق، ص 189.
[6] انسام سمير طاهر، المرجع السابق، ص 147.

أولا: مدى تطبيق النصوص الموضوعية لجريمة السرقة التقليدية على جريمة السرقة الرقمية.

1-الرأي المؤيد: اختلف الفقهاء بخصوص فكرة السرقة المعلوماتية فالرأي المؤيد لفكرة السرقة المعلوماتية يرى أن الركن المادي للسرقة المعلوماتية وهو فعل الاختلاس يتكون من عنصرين هما: العنصر الموضوعي وهو النشاط أو السلوك الإرادي المؤيد إلى النتيجة مع وجود علاقة سببية بينهما، أما العنصر الآخر الشخصي هو نية الجاني تملك الشيء وحيازته حيث عند تشغيل الحاسب الآلي و الحصول على معلومات أو البيانات تكون قد اختلسها و استحوذ عليها بطريق غير مشروع،[1] وبذلك اللذان أبدت فيهما قرارها الصادر في 1989-1-12 الذي قضى بإدانة شخصين من أجل سرقة اقراص ممغنطة وسرقة محتواها خلال الفترة الضرورية لنقل المعلومات إلى سند آخر.[2]

2-الرأي المعارض: أما الرأي المعارض فقد رأى عدم وجود إمكانية وقوع جريمة السرقة المعلوماتية الارتباط فعل الاختلاس بالمحل المادي لاختلاس السرقة وبالتالي حفاظا على المصلحة العامة والخاصة ولكيلا يقلت المجرم من العقاب يجب تطبيق القواعد العامة التي تحكم جريمة السرقة إلا أن يصدر تشريع خاص لها دون أن يكون في ذلك أي إخلال بالمبادئ العامة التي تحكم القانون الجنائي.

3-موقف المشرع الجزائري: لم يشرع نصوصا تجرم السرقة المعلوماتية من خلال النص صراحة على سرقة المعلومات إلا أنه أضفى حماية للمعلومات من خلال قوانين متعددة كالقانون 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها المادة 2 الفقرة | 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 للاتصالات الإلكترونية، وبالتالي وفقا للمشرع الجزائري فإن جريمة السرقة الإلكترونية هي جريمة السرقة التقليدية المنصوص عليها في قانون العقوبات كما سبق عرضه يضاف لها أن ترتكب جريمة السرقة أو يسهل ارتكابها بواسطة منظومة معلوماتية أو نظام للاتصالات الإلكترونية[3]

ثانيا: العقوبات جريمة السرقة الرقمية المنصوص عليها في إطار القوانين الخاصة

1-العقوبات المنصوص عليها في الامر 03 – 05 المتعلق بحق المؤلف والحقوق المجاورة

---

[1] معتوق عبد اللطيف، **الإطار القانوني لمكافحة الجرائم المعلوماتية في التشريع الجزائري والتشريع القانوني**، مذكرة مقدمة لنيل شهادة الماجيستر في العلوم القانونية، تخصص في القانون الجنائي، كلية الحقوق والعلوم السياسية، قسم الحقوق ،جامعة الحاج الأخضر، باتنة، 2012، ص 35.

[2] سوير سفيان، مرجع سابق، ص 56- 55.

[3] معتوق عبد اللطيف, **الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن**, مذكرة مقدمة لنيل درجة الماجستير في العلوم القانونية تخصص القانون الجنائي, كلية الحقوق و العلوم السياسية ، قسم الحقوق ، جامعة باتنة 2012، ص 38.

نفس الاتجاه الذي ذهب إليه المشرع الفرنسي اتبعه المشرع الجزائري بحيث استبعد برامج الكمبيوتر صراحة من نطاق الحماية بواسطة قانون براءة الاختراع، وذلك طبقا للمادة 7 من مرسوم تشريعي رقم 93-17 المؤرخ في 19 جولية 2003 فيما يخص براءة الاختراع لا تعد من قبيل الاختراعات في مفهوم هذا الأمر برامج الحاسوب فالمشرع قد تبنى نظام حق المؤلف كبيئة الحماية البرامج دون نظام البراءة [1] وشدد العقوبات الناجمة عن المساس بحقوق المؤلفين لاسيما مؤلفي المصنفات المعلوماتية، إذ تجرم الاعتداءات على الفكرية بحيث تناولته المواد 390 394 من عقوبات، إلا أن بموجب الأمر 97-10 من مظلة قانون العقوبات والتي أصبح لها قانون خاص في قانون العقوبات المادة 393 نقر الغرامة كعقوبة للاعتداء على حق المؤلف، بينما الأمر 93-17 والأمر 03-05 يقرران عقوبتي الحبس والغرامة.[2] والغي هذا الأمر كذلك بموجب الأمر 03-05 حيث تجد عقوبات أصلية وعقوبات تكميلية.

1.1-عقوبات أصلية: نصت المادة 153 من الأمر 03-05 الصادر في 19/07/1003 المتعلق بحق المؤلف والحقوق المجاورة المعدل والمتمم 73-14 على عقوبة التقليد بقولها يعاقب مرتكب جنحة تقليد مصنف أو أداء كما هو المنصوص عليه في المادتين 151 و 152 أعلاه بالحبس من ستة أشهر (6) إلى ثلاثة (3) سنوات وبغرامة مالية من خمسمائة ألف دينار (500.000 دج) إلى مليون دينار (1.000.000 دج سواء كان النشر قد حصل في الجزائر أو في الخارج وكما نصت المادة 154 ق. كذلك بعد مرتكبا الجنحة المنصوص عليها في المادة 151 من هذا الأمر ويستوجب العقوبة المقررة في المادة 153 أعلاه، كل من يشارك بعمله أو بالوسائل التي يحوزها للمساس بحقوق المؤلف أو أي مالك للحقوق المجاورة)[3] وأيضا المادة 155 من نفس القانون يعاقب بنفس العقوبة المقررة في المادة 153 كل من لا يريد أن يدفع المكافأة للمؤلف التي يستحقها أو لأي مالك حقوق مجاورة آخر خرقا للحقوق المعترف بها (9). [4]

2.1- العقوبات التكميلية: تتمثل في المصادرة وغلق المؤسسة وطبقا للمادة 157 من نفس القانون فان المصادرة قد تقع على المبالغ المالية المتأتية من الاستغلال غير الشرعي للمصنف أو الأداء كما تتصرف المصادرة إلى العناد الذي تم ضبطه وحجزه والذي استعمل في إنتاج النسخ المقلدة[5]، وفي المادة 156 من الأمر رقم 03-05 منح للجهة القضائية حق علق المؤسسة التي يستغلها المقلد أو شريكه كمؤسسات التوزيع والبيع بالتجزئة لكن بشرط أن تقوم بإنذار المخالف بواسطة السلطة العمومية [6]

---

[1] اختير مسعود، **الحماية الجنائية لبرامج الحاسوب وأساليبه ونقاط ضعفه** طبعة 2010، دار الهدى، عين مليلة، الجزائر، ص. 76.
[2] يوسف الصغير، مرجع سابق، ص 107.
[3] اختير مسعود، مرجع سابق، ص 99.
[4] اختير مسعود، مرجع نفسه، ص 100.
[5] بوري أحمد، **الحماية القانونية لحق المؤلف والحقوق المجاورة في التشريع الجزائري والاتفاقيات الدولية**. أطروحة لنيل درجة الدكتوراه في العلوم القانونية في القانون الجنائي، كلية الحقوق العلوم السياسية، قسم الحقوق، جامعة باتنة 2015، ص. 130 ,301.
[6] بوري أحمد، المرجع نفسه، ص. 302.

1.3-العقوبات المنصوص عليها في الامر 09-04 المتعلق بالوقاية من جرائم للتكنولوجيا الاعلام واتصال ومكافحتها.

تكمن أهمية هذا القانون في كونه يجمع بين القواعد الإجرائية المكملة لقانون الإجراءات الجزائية وبين القواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة هذه والتدخل السريع لتحديد مصدرها والتعرف على مرتكبها[1] ولذلك أوجد المشرع بموجب القانون رقم 09 04 المتعلق بالوقاية من الجرائم المتصلة بالتكنولوجيا الإعلام والاتصال ومكافحتها العديد من الآليات للوقاية من الجرائم الالكترونية ومن بين هذه الجرائم السرقة وهي تتمثل أساسا في كل من الوقاية والتفتيش والحجز على ألا تستعمل المعلومات المتحصل عليها أثناء عملية المراقبة إلا في الحدود الضرورية للتحريات أو التحقيقات الفضائية، وهذا تحت طائلة العقوبات المنصوص عليها في ذات القانون. [2]وكما أنشاء هيئة وطنية للوقاية من الإجرام المتصل بتكنولوجيات الإعلام والاتصال ومكافحته ومن أحكام خاصة بالتعاون والمساعدة القضائية الدولية[3].

يستنتج في الأخير أن أحكام رقم 09-04 جاء عامة ومطلقة في مجال مكافحة الجرائم المتصلة بتكنولوجية الإعلام والاتصال بحيث تجرم كل الأفعال المخالفة للقانون التي ترتكب عبر وسائل الإعلام والاتصال ويطبق على كافة التكنولوجيات القديمة والجديدة، بما فيها شبكة الانترنت وعلى أي تقنية يمكن أن تظهر مستقبلا. وهدف من هذا القانون هو من أجل الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[4]

3-العقوبات المنصوص عليها في الامر 04-15 المتعلق بقانون العقوبات

سعى المشرع الجزائري في تعديله الأخير القانون العقوبات من الأمر 66-165 إضافة قسم سابع مكرر عنونه المساس بأنظمة المعالجة الآلية للمعطيات" ويشمل المواد من 394 مكرر إلى 394 مكرر.7 [5]وعليه جرم المشرع بموجب هذا القانون الأفعال التي يقوم بها لتعدي على المعالجة الآلية للمعطيات وهي: جريمة الدخول غير المرخص به وهذا ما جاء ذكره في نص المادة 394 مكرر من قانون العقوبات على انه **(يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة**

---

[1] سمية مزغيش، **جرائم المساس بنظم المعلومات**، مذكرة الحصول على درجة الماجستير في القانون الجنائي، كليه الحقوق والعلوم السياسية ، قسم الحقوق ،جامعة محمد خضر، بسكرة 2014، ص 65.

[2] عبد الصديق آل الشيخ، **منع الجرائم الإلكترونية بموجب القانون رقم 04.09 يتضمن قواعد خاصة لمنع الجرائم المتعلقة بتقنيات الإعلام والاتصال ومكافحتها**، مجلة المعالم للدراسات القانونية والسياسية، المجلد 4، العدد 1, 2020، ص197.

[3] سوير سفيان، مرجع سابق، ص22.

[4] براهيمي جمال، **مكافحة الجرائم الإلكترونية في التشريع الجزائري**، مجلة النهضة، المجلد 2، العدد 3، كلية العلوم والعلوم السياسية، جامعة مولود معمري، تيزي وزوو ص 154.

[5] اختير مسعود، مرجع السابق، ص 108.

من 50.000 دج إلى 200.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك). [1]

ويقصد بفعل الدخول هنا هو الركن المادي الجريمة الاعتداء على نظام المعالجة الآلية للمعطيات، ذلك الدخول المعنوي أو الالكتروني باستعمال الوسائل الفنية والتقنية إلى النظام المعلوماتي، ولا بعد فعل الدخول بحد ذاته سلوكا غير مشروع وإنما يتخذ وصفه الإجرامي انطلاقا من كونه قد تم دون وجه حق أو دون ترخيص[2]. نلاحظ المشرع الجزائر يعاقب كل من يدخل أو يبقى في المنظومة المعلوماتية بالحبس والغرامة ويدل ذلك على انه حاول بان يحميها بواسطة هذه المادة.

(تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير المعطيات المنظومة، وإذا ترتب عن أفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من سنة (6) أشهر إلى سنتين (2) والغرامة من 50.000 دج إلى 150.000 دج). وأورد المشرع ظرفين لتشديد عقوبة الدخول غير المشروع إلى المنظمات المعلوماتية، وهو حذف أو تغيير المعطيات وظرف ثاني هو تخريب نظام اشتغال المنظومة. [3]

1.3-الاعتداء على المعطيات الداخلية: وحدد المشرع عقوبة الاعتداء العمدي على المعطيات الموجودة داخل النظام في **المادة 394 مكرر 1 بالحبس من سنة أشهر إلى ثلاث سنوات وبغرامة من 500000 دج إلى 2000000 دج. كل من ادخل بطريق القش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها** [4]ويقصد بالأفعال المنصوص عليها في المادة:

2.3-الإدخال: يقصد به إضافة معطيات جديدة على الدعامة الخاصة بها، سواء كانت خالية أم كان يوجد عليها معطيات من قبل، وكما يتحقق فعل الإدخال في كل حالة يتم فيها إدخال برنامج غريب يضيف معطيات جديدة فيروسات حصان طروادة، قنبلة معلوماتية زمنية[5]

3.3-فعل المحو: يقصد بفعل المحو إزالة جزء من المعطيات المسجلة على دعامة والموجودة داخل النظام أو تحطيم تلك الدعامة أو نقل وتخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة.[6]

---

[1] فتيحة مهري، **جريمة الدخول والدخول إلى أنظمة معالجة البيانات**، مذكرة لنيل شهادة الماجستير في القانون الجنائي، كليه الحقوق و العلوم السياسية ،قسم الحقوق ، جامعة العربي بن مهيدي، أم البواقي، 2016، ص 36.

[2] براهيمي جمال، مرجع سابق، ص 126.

[3] صغير يوسف، **الجريمة المرتكبة عبر الإنترنت**: مذكرة للحصول على درجة الماجستير في قانون الأعمال الدولي، جامعة مولود معمري تيزي وزوو، 2013 ص108

[4] الأمر رقم 04-15 المؤرخ في 10 نوفمبر 2004 المكمل والمعدل للأمر رقم 66-156 المتضمن قانون العقوبات.

[5] البدري فيصل، **مكافحة الجرائم الإلكترونية في القانون الدولي والداخلي**. أطروحة للحصول على درجة الدكتوراه في القانون العام ، كلية الحقوق والعلوم السياسية ،قسم الحقوق ، جامعة الجزائر وحيد بني خدام. ، 2018، ص175-176.

[6] البدري فيصل، مرجع سابق، ص 176.

4.3-فعل التعديل: يقصد بفعل التعديل تغيير المعطيات الموجودة داخل النظام واستبدالها بمعطيات أخرى، ويتحقق فعل المحو والتعديل عن طريق برامج غريبة تتلاعب بالمعطيات سواء بمحوها كليا أو جزئيا أو بتعديلها، وذلك باستخدام القنبلة المعلوماتية الخاصة بالمعطيات وبرنامج الممحاة أو برنامج الفيروسات بصفة عامة [1]

كما أن أفعال الإدخال والمحو والتعديل وردت على سبيل الحصر، ومنه لا يقع تحت طائلة التجريم أي فعل آخر غيرها حتى ولو تضمن اعتداء على المعطيات الموجودة داخل نظام المعالجة الآلية للمعطيات [2]

5.3-جريمة الاحتيال المعلوماتي: كما عاقب على استخدام هذه المعطيات في ارتكاب الجرائم الماسة بالأنظمة المعلوماتية، تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم، وكذا حيازة أو إنشاء أو نشر أو استعمال المعطيات التحصيل عليها من إحدى الجرائم الماسة بالأنظمة المعلوماتية بنص **المادة 394 مكرر 2 بالحبس من شهرين إلى ثلاث سنوات وبغرامة من 1000000 دج إلى 5000000 دج**[3].

6.3-الاعتداءات الواقعة على الأسرار: تسبب أضرار أدبية ومادية معتبرة، لذا حرص المشرع الجزائري على حماية هذه الأسرار من خلال الباب الأول المتعلق بالجنايات والجنح ضد الشيء العمومي **من المادة 61 إلى 96 مكرر من قانون العقوبات**[4] بالإضافة إلى **المادة 39 مكرر 3 من قانون العقوبات التي نصت وتضاعف العقوبات في المادة 394 مكرر 3 المنصوص عليها في هذا القسم، إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام دون الإخلال بتطبيق عقوبات اشد.**

كما نصت **المادة 394 مكرر 4 على معاقبة الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس (5) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي** [5]وأيضا أكد المشروع الجزائري بموجب المادة 394 مكرر 5 على تجريم "**الاشتراك في مجموعة أو اتفاق بغرض الإعداد لجريمة من الجرائم الماسة بالأنظمة المعلوماتية في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها**" غير أن المسؤولية الجزائية للشخص المعنوي لا تستبعد المسؤولية الجزائية

[1] ابدري فيصل، المرجع السابق، ص176.
[2] سوبر سفيان، مرجع سابق، ص 94.
[3] بدري فيصل، مرجع سابق، ص197.
[4] سوبر سفيان، مرجع سابق، ص 38.
[5] قانون رقم 04-15 مؤرخ في 10 نوفمبر 2004 يعدل الأمر رقم 66-156 المدرج في قانون العقوبات.

للأشخاص الطبيعيين بصفتهم فاعلين أو شركاء في نفس الجريمة.[1] وأما الشروع في جريمة المعلوماتية طبقا للمادة 394 مكرر 7 (يعاقب حتى على الشروع في ارتكاب الجنح المنصوص عليها هذا القسم بالعقوبات المقررة للجنحة ذاتها يبدو من خلال النص أن رغبة المشرع في توسيع نطاق العقوبة لتشمل أكبر قدر من الأفعال الماسة بالأنظمة المعلوماتية[2] تلاحظ بان المشرع اقر عقوبات أصلية وعقوبات تكميلية ليعاقب المجرم الذي يتعدى على المنظومة المعلوماتية من اجل مكافحة الجريمة.

تجدر الإشارة أن المشرع الجزائري قد خطى إلى الأمام في هذا المجال بصدور القانون رقم 04-15 المعدل والمتمم للأمر 66/156 المتضمن قانون العقوبات، والذي استحدث بموجبه أحكاما خاصة بالجرائم الماسة بالأنظمة المعلوماتية من المادة 394 مكرر إلى غاية المادة 39 مكرر 7 من السابع مكرر الخاص بالمساس بأنظمة المعالجة الآلية للمعطيات[3]. فالمشرع الجزائري أدرج في نصوص قانون العقوبات التكميلية للمنظومة المعلوماتية والتي تتمثل في المصادرة وغلق المواقع والمتمثلة فيما يلي:

العقوبات التكميلية التي يقرها المشرع في اعتداء المنظومات المعلوماتية هي المصادرة وغلق المؤسسة ويدل ذلك في ما نصت عليه **المادة 394 مكرر 6 كالتالي (مع الاحتفاظ بحقوق الغير حسن النية يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة والملاحظ أن المشرع اخذ بعين الاعتبار حسن النية وبذلك يكون قد انسجم مع مبدأ الشرعية)**[4] إلى جانب عقوبة المصادرة نص المشرع على عقوبة تكميلية وجوبية أخرى هي الغلق وذلك بموجب **المادة 394 مكرر 6 كما يلي: ... مع غلق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها)**[5]

تتمثل الجزاءات المقررة بموجب الفصل السابع مكرر في العقوبات الأصلية وهي عقوبة الحبس والغرامة، وعقوبات تكميلية بموجب نص المادة 394 مكرر 6 والمتمثلة في مصادرة الأجهزة والبرامج والوسائل المستخدمة وإغلاق المواقع والمحل، أو أماكن الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها ومثال ذلك إغلاق مقهى الانترنت الذي يرتكب فيه هذه الجرائم بشرط علم مالكه[6].

المبحث الثاني الخصوصية جريمة السرقة المالية المعلوماتية

[1] صغير يوسف، مرجع السابق، ص 111.
[2] رابحي عزيزة، مرجع سابق، **ص** 250.
[3] سفيان سوبر، مرجع سابق، ص 22.
[4] رابحي عزيزة، مرجع سابق، ص 247.
[5] رابحي عزيزة، المرجع نفسه، ص 247.
[6] صغير يوسف، مرجع سابق، ص 110.

يعد الاثبات في جريمة السرقة الرقمية من صعوبات بمكان حيث يصعب تتبعها واكتشافها فهي لا تترك اثر يقتفى حيث تعتبر مجرد ارقام فان تعقبها يتطلب خبرة فنية يصعب تواجدها لدى محقق العادي من هدا منطلق قمنا بتقسيم المبحث الى مطلبين بحيث نتناول في المطلب الأول: الاثبات في جريمة السرقة الرقمية وقمنا بتقسيم المطلب الى الفرعين بحيث نستعرض في الفرع الأول خصوصيات الاثبات في جريمة السرقة الرقمية نتناول فيها الدليل الرقمي في اثبات السرقة بالإضافة الى معيقات الاثبات اما في الفرع الثاني نستعرض فيه خصوصيات إجراءات التحقيق في جريمة السرقة الرقمية اما في المطلب الثاني: مكافحة جريمة السرقة الرقمية على الصعيد الوطني والدولي

المطلب الأول: الاثبات في جريمة السرقة الرقمية

تعتبر جريمة السرقة الرقمية من أخطر الجرائم لصعوبة اكتشافها واثباتها خاصة انها تتم في العالم الافتراضي. كما تعد متابعة الجريمة المعلوماتية بصفة عامة من بين اهم التحديات التي تواجهها رجال الضبطية القضائية قمنا نتناول في المطلب الأول: الاثبات في جريمة السرقة الرقمية وقمنا بتقسيم المطلب الى الفرعين بحيث نستعرض في الفرع الأول خصوصيات الاثبات في جريمة السرقة الرقمية نتناول فيها الدليل الرقمي في اثبات السرقة بالإضافة الى معيقات الاثبات اما في الفرع الثاني نستعرض فيه خصوصيات إجراءات التحقيق في جريمة السرقة الرقمية.

الفرع الاول: خصوصية الإثبات في جريمة السرقة الرقمية

يختلف الوسط الذي ترتكب فيه الجريمة المعلوماتية من وسط مادي إلى وسط معنوي (الوسط الافتراضي) مما أدى إلى ظهور أدلة جنائية خاصة يمكن الاعتماد عليها في الإثبات بحيث تكون من ذات الطبيعة التقنية الناجمة عن النظام الإلكتروني التي تنتج منها في حالة الاعتداء عليها، وتتفق مع طبيعة الوسط الذي ارتكبت فيه الجريمة وهي الأدلة الرقمية أو الإلكترونية حسب ما غيرت عنها الاتفاقية الأوربية المكافحة الجرائم المعلوماتية.[1]

أولا: الدليل الالكتروني في اثبات السرقة الالكترونية

1_تعريف الاثبات الجنائي: نظرا للصعوبة والتعقيد يكتنف موضوع الإثبات في مجال القانون الجنائي، فقد اختلف الفقهاء في تحديد معنى دقيق وثابت له، ومن بين أهم التعريفات تذكر هو اقامة الدليل إما القضاء بالطرق التي حددها القانون على وجود واقعة قانونية متنازع عليها بين الخصوم[2]

2_مفهوم الدليل الإلكتروني.

[1] سعيد علي نعيم، **اليات البحث والتحري عن الجرائم المعلوماتية في القانون الجزائري**، مذكرة لنيل شهادة الماجيستير في القانون العام، كلية الحقوق و العلوم السياسية ، قسم الحقوق ، جامعة الحاج لخضر باتنة، 2012، ص 119.
[2] احمد عزمي الجروب، **السندات الرسمية الالكترونية**، ط1، دار الثقافة للنشر والتوزيع، عمان, 2010، ص 25.

إن الجرائم الإلكترونية ذات طبيعة خاصة، فإن الكشف عن هذا النوع من الجرائم يحتاج إلى أدلة تعيش في العالم الافتراضي حيث تستخدم فيها الطبيعة التقنية وتتمثل في الدليل الإلكتروني وبعد الوسيلة الوحيدة للإثبات في هذه الجرائم والتحديد مضمون الدليل الإلكتروني لا بد من التطرق إلى تعريفه وخصائصه وأشكاله وانواعه ،عرفه المنظمة العالمية لدليل الحاسوب في قرار لها في أكتوبر 2001 بانه المعلومات ذات القيمة المحملة أو المخزنة أو المنقولة في صورة رقمية، وكانت قد عرفته في مارس 2000 بانه المعلومات المخزنة أو المنقولة والتي يمكن الاعتماد عليها في المحكمة.[1]

3-خصائص الدليل الإلكتروني:

باعتبار أن الدليل الإلكتروني يعيش ضمن البيئة الافتراضية أو الرقمية فهو بذلك يتميز بطبيعة خاصة تميزه عن الدليل العادي من أهمها أن الدليل الإلكتروني دليل علمي فهو يتكون من بيانات ومعلومات ذات صفة الكترونية غير ملموسة وتدرك بالحواس العادية، بل يتطلب إدراكها الاستعانة بالحاسوب والأجهزة الإلكترونية باستخدام فالحصول والاطلاع على الدليل الإلكتروني لا يكون إلا باستخدام الأساليب العلمية. برامج الكترونية خاصة بذلك،[2]ويتميز أيضا الدليل الإلكتروني بأنه دليل تقني بحيث أن التعامل معه يكون من طرف تقنيين مختصين في العالم الافتراضي ،ويتميز أيضا بأنه متنوع و متطور فهو يشمل جميع أنواع البيانات الرقمية التي يمكن تداولها الكترونيا، فبالرغم من أن تكوين الدليل الإلكتروني يعتمد على لغة الحواسيب و الرقمة إلا أنه يتخذ أشكالا مختلفة ، كان يكون في شكل بيانات غير مقروءة كما هو الحال في المراقبة عبر الشبكات و قد يكون عبارة عن بيانات مقروءة كالوثيقة المعدة بنظام المعالجة الآلية بالإضافة إلى ذلك يمكن أن يكون عبارة عن صورة ثابتة أو متحركة أو مخزنة في البريد الإلكتروني فهو يشمل أنواع متعددة من البيانات الرقمية و التي تصلح بأن تكون دليل إدانة أو براءة و الدليل الإلكتروني [3]في مواكبة مستمرة للتطور الحاصل في تكنولوجيا المعلومات ، فهو تبعية دائمة للتطور المتواصل في البيئة الإلكترونية.

4-أشكال الدليل الالكتروني: الدليل الرقمي لا يأخذ صورة واحدة بل يوجد له العديد من الصور والأشكال من بينها الصورة الرقمية وهي عبارة عن تجسيد الحقائق المربية حول الجريمة، وفي العادة تقدم الصورة في شكل ورقي أو في شكل مرئي، باستخدام الشاشة المرئية والصورة الرقمية تمثل تكنولوجيا بديل للصورة التقليدية[4]ومن بينها أيضا النصوص المكتوبة والتي تشمل الأوراق

[1] سعيد علي نعيم، مرجع سابق، ص 119.
[2] خالد عياد الحلبي، **إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت**، ط1، دار نشر، عمان، ص 230.
[3] خالد عياد الحلبي، المرجع نفسه، ص 231.
[4] سعيد علي نعيم، مرجع سابق، ص 124.

التحضيرية التي يتم إعدادها بخط اليد كسودة أو تصور العلمية التي يتم برمجتها وكذلك نصوص أساسية وقانونية محفوظة في الملفات العادية وتكون لها علاقة بالجريمة.

إضافة إلى التسجيلات الصوتية التي يتم ضبطها وتخزينها بواسطة الآلة الرقمية أو تشعل المحادثات الصوتية على الانترنت [1] .

5-انواع الدليل الالكتروني: هناك من الأدلة الإلكترونية ما أعدت لتكون وسيلة إثبات وتتمثل في السجلات التي تم إنشاؤها بواسطة الجهاز تلقائيا وهي مخرجات الحاسوب التي لم يكن للأفراد يد في إنشاؤها، وكأمثلة عن ذلك البطاقات البنكية والسجلات التي تم حفظ جزء منها والجزء الآخر تم إنشاؤه بواسطة الحاسب الآلي كرسائل غرف المحادثة المتبادلة عبر الانترنت أما الأدلة التي لم تعد لتكون وسيلة إثبات هي تلك الأدلة التي نشأت دون إرادة الفرد. فهي عبارة عن آثار يتركها الجاني في مسرح الجريمة دون رغبته في وجودها ويطلق عليها تسمية البصمة الوراثية، حيث أن هذا النوع من الأدلة لم يعد للحفظ لكن الوسائل الفنية الخاصة تمكنت من ضبط هذه الأدلة حتى وأن مرت عليها فترة زمنية طويلة ومثال ذلك الاتصالات التي تتم عبر الانترنت والمراسلات التي صدرت من الجاني أو تلقاها. [2]

ثانيا: شروط قبول القاضي الجزائي للأدلة الرقمية من جرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

حتى يتحقق الدليل الازم للإثبات فإنه لابد من أن تتوفر فيه شروط تجعل له حجية وقيمة يثبت بها الحق

1_شرط مشروعية الدليل الرقمي: يشترط في الدليل الرقمي الجنائي عموما لقبوله كدليل إثبات أن تتم الحصول عليه بطريقة مشروعة ووفقا للأمانة والنزاهة ذلك أنه يستلزم على القاضي الجنائي تطبيق الدليل تطبيقا سليما وأن يستمد اقتناعه من دليل رقمي مقبول، لأن محل الحرية التي يتمتع بها القاضي الجنائي هو الأدلة المقبولة،[3] وألا يتحصل عليه من أدلة غير مشروعة كالإكراه المادي أو المعنوي أو الغش ضد الجاني في الجرائم المعلوماتية من أجل فك الشيفرة وهو ما ذهب إليه المشرع الجزائري. اذ عبر صراحة في نص المادة 160 من في ا ج على استبعاد الأدلة الغير مشروعة، وبالثاني فإن الأدلة الرقمية غير المشروعة تستبعد ولا يؤخذ بها استنادا إلى القواعد العامة.

2_شرط يقينية الأدلة الإلكترونية الناتجة عن جرائم المساس بأنظمة المعالجة الآلية للمعطيات.

---

[1] سعيد علي نعيم، المرجع السابق، ص 127.

[2] خالد عياد الحلبي، المرجع نفسه، ص 234.

[3] خالد عياد الحلبي، **إجراءات التحري والتحقيق وجمع الأدلة في جرائم الحاسوب والانترنت**، طبعة الأولى، دار الثقافة، الأردن, 20111، ص 238.

إن القاعدة العامة تقتضي بأن الأصل في الإنسان البراءة ، وهذا يتطلب أن يكون الدليل قريبا من الحقيقة الواقعة وأن يكون بعيدا عن التخمين والطن وهذا يخاف نتيجة مفادها إن جميع الأدلة ومنها المستخلصة من الوسائل الإلكترونية تخضع لتقدير القاضي الذي يقدر مدى اقتناعه بها بعد التثبت من صحة وسلامة الإجراء الذي اتبع في استخلاصها من خلال بناء حكمه على الأدلة اليقينية الجازمة[1]، وذلك يتطلب نوعين من المعرفة أولهما: المعرفة الحسنة التي تتركها الحواس من خلال معاينة هذه المخرجات وتفحصها، وثانيهما: المعرفة العقلية عن التحليل والاستنتاج من خلال الربط بين هذه المخرجات والملابسات التي أحاطت بها، ولم يخص المشرع الجزائري نصوص صريحة تتناول كيفية قبول الدليل الرقمي مما يحيلنا إلى طرق الإثبات العامة المطبقة في قبول الأدلة والتي تخضع إلى السلطة التقديرية للقاضي عملا بنص المادة 212 ق ا ج ما يجعلها مقبولة نظريا. [2]

3-شرط مناقشة الدليل الرقمي للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

نصت المادة 212 الفقرة 02 من ق (ج على أنه ولا يسرع للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت فيها المناقشة حضورية أمامه، ويستوي الأمر بالنسبة للأدلة الرقمية سواء كانت في شكل مخرجات ورقية أو الكترونية أو معروضة بواسطة الكمبيوتر على الشاشة الخاصة به، فيجب أن تعرض للمناقشة أثناء المحاكمة. بوصفها أدلة إثبات، والقاضي الجزائي الحرية في أن يستمد قناعته منها طالما أن لها ووقعت عليها المرافعات وناقشها أطراف الدعوى، ويترتب على هذه القاعدة شرطان أساسيان هما:

أ_ وجوب مناقشة الدليل الإلكتروني بين أطراف الدعوى.[3]

ب_ الضوابط المتعلقة بالاقتناع القضائي: إذ أن سلطة القاضي الجزائي في تقديم الأدلة الرقمية وموازنتها وفقا لما يمليه وجدانه لا يخضع في ذلك الرقابة المحكمة العليا إلا أنه مع ذلك مقيد بضرورة تأسيس اقتناعه على الجزم واليقين من غير أن يكون هذا الاقتناع مخالفا لمقتضيات العقل والمنطق السليم.

ثالثا: موقف المشرع الجزائري.

سنتطرق للحديث عن موقف المشرع الجزائري من النص عن الأدلة الرقمية ثم موقفه من قبول هذه الأدلة الغير مرئية في إثبات الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

---

[1] ممدوح حسن مانع العدوان، نادر عبد الحليم السلامات، **مشروعية وحجية الدليل المستخلص من التفتيش الالكتروني في التشريع الجزائري الأردني**، مجلة دراسات علوم الشريعة والقانون، كلية الشريعة والقانون، جامعة العلوم الإسلامية العلمية، المجلد 45، العدد 04، 2018، ص 64

[2] بحرية هارون، مرجع السابق، ص 10-15-16.

[3] بحرية هارون، المرجع نفسه، ص 13-14.

1-موقف المشرع الجزائري من النص على الدليل الرقمي الناتج عن جرائم المعالجة الآلية للمعطيات.

تناول المشرع الجزائري في القانون 09-04 طرق حديثة لاستخلاص الأدلة الرقمية منها المراقبة الإلكترونية، التفتيش والضبط المعلوماتي، وهي إجراءات ذات بعدين أولها للوقاية من الجرائم المعلوماتية وثانيها لمكافحة الجريمة وذلك بضبط الأدلة الرقمية، وبعد الاطلاع على نص المادة 06 من قانون تكنولوجيا الإعلام والاتصال 09-04 نجد أن المشرع الجزائري تحدث عن حجز المعطيات المفيدة في كشف الجرائم أو مرتكبيها بعد أن يتم نسخ المعطيات على دعامة تخزين وحجزها وهي شكل من أشكال الأدلة الرقمية كما سبق بيانه، فالمشرع هنا يقصد بالأدلة الرقمية ولو لم يسميها إلا أنه يحرص على تحريز الدليل الرقمي لإثبات أنه أصيل وموثوق به ويقع ضمن سلسلة الأدلة مقدمة الدعوى.[1]

مما يعني أن المشرع الجزائري تبنى الأدلة الرقمية لكن بدون تسمية صالحة، وصفوة القول إن مبدأ قبول الأدلة الرقمية يجد له أساس قانون الإجراءات الجزائية في باب طرق الاثبات أين ترك المجال مفتوحا لقبول أي دليل من شأنه إثبات الجريمة تطبيقا لمبدأ حرية الاثبات لذلك لم يجد المشرع خرجا لما وضع نصوص في القانون 09-04 وجاءت خالية من ذكر الدليل الرقمي شأنه في ذلك شأن الأدلة العلمية الأخرى مثل: ADN

2-موقف المشرع الجزائري من قبول الدليل الرقمي في إثبات الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

لم يخص المشرع الجزائري نصوص صريحة تتناول كيفية قبول الدليل الرقمي مما يحيلنا إلى طرق الإثبات العامة المطبقة في قبول الأدلة والتي تخضع إلى السلطة التقديرية للقاضي عملا بنص المادة 212 من ق. إ. ج"، يجوز إثبات الجرائم بأي طريقة من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الشخصي، مما يجعلها مقبولة نظريا ومنه تبقى مسألة تقييم الدليل الجنائي في إثبات الواقعة الجرمية هي مسألة موضوعية محصنة، ولهذا يترك للقاضي الجنائي حرية تقدير أدلة جنائية وتكوين قناعته ويبني حكمه على أي دليل ما تطمئن إليه ولو كان مستمد من محاضر الاستدلالات، وهذا ما أوردته المادة 215 من ق ع ج بقولها لا تعتبر المحاضر والتقارير المثبتة للجنايات أو الجنح إلا مجرد استدلالات مالم ينص القانون على خلاف ذلك، وأما بالنسبة لتقارير الخبرة الفنية فإن المشرع

[1] نائلي لحسن، **التحقيق في الجرائم المتصلة بتكنولوجيا المعلوماتية (بين النصوص التشريعية والخصوصية التقنية)**، دط ، النشر الجامعي الجديد، الجزائر, 2017، ص 116

الجزائري اعتبرها مثل باقي أدلة الاثبات من خلال خضوعها للسلطة التقديرية للقاضي وهو ما أكدته المادة 215 المذكورة أعلاه[1].

رابعا: معيقات إثبات الجريمة الالكترونية.

فالجرائم الالكترونية تتصف بالخفاء أي عدم وجود آثار مادية يمكن متابعتها وهي خطيرة وصعبة الاكتشاف أو هي صعبة في تحديد مكان وقوعها، أو مكان التعامل معها بسبب اتساع نطاقها المكاني، وضخامة البيانات.

وبعد إثبات الجريمة الالكترونية من الصعوبة بمكان حيث يصعب تتبعها واكتشافها فهي لا تترك أثرا يقتفي، حيث تعتبر مجرد أرقام، فمعظم الجرائم الالكترونية تم اكتشافها بالصدفة وبعد وقت طويل من ارتكابها كما أنها تفتقر الى الدليل المادي التقليدي مثلا ومن جهة أخرى، فإن تعقبها يتطلب خبرة فنية يصعب تواجدها لدى المحقق العادي للتعامل معها. [2]

وتتميز عن الجريمة التقليدية في كونها تتميز بطابع خاص لا نظير له في الجرائم الأخرى خاصة التقليدية، يتمثل في صعوبة اكتشافها وإثباتها نظرا لأسباب تتمثل في:

1.4-فضاء الجريمة: أي أن الجريمة الالكترونية في الغالب تكون منتشرة وخفية لا يلاحظها المجني عليه وذلك لأنها لا تترك أي أثر خارجي بعد ارتكابها لانعدام الدليل المرئي الملموس[3] في حين أن الجريمة التقليدية لا تكون خفية حيث يتم ملاحظتها مثل: وجود جثة لقتلى أو آثار اقتحام السرقة الأموال.

2.4-صعوبة الاحتفاظ بآثار الجريمة: حيث تعتبر الأدلة فيها غير مرئية فهي عبارة عن نبضات الكترونية تنساب عبر أجزاء الحاسوب والشبكة، وهذا ما يساعد الجاني في محو الأدلة وتدميرها في زمن قصير كما أن الدليل في هذه الجرائم غالبا ما يكون مرموزا أو مشفرا حيث لا يمكن للشخص قراءتها دون اللجوء الى الأدلة وبظهورها على شاشة الحاسوب. [4]

في حين أن الأدلة في الجريمة التقليدية تكون مرئية ويكون من الصعب على الجاني محوها في زمن قصير، ويمكن لشخص قراءتها دون اللجوء الى الآلات أو الحواسيب.

الفرع الثاني: خصوصية إجراءات التحقيق في جريمة السرقة الرقمية

باعتبار ان السرقة المالية المعلوماتية هي جريمة الكترونية فهي تخضع لنفس القواعد التي تخضع لها هذه الأخيرة من إجراءات المعاينة والتفتيش والضبط وأساليب التحري الخاصة.

أولا: التفتيش والضبط في جريمة السرقة الرقمية

[1] سعيداني نعيم، مرجع سابق، ص 214.
[2] خالد ممدوح إبراهيم، مرجع سابق، ص 79.
[3] هشام رستم، الجرائم المعلوماتية، **أصول التحقيق الجنائي، مجلة الامن والقانون**، مجلة دبي، الامارات العربية المتحدة، المجلد5، العدد 2، 1999، ص 11.
[4] هبة نبيلة هرول، مرجع سابق، 48.

عرف التفتيش بأنه: " البحث عن الأشياء المتعلقة بالجريمة لضبطها وضبط كل ما يفيد في كشف حقيقتها ويجب أن يكون التفتيش سند من القانون".[1] من خلال هذه التعريفات يتضح بأن التفتيش ينطبق على الجرائم التي تترك اثار مادية وبالتالي فلا توجد مشكلات تعيق إجراؤه لأن من خلاله سيتم البحث عن الأدلة المادية الملموسة.[2]

1_ نطاق تفتيش مكونات النظام المعلوماتي في جرائم الأنترنت:

1.1- تفتيش مكونات النظام المعلوماتي المعنوية: يتكون النظام المعلوماتي من مكونات مادية ومعنوية:

أ-تفتيش مكونات النظام المعلوماتي المعنوية

قد يرد التفتيش على مكونات النظام المعلوماتي المتمثل في المعلومات المعالجة آليا، ولعل الصورة المعتادة والمثال العملي الذي يمكن تقريره هو فحص البرمجيات، الذي بعد من الوسائل الرئيسية في الكشف عن أكثر جرائم الاعتداء على نظم المعالجة الآلية لوجود برمجيات غير مصنفة تعمل في بيئة الاختراق أو تساعد عليه، كما هو الشأن في برمجيات المسح للكشف عن الأبواب المفتوحة يمكن أن يشكل منطقة استفهام ودلالة كافية أيضا على ارتكاب الشخص الجريمة الدخول غير المشروع النظام المعالجة الآلية إذا استتبع ذلك اعترافا شفويا بارتكاب الجريمة حيث أجاز المشرع الجزائري تفتيش المعطيات المعلوماتية وذلك بموجب المادة 05 من القانون رقم 09-04 السالف الذكر، وقد أجازت هذه المادة للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 04 من نفس القانون التي من بينها توافر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الاقتصاد الوطني وللوقاية من هذه الجرائم الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها وكذا منظومة تخزين المعطيات.[3]

ب_ تفتيش المنظومة المعلوماتية عن بعد في الجرائم الإلكترونية

التفتيش في نطاق الجرائم الالكترونية لا يخرج عن إحدى العرضيتين:

ت -شروط التفتيش الجرائم الالكترونية

يمكن تقسيمهم إلى نوعين:

_ القواعد الموضوعية للتفتيش وتتضمن عدة شروط وهي:

[1] خالد ممدوح إبراهيم، **فن التحقيق الجنائي في الجرائم الالكترونية**، ط1، دار الفكر الجامعي، الإسكندرية، مصر ,2009ص 182
[2] دلال مولاي ملياني، مرجع سابق، ص 214.
[3] دلال مولاي ملياني، المرجع نفسه، ص 218.

-وقوع جريمة معلوماتية وهي كل فعل غير مشروع مرتبط باستخدام الحاسوب التحقيق أغراض غير مشروعة

- تورط شخص او اشخاص معينين في ارتكاب الجريمة الالكترونية أو الاشتراك _توافر إمارات قوية أو قرائن على وجود اشياء أو أجهزة أو معدات معلوماتية تفيد في كشف الحقيقة.

-أن يكون محل التفتيش هو الحاسوب بكل مكوناته المادية والمعنوية وشبكات الاتصال الخاصة به.

ث-القواعد الشكلية للتفتيش وتتضمن عدة شروط منها:

_أن يتم التفتيش بأسلوب الى الكتروني من قبل الأجهزة القائمة بالتفتيش وبصورة سريعة.

_أن يكون أمر التفتيش مسببا أي يجب أن يتضمن الاسباب التي أدت إلى إجراءه. _تكوين فريق التفتيش يجب أن يتضمن خبراء مسرح الجريمة من الفلبين والمختصين بشكل ممتاز بالحاسوب والأنظمة الالكترونية وبالإضافة إلى رجال الشرطة وأن يتكون الفريق من المشرف على التحقيق، فريق التفتيش العملي من خبراء الحاسوب، فريق الأمن والحماية من رجال الشرطة.[1]

-الضبط في الجرائم الالكترونية في إطار قانون 09-04

لما أقر المشرع الجزائري تفتيش المنظومة المعلوماتية كما سبق وأن فصلنا في الضرورة كان لابد له أن يقر ضبط الاشياء المستخلصة من تفتيش البيئة الافتراضية بما يناسبها وهو الحجز بأنواعه، والحجز هنا هو كل ما يتعلق بإجراءات التحقيق أي التفتيش عن بعد والضبط هذا بعد من إجراءات التحقيق حيث أن الضبط بعد في الأصل من إجراءات الاستدلال.[2]

حيث نظم المشرع الجزائري الضبط في المادة (16) من القانون 09-04) والتي تتمكن من خلالها السلطة التي تباشر التقديم من ضبط أو حجر المعطيات تكون مفيدة في كشف الجرائم أو مرتكبيها. والضبط يعني وضع اليد على أي شيء يتصل بالجريمة التي وقعت من أجل الكشف عن الحقيقة وعن مرتكبيها.[3]

_ إجراءات الضبط في الجريمة الالكترونية

نص المشرع الجزائري على حجز المعطيات في المواد 106 إلى 09 من القانون 04-09 فوفقا للمادة 06 عندما تكتشف السلطة التي تباشر التفتيش معطيات تفيد في كشف الجرائم أو مرتكبيها يتم نسخ المعطيات محل البحث على دعامة تخزين الكترونية تكون قابلة للحجز والوضع في أجران وفقا للقواعد المقررة في قانون! ج. ج وإذا استحال الحجز الأسباب تقنية يتعين على

[1] خالد حياد الحلبي، **إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت**، ط1، دار الثقافة للنشر والتوزيع، عمان, 2011، ص 154_155.
[2] دلال مولاي ملياني، مرجع سابق، ص 228.
[3] خالد عياد الحلبي، مرجع سابق، ص 168.

السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة المنع الوصول إلى المعطيات أو نسخها ويجب عليها السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية.[1]

ثانيا: المعاينة والمراقبة الالكترونية

بالإضافة إلى التفتيش والضبط تأتي إجراءات تتعلق بالمعاينة والمراقبة:

1-معاينة في الجريمة الالكترونية

2-معاينة مسرح الجريمة

المعاينة في الجريمة الإلكترونية ليست مسألة مرتبطة بالضرورة بالانتقال غير العالم المادي بل قد تتم عبر العالم الافتراضي وهناك عدة طرق يستطيع بها عضو سلطة التحقيق أن ينتقل الى العالم الافتراضي المعاينة ومن ذلك:

من مكتبه بالمحكمة من خلال الحاسب الآلي الخاص به.

-كما يمكنه اللجوء إلى مقهى الانترنت وأيضا يمكنه اللجوء إلى مزود خدمة الانترنت الذي يعتبر أفضل مكان يمكن إجراء المعاينة فيه[2]

-ويستطيع المحقق المعاينة في المسرح التقليدي ويقع خارج بيئة الحاسوب ويتكون بشكل رئيسي من المكونات المادية المحسوسة للمكان الذي وقعت فيه الجريمة كالبصمات وغيرها وربما ترك متعلقات شخصية.[3]

3-ضوابط الواجب مراعاتها عن مسرح الجريمة

عند إجراء المعاينة بعد وقوع الجريمة في المجال الالكتروني فيجب مراعاة الضوابط التالية:

-ضبط أو سحب أو جمع أو التحفظ على البيانات والمعلومات أو أنظمة المعلومات أو تتبعها في أي مكان أو نظام ويتم تسليم أدلتها الرقمية للجهة مصدرة الأمر على ألا يؤثر ذلك على استمرارية النظم وتقديم الخدمة إن كان لذلك مقتضى.

-البحث والتفتيش والدخول والنفاذ إلى برامج الحاسب وقواعد البيانات وغيرها من الأجهزة والنظم المعلوماتية تحقيقا لغرض الضبط.[4]

-تصوير الحاسب والأجهزة الطرفية المتصلة به على أن يتم تسجيل وقت وتاريخ ومكان التقاط الصورة.

---

[1] صالح شتين، **إجراءات التحري والتحقيق في جرائم تكنولوجيا الاعلام والاتصال في التشريع الجزائري**، مجلة الدراسات القانونية، جامعة عبد الرحمان ميرة، بجاية، الجزائر، المجلد 4،العدد 01، ص 283.

[2] خالد ممدوح إبراهيم، مرجع سابق، ص 156_157.

[3] منير محمد الجنيبي، **صعوبات التحقيق واستخراج الأدلة في جرائم المعلومات**، ط1، دار الفكر الجامعي، الإسكندرية,2018، ص 63.

[4] خضرة شنتير، مرجع سابق، ص 68.

إخطار الفريق الذي سيتولى المعاينة قبل موعدها بوقت كاف حتى يستعد من الناحية الفنية والعلمية، وذلك لكي يضع الخطة المناسبة لضبط أدلة الجريمة حال معاينتها. إعداد خطة المعاينة موضحة بالرسومات مع تمام المراجعة التي تكفل تنفيذها. أن تتم هذه الإجراءات وفق مبدأ المشروعية وفي إطار ما تنص عليه القوانين الجنائية. والمعاينة وإن أنت في الجرائم إلا أن أهميتها تتضاءل في بعض الجرائم مثل جريمة السب".[1]

4_المراقبة الإلكترونية:

استحدث المشرع الجزائري إجراءات المراقبة الإلكترونية بموجب المادة 03 من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، لم يتطرق إلى تحديد المقصود بمراقبة الاتصالات الإلكترونية واكتفى بتحديد مفهوم الاتصالات الإلكترونية وذلك في الفقرة "د" من المادة الأولى من نفس القانون.[2]

5_ اعتراض المراسلات السلكية واللاسلكية:

المراسلات التي يمكن اعتراضها يجب أن تتسم بالخصوصية ولكي تكون كذلك بلزمة أن يتوافر فيها عنصران أساسيان هما:

_ عنصر موضوعي يتعلق بموضوع ومضمون الرسالة في حد ذاتها بمعنى أن تكون الرسالة ذات طابع شخصي وسري.

_ عنصر شخصي والمراد به إرادة المراسل في تحديد المرسل ورغبته في عدم السماح للغير بالاطلاع على مضمون الرسالة[3]

لا يمكن لضباط الشرطة القضائية اللجوء إلى اعتراض المراسلات إلا بعد أن يحصل على إذن مكتوب ومبين من طرف وكيل الجمهورية أو قاضي التحقيق في حالة فتح تحقيق قضائي.

المطلب الثاني: مكافحة جريمة السرقة الرقمية .

تعرف الجريمة الالكترونية أنها ذات بعد دولي عابر للحدود الوطنية وأن من بين الإجراءات المهمة التي تساعد في إثبات الجريمة والحد من الإشكالات المطروحة من هذه الناحية، فإن مكافحتها لا يتحقق إلا بوجود تعاون دولي على المستوى الإجرائي الجنائي كما أن التحقيقات المتبادلة في الجريمة الإلكترونية وملاحقتها قضائيا تؤكد أهمية المساعدة القانونية المتبادلة بين الدول.[4]

---

[1] منير محمد الجنيهي، مرجع سابق، ص 66.

[2] المادة الأولى من القانون رقم 09_04 المتضمن القواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها.

[3] سعيد علي نعيم، **اليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري**، مذكرة لنيل شهادة الماجيستر تخصص علوم جنائية، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة الحاج لخضر، باتنة، الجزائر،2012، ص 179.

[4] غانم مرضي، **الجرائم المعلوماتية، ماهيتها، خصائصها، كيفية، التصدي لها قانونا**، دار الطيبة الدولية للنشر والتوزيع، عمان، الأردن، 2016، ص 98.

الفرع الأول: مكافحة جريمة السرقة الرقمية على صعيد الدولي.

تعرف الجريمة الالكترونية انها ذات بعد دولي عابر للحدود الوطنية و ان من بين الإجراءات المهمة التي تساعد في اثبات الجريمة و الحد منها فان مكافحتها لا يتحقق الا بوجود تعاون دولي على المستوى الاجرائي الجنائي.

أولا: تعريف التعاون القضائي الدولي

يعرف التعاون القضائي الدولي بأنه كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم،[1]حيث أن المشرع الجزائري قد أوجد استثناء فالأصل أن هذه المساعدة تتم عن طريق التمثيل الدبلوماسي أو ما يعرف بالقنوات الدبلوماسية كما هو منصوص عليه في المادة 721 من قانون. ج. لكن ومواكبة للتطور السريع والمستمر وفى حالة الاستعجال وهذا في محاولة إلى إزاحة عوائق التعاون الدولي ومن بينها المساعدة القضائية بتسيير الاتصال وتنسيق العمل على أساس احترام السيادة والمعاملة بالمثل يتم جمع الأدلة ومن بينها الأدلة الجنائية الالكترونية بالطرق السريعة والتي تتجسد في الفاكس والتريث الالكتروني ولكن بشروط معينة.[2]

ويتخذ التعاون القضائي صورا عدة منها:

1- تبادل المعلومات:

وهو يستعمل تقديم البيانات والمعلومات والوثائق والمواد التي من شأنها تسهيل مهمة المحاكمة وقد يشمل ذلك التبادل السوابق القضائية للجناة[3]، وأن مكافحة الجرائم لا تتحقق إلا من خلال تعاون دولي حقيقي، وقد تبلور هذا النوع من التعاون منذ إنشاء المنظمة الدولية للشرطة الجنائية (الإنتربول) وتقوم هذه المنظمة بتشجيع التعاون الدولي بين أجهزة الشرطة في الدول الأطراف على نحو فعال يحقق مكافحة الجريمة.[4]

2-نقل الإجراءات:

ويقصد بذلك قيام دولة ما بناء على اتفاقية أو معاهدة باتخاذ إجراءات جنائية وهي بصدد جريمة ارتكبت في إقليم دولة أخرى والمصلحة هذه الدولة متى توافرت شروط معينة من أهم هذه الشروط التجريم المزدوج والمقصود به أن يكون الفعل المنسوب إلى الشخص بشكل جريمة في الدولة الطالبة والدولة المطلوب إليها نقل الإجراءات المطلوب اتخاذها بمعنى أن يكون الإجراءات

---

[1] غانم مرضي، المرجع السابق، ص 98.
[2] المادة 16 من القانون 09_04.
[3] غانم مرضى، مرجع سابق، ص99.
[4] محمد موسى، **تنازع الاختصاص في الجرائم الالكترونية**، مجلة دفاتر السياسة والقانون، جامعة قاصدي مرباح، ورقلة، العدد2 سبتمبر 2009، ص 153.

المطلوب اتخاذها مقررة في قانون الدولة المطلوب إليها عن ذات الجريمة، وقد أقرت العديد من الاتفاقيات الدولة كمعاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية.

3-الإنابة القضائية الدولية:

يقصد بالإنابة القضائية طلب اتخاذ إجراء قضائي من إجراءات الدعوى الجنائية تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها لضرورة ذلك الفعل في مسألة معروضة على السلطة القضائية في الدولة الطالبة ويتعذر عليها القيام بنفسها وأن تنفيذ طلب الإنابة غير ملزم للدول المناب لأن أساسها اعتبارات المجاملة الدولية.[1]

ثانيا: جهود المنظمة الدولية للشرطة الجنائية (الإنتربول)

وهي تسمى باللجنة الدولية للشرطة الجنائية (ICPO) ومقرها بباريس في فرنسا وقد غير اسمها ليصبح المنظمة الدولية للشرطة الجنائية، وتضم في عضويتها أكثر من 182 دولة عضو وتهدف هذه المنظمة إلى تأكيد وتشجيع التعاون بين أجهزة الشرطة في الدول الأطراف وعلى نحو فعال في مكافحة الجريمة من تجميع البيانات والمعلومات المتعلقة بالمجرم والجريمة وذلك عن طريق المكاتب المركزية فيما بينها، بالإضافة إلى التعاون في ضبط المجرمين بمساعدة أجهزة الشرطة في الدول الأطراف.[2]

الفرع الثاني: مكافحة جريمة السرقة الرقمية على صعيد الوطني

لتصدي للجريمة السرقة الرقمية تتم بوجود هيئات خاصة تعمل على الوقاية من هذه الجرائم ومكافحتها حيث ان المشرع الجزائري احدث هيئة وطنية من الجرائم المتصلة بتكنولوجيا للإعلام والاتصال

أولا: التعريف بالهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال:

من خلال نص المادة 13 من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها فتعرف الهيئة على أنها هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته، وتعرف أيضا على أنها مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلالية المالية تحت سلطة وزارة الدفاع الوطني. يحدد مقر الهيئة بمدينة الجزائر ويمكن نقله إلى أي مكان آخر من التراب الوطني بموجب قرار من وزير الدفاع الوطني.

[1] غانم مرضى، مرجع سابق، ص 99.
[2] غانم موسى، مرجع سابق، ص 97.

ثانيا: مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال:

حددت المادة 14 من القانون رقم 09-04 [1]المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال مهام الهيئة على سبيل المثال لا على سبيل الحصر وهي كالتالي:

1 – تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها

2 – مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيا الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية.

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

ثالثا: تنظيم وتشكيل الهيئة

تم تنظيم وتحديد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بموجب المرسوم الرئاسي رقم 19-172 الذي يحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها[2] تنص المادة 04 من المرسوم الرئاسي رقم 19-172 على أن الهيئة تتشكل من مجلس توجيه ومديرية عامة 01/ مجلس توجيه:

نظمت المواد 05 و206 و07 و08 من المرسوم الرئاسي رقم 19-172 على أن تشكيلة المجلس ومهامه ودوراته، حيث يتشكل المجلس من ممثلي وزارات حددها المرسوم على سبيل الحصر وهي ممثلة عن وزارة الدفاع الوطني، وممثل عن الوزارة المكلفة بالداخلية، وممثل عن كل من وزارة العدل والوزارة المكلفة بالمواصلات السلكية واللاسلكية، ويرأس مجلس التوجيه وزير الدفاع الوطني باعتبار أن الهيئة موضوعة تحت سلطة وزارة الدفاع الوطني. [3]

حددت المادة 06 مهام مجلس التوجيه على سبيل الخصوص وليس على سبيل الحصر حيث يكلف

1_ التداول حول الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

2-التداول حول مسائل التطوير والتعاون مع المؤسسات والهيات الوطنية المعنية بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

3-الموافقة على برامج الهيئة.

---

[1] مرسوم رئاسي **يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال**، مقالة منشورة بالموقع "http://www.aps ds.

[2] مرسوم رئاسي رقم 19-172 مؤرخ في 3 شوال عام 1440 الموافق 6 يونيو سنة 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وتنظيمها وكيفيات سيرها.

[3] المادة 05 من المرسوم الرئاسي رقم 19-172 المتعلق بتحديد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

- إعداد نظامه الداخلي والمصادقة عليه أثناء أول اجتماع له.
- دراسة التقرير السنوي لنشاطات الهيئة والمصادقة عليه.
- إبداء رأيه في كل مسألة تتصل بمهام الهيئة.
- تقديم كل اقتراح يتصل بمجال اختصاص الهيئة.
- المساهمة في ضبط المعايير القانونية في مجال اختصاصه
- دراسة مشروع ميزانية الهيئة والموافقة عليه. [1]

2_ المديرية العامة:

نصت المادة 10 من المرسوم الرئاسي رقم 19-172 على أن المديرية العامة تضم مديرية تقنية ومديرية للغدارة والوسائل والمصالح حيث يرأسها مدير عام، من بين أهم الصلاحيات الممنوحة للمديرية العامة السهر على حسن سير الهيئة، وإعداد مشروع ميزانية الهيئة، وإعداد وتنفيذ برامج عمل الهيئة،

أ_ تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها وتبادل المعطيات المتعلقة بتحديد مكان مرتكب الجرائم المتصلة بتكنولوجيا الإعلام والاتصال والتعرف عليهم.

ب_ تحضير اجتماعات مجلس التوجيه وإعداد التقرير السنوي لنشاطات الهيئة[2].

وتتولى المديرية العامة أمانة المجلس. [3]

تكلف المديرية التقنية بمهمة المراقبة الوقائية للاتصالات الإلكترونية في إطار الوقاية من الجرائم الموصوفة بأفعال إرهابية أو تخريبية أو الاعتداء على أمن الدولة. [4]

تضع المديرية التقنية التجهيزات والوسائل والأجهزة التقنية الضرورية لتنفيذ مهامها على مستوى المنشآت القاعدية للمتعاملين ومقدمي الخدمات في مفهوم التشريع المعمول به. [5]

[1] لمادة 06 من المرسوم الرئاسي رقم 19-172 المتعلق بتحديد تشكيلة الهيئة الوطنية للوقاية من الجرائم الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها.

[2] المادة 09 من المرسوم الرئاسي رقم 19-172 المتعلق بتحديد تشكيلة الهيئة الوطنية للوقاية من الجرائم الم الإعلام والاتصال ومكافحتها

[3] المادة 05 من نفس المرسوم.

[4] المادة 11 من نفس المرسوم.

[5] المادة 15 من المرسوم الرئاسي رقم 19-172 المتعلق بتحديد تشكيلة الهيئة الوطنية للوقاية من الجر الاعلام الاتصال ومكافحتها تنظيمها وكيفيات سيرها

خلاصـــة:

واخيرا نستخلص في نهاية هذا الفصل الذي تناولنا فيه التنظيم القانوني لجريمة السرقة الرقمية أين تطرقنا إلى التكيف القانوني لهذه الجريمة بداية من خلال أبرزا الاركان المكونة، فهي تقوم كغيرها من الجرائم على أركان عامة حيث يتجسد الركن المادي في فعل اختلاس المال المعلوماتي والذي أثار جدلا فقهيا كبيرا حول مدى اعتباره سلوكا إجراميا لجريمة السرقة الرقمية. وباعتبار آن جريمة السرقة الرقمية جريمة عمدية فلا بد من توافر القصد العام والقصد الخاص لقيام الركن المعنوي، اما بالنسبة الى الاركان الخاصة فهي تتميز بركن مفترض يضفي عليها طابع الخصوصية والمعبر عنه بمحل جريمة السرقة الرقمية او المال المعلوماتي، كما قمنا بتبيان موقف الانظمة القانونية المقارنة على اختلاف توجهها وصولا بذلك الى موقف المشرع الجزائري من هذه الجريمة، ومن خلال دراستنا مدى تطبيق القواعد الموضوعية لسرقة التقليدية على جريمة السرقة الرقمية، وكذا العقوبات المنشورة لها في ظل القوانين الخاصة ومن خلال ما سبق ذكره نستنتج أن جريمة السرقة الرقمية لها نفس خصوصية الجرائم المعلوماتية من حيث الإثبات واجراءات التحقيق واساليب التحري. الخاصة، كما يمكن تطبيق نصوص السرقة التقليدية على جريمة السرقة الرقمية، الا ان هذه النصوص غير كافية لمواجهة هذه الظاهرة الاجرامية لذلك.

لجأ المشرع الجزائري لإدراج قوانين خاصية لمكافحة هذه الجريمة الماسة بالذمة المالية الرقمية للأشخاص، كما استحدث المشرع هياكل وطنية خاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال بالإضافة الى تعزيز دور التعاون الدولي في إطار، مكافحة الجرائم الالكترونية عامة والسرقة الرقمية خاصة.

خاتمة

خاتمة:

لقد ادى التطور الكبير والمتسارع للوسائل التكنولوجيا الحديثة والتحول الى العالم الرقمي لخلق مجموعة من أخطر جرائم التي يشهدها العالم اليوم والتي باتت تهدد مختلف فئات المجتمع دون استثناء، وتعد جريمة سرقة الرقمية جريمة الإلكترونية حديثة نتجت عن سوء استخدام التطور التكنولوجي في المجال المالي، حيث تتجسد هذه الجريمة في اختلاس المال المعلوماتي في البيئة الرقمية.

وبعد دراسة موضوع البحث ومحاوله الاحاطة بكل جوانبه الموضوعية والقانونية بدءا بتحديد الاطار الموضوعي لجريمة سرقة الرقمية في الفصل الاول وذلك بالتطرق الى الاحكام العامة لهذه الجريمة، اين تناولنا من خلاله مختلف التعاريف الفقهية والقانونية لجريمه السرقة الرقمية.، اين توصلنا الى عدم اجماع الفقهاء على تعريف موحد لجريمة السرقة الرقمية وذلك يعود اساسا الى اختلاف تحديد نطاق هذه الجريمة خصوصا ان البعض وسع كثيرا من نطاقها واعتبر انها ان كل فعل غير مشروع يكون للحاسب الالي دور فيه وقد تبنى هذا المشرع الجزائري حيث نص على ذلك في القانون09/04 وحدد نطاق الجريمة الالكترونية، بالجريمة التي تمس بالنظام المعلوماتي او اي جريمة ترتكب، او يسهل ارتكابها عن طريق المنظومة المعلوماتية او نظام الاتصالات.

ومن خلال هذا تم تبيان خصائص هده الجريمة السرقة الرقمية التي جعلتها ذا الطابع خاص تنفرد به عن جريمة سرقه التقليدية بالإضافة الى ابراز الدوافع المؤدية لارتكاب هذه الجريمة وتتجسد سرقه المال المعلوماتي في البيئة الرقمية باستخدام العديد من التقنيات إذا تعدد التطبيقات السرقة الرقمية باختلاف صور الاعتداء عليها.

ولقد حاولنا كذلك من خلال هذه الدراسة الإحاطة في الفصل الثاني بالتنظيم القانوني لجريمة السرقة الرقمية اين تناولنا في هذا الفصل اركان جريمة السرقة وفقا للمبادئ العامة، وهي الركن المادي المتمثل في فعل الاختلاس والتبيان التضارب الفقهي حول مدى اعتباره سلوكا اجراميا، وكذلك الركن المفترض المعبر عنه بمحل جريمة سرقه الرقمية او المال المعلوماتي، وباعتبار ان جريمة السرقة الرقمية جريمة عمديه تفرض وجود القصد العام والخاص لقيام الركن المعنوي.

كما قمنا بإبراز موقف الأنظمة القانونية المقارنة من هذه الجريمة وصولا بذلك الى موقف المشرع الجزائري عن مدى امكانية تطبيق النصوص سرقه التقليدية على السرقة الرقمية وكذلك

خاتمة:

العقوبات المقررة لهذه الجريمة المستحدثة في ظل القوانين الخاصة. اما بالنسبة لخصوصيه اثبات جريمة السرقة الرقمية واجراءات التحقيق فلها نفس الخصوصية الجريمة المعلوماتية، من خلال ما جاء به القانون رقم09/04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها فمنح لها خصوصية في التفتيش والضبط والمراقبة الالكترونية واعتراض المراسلات السلكية واللاسلكية وفقا، بما يتماشى مع طبيعة الجريمة المرتكبة في العالم الافتراضي.

ولمواجهه هذا الصنف من الجرائم استحدثت المشرع الجزائري بموجب المرسوم الرئاسي رقم19/172 انشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال والتي كان لها دورا بارزا في اثبات وكشف الجرائم المعلوماتية، كما يستوجب تظافر التعاون الدولي لمكافحه الجرائم الالكترونية وذلك من خلال تبادل المعلومات المتعلقة بالجريمة والمجرمين.

وقد توصلنا من خلال دراستنا الى مجموعه من النتائج التي كانت اجابه عن الإشكالية التي طرحناها سابقا وهي كالتالي:

النتائج:

1 –ان جريمة السرقة الرقمية جريمة مستحدثة وهي من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال.

2–عدم وجود تعريف او مفهوم موحد للجريمة السرقة الرقمية وكذا صعوبة حصرها لتعدد مجالات ووسائل ارتكابها.

3–جريمة السرقة الرقمية ذات طابع دولي عابره للحدود الوطنية فهي عالمية الوجود.

4 –تختلف الاموال في جريمة السرقة الرقمية عن جريمة سرقة التقليدية من مال مادي الى اموال معنوية.

5–تتمتع هذه الجريمة بخصائص تختلف عن خصائص جريمة سرقه التقليدية.

6–صلاحيه المعلومات الرقمية لتكون محل السرقة لان الاموال المعنوية والمعلوماتية اصبحت تشكل قيمة مالية تفوت الاموال المنقول والعقارات.

7–جريمة السرقة الرقمية جريمة عمدية تتطلب توفر قصد الجنائي العام والخاص لقيام الركن المعنوي.

8_ تتسم هذه الجريمة بالغموض حيث يصعب اثباتها والتحقيق فيها مما يضع مسؤولية كبيره على ضباط الشرطة والقضاء.

9-نقص الخبرة لدى الأجهزة الأمنية فيما يتعلق بثقافة الحاسب الالي وهذا راجع الى نقص وسائل التكنولوجيا التي تساعد في الكشف عن الجرائم الإلكترونية وملاحقه مرتكبيها

10-وسائل التحقيق التقليدية لا تتناسب مع هذا النوع من الجرائم المستحدثة كونها تتم في العالم الافتراضي وقد لا يترك الجاني اثارا ملموسه

11- عدم اقرار المشرع نصوصا خاصه للمجال المعلوماتي في إطار قانون العقوبات بل اعتبرها من الجرائم الدخول او البقاء غير مشروع والتي بينها في ال ماده394 من قانون العقوبات الجزائري وبالتالي امكانيه زيادة الجرائم الواقعة على الاموال الإلكترونية

12- قام المشرع الجزائري بمكافحه الجريمة الإلكترونية على غرار باقي الدول بموجب تعديل قانون العقوبات رقم04/15، حيث اعتبر الدخول غير مشروع للنظام المعلوماتي والبقاء فيه والمساس بمنظومة معلوماتية وبعض الافعال الاخرى افعال اجرامية وسطر لها عقوبات، واستدرك النقص في المجال الاجرائي بإصدار قانون09/04 اذ تضمن قواعد اجرائية واخرى وقائية وهذه خطوه ايجابيه الا انها غير كافيه لمواجهه خطر جريمة السرقة الرقمية

13- المشرع الجزائري لم يقم بتحديد الجريمة المرتكبة باستخدام النظام المعلوماتي وترك المجال واسعا ليدخل في نطاقها كل ما تفرزه التقنية الجديدة وتطوراتها.

14- تخضع جريمة سرق الرقمية الى نفس القواعد الاجرائية التي تخضع لها الجريمة الإلكترونية من اجراءات المعاينة والتفتيش والضبط، واساليب التحري الخاصة.

15-قصور التشريع في مواجهة السرقة الرقمية ودلك بسبب غموض الجريمة.

ومن خلال هذه الدراسة توصلنا الى التوصيات التالية:

1-العمل على ايجاد مفهوم او تعريف موحد للجريمة السرقة الرقمية، واضافه نص جديد الى جانب النصوص التي استحدثها المشرع الجزائري يجرم سرقه المعطيات الرقمية من اجل حل اشكالات القانونية التي صارت بشأنها نتيجة قصور ال ماده 350ق ع

2-العمل على اسراء ال قانون09/04 المتضمن القواعد الخاصة للوقاية من الجرائم الإلكترونية ببعض المواد القانونية لتجنب الوقوع في اي ثغره قانونيه من شانها فتح المجال للمجرمين للإفلات من العقاب.

3-وضع اليات ردعيه تتماشى مع التطورات الحاصلة من خلال فتح المجال لأصحاب الخبرات من خارج القطاع الامني للمشاركة في مكافحة الجريمة الكترونيه.

4-رفع مستوى التكوين بالنسبة للقضاة ورجال الضبطية القضائية في مجال المعلوماتي من اجل خلق قضاء متخصص حول الجرائم المعلوماتية ومواجهتها بشكل أفضل.

5-افراد نصوص قانونية خاصة ينظم التعامل بالأموال الالكترونية لكل جريمة على حد بدلا من اعتبارها جرائم دخول غير مشروع او بقاء غير مشروع وهذا نتيجة لخطورة هذه الجرائم

6-عقد حملات توعوية للأفراد في المجتمع حول كيفية حماية حياتهم الخاصة عند استخدامهم للأجهزة المعلوماتية.

7-توعيه المجتمع والجهات الخاصة والحكومة بأهمية الابلاغ عن اي عمليه مشبوهة او مخالفه للقانون عند رصدها في الشبكة المعلوماتية

8-تخصيص مواقع رسمية للإبلاغ عن الجرائم الإلكترونية بمختلف انواعها واللجوء الى تفعيل التعاون الدولي الذي يعد من اهم سبل مكافحة وملاحقة

قائمة المصادر والمراجع

قائمة المصادر:

1_ معجم:

جمال الدين بن فضل الافغاني، محمد بن كرم بن منظور الانصاري، لسان العرب دار. بيروت 1996.

2_ القوانين:

أ- القوانين العادية:

1. قانون رقم 04-15 مؤرخ في 10 نوفمبر 2004 يعدل الأمر رقم 66-156 المدرج في قانون العقوبات
2. القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال
3. المادة 16 من القانون 09-04 المؤرخ في 05 اوت 2009 المتضمن القواعد الخامسة للوقاية من الجرائم المتعلقة بتكنولوجيا الاعلام والاتصال ومكافحتها، ج.م، ج. د.س، العدد 47 المؤرخة في 16 اوت 2009
4. انظر المادة 64 والمواد 44الى 47 من القانون رقم 06_22 المؤرخ في 20 ديسمبر 2006معدل ومتمم رقم 66_155 ج.م، ج د ش العدد 84 الصادر في 24 ديسمبر 2006
5. المادة الأولى من القانون رقم 09_04 المتضمن القواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها

ب- الأوامر:

1. الأمر 05/03 المتعلق بحقوق المؤلف والحقوق المجاورة. الصادر بتاريخ 23/7/2003 الموافق ل 23 جمادى الأولى عام 1424 هجري الموافق عليه بالقانون 03/17 الجريدة الرسمية رقم 44
2. الأمر رقم 03-05 مؤرخ في 19 جمادي الأولى عام 1412 الموافق 19 يوليو سنة 2003 يتعلق بحقوق المؤلف والحقوق المجاورة
3. الأمر رقم 04-15 المؤرخ في 10 نوفمبر 2004 المكمل والمعدل للأمر رقم 66-156 المتضمن قانون العقوبات

د-المراسيم التنظيمية:

1. المرسوم الرئاسي رقم 15-261 المؤرخ في 8 اكتوبر 2015 يحدد تشكيل وتنظم وفقرات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا

الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، عدد 53 الصادر في ل 8 أكتوبر 2015

2. مرسوم رئاسي رقم 19-172 مؤرخ في 3 شوال عام 1440 الموافق 6 يونيو سنة 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وتنظيمها وكيفيات سيرها

3. المادة 05 من المرسوم الرئاسي رقم 19-172 المتعلق بتحديد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

4. لمادة 06 من المرسوم الرئاسي رقم 19-172 المتعلق بتحديد تشكيلة الهيئة الوطنية للوقاية من الجرائم الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها.

5. المادة 09 من المرسوم الرئاسي رقم 19-172 المتعلق بتحديد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها

6. المادة 15 من المرسوم الرئاسي رقم 19-172 المتعلق بتحديد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

. مرسوم رئاسي يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، مقالة منشورة بالموقع http://www.aps ds"

- **قائمة المراجع بالغة العربية:**

1. الكتب العامة:

1. ابتسام سمير طاهر، جريمة السرقة الإلكترونية، جامعه نايل للعلوم الاستشرافية، مجلد 27، العدد خمسه، 2019.

2. ابراهيم بعمليات، أركان الجريمة وطرق اثباتها في القانون الجزائري، د.ت، دار الخلدونية النسر والتوزيع، الجزائر

3. إبراهيم السنوسي نصر، مقدمة للإنترنت البرنامج التمهيدي للتدريب على استخدام الحاسوب والانترنت، جامعة سبها مكتب التدريب 2015

4. أحسن بوقيعة، الوجيز في القانون الجزائي الخاص، الجزء الاول، الطبعة الثالثة، دار هومة للطباعة والنشر، الجزائر، 2005

5. احمد خليفه، جرائم المعلوماتية، طبعه 2، دار الفكر الجامعي الإسكندرية.

6. احمد عبد الرؤوف المنيفي، السرقة الإلكترونية وحكمها في الاسلام، طبعه1، 2017،

7. احمد محمد عبد الرؤوف المنيفي، فيروسات الحاسب الآلي، اليمن، 2019
8. احمد عزمي الجروب السندات الرسمية الالكترونية، ط1، دار الثقافة للنشر والتوزيع، عمان, 2010
9. اختير مسعود، الحماية الجنائية لبرامج الحاسوب وأساليبه ونقاط ضعفه، دار الهدى، عين مليلة، الجزائر، طبعة 2010
10. اسامة أحمد المنارة، جلال محمد الزغبي، جرائم تقنية نظام المعلومات الالكترونية، الطبعة الثالثة، دار الثقافة النسر والتوزيع،
11. أسامة فتحي، فيروسات الحاسوب، دون بلد النشر، 2014
12. أيمن عبد الله فكري، الجرائم المعلوماتية دراسة مقارنة في التشريعات العربية والأجنبية، معهد الإدارة العامة، الطبعة الأولى، الرياض
13. تركي بن عبد الرحمن، بناء نموذج أمنى لمكافحه الجرائم المعلوماتية وقياس فعاليته، دار الجامعة نايف للنشر، الرياض 2012
14. جميل عبد الباقي الصغيرة الحماية الجنائية والمدنية البطاقات الائتمان الممغنطة، دار النهضة العربية، القاهرة,1999
15. حسين محمود الشيلي، مهد فايز الدويكات، التزوير والاحتيال البطاقة الائتمان، الطبعة الأولى، دار مجدلاوي للنشر والتوزيع – عمان، 2009
16. خالد حياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، ط1، عمان, 2011،
17. خالد ممدوح ابراهيم، امن الجريمة الإلكترونية، طبعه واحد دار الجامعية الإسكندرية، 2008
18. سلامه محمد عبد الله، موسوعة الجرائم المعلوماتية جرائم الكمبيوتر والانترنت منشئه المعارف الإسكندرية، 2006
19. عمر عبد القادر، تحديات القانونية لأثبات الجريمة المعلوماتية، دار النشر الجامعي الجديد، تلمسان الجزائر، 2021
20. عماد علي الخليل، الحماية الجزائية لبطاقة الوفاء دراسة تحليلية مقارنة، طبعة الأولى، دار–وائل–للنشر، عمان, 2000
21. عصام عبد الفتاح مطر، التجارة الالكترونية في التشريعات العربية والأجنبية، دار الجامعة الجديدة، الإسكندرية, 2009
22. على حسن عباس مخاطر استخدام بطاقات الدفع الالكتروني عبر شبكة الإنترنت (المشاكل والحلول، ورقة عمل مقدمة إلى ندوة الصور المستحدثة لجرائم

بطاقات الدفع الالكتروني الت نظمها مركز بحوث الشرطة بأكاديمية الشرطة القاهرة 14/12/1998

23. عمر أبو الفتوح عبد العظيم الحمامي، العمالية الجنائية للمعلومات المسجلة الكترونيا، بدون طبعة، دار النهضة العربية. 560 2010

24. غازي حنون خاف الدراجي، استظهار القصد الجنائي في جريمة القتل العمد، ط1، منشورات الحلبي الحقوقية – لبنان ،2012

25. غانم مرضي، الجرائم المعلوماتية، ماهيتها، خصائصها، كيفية، التصدي لها قانونا، دار الطيبة الدولية للنشر والتوزيع، عمان، الأردن, 2016

26. فؤاد حسين العزيري، جرائم المعلوماتية، طبعه واحد، دار الفكر الجامعي الإسكندرية

27. معز خليل العمر، جرائم مستحدثه، الطبعة الاولى، دار وائل للنشر والتوزيع، عمان 2012

28. محمد نجيب حسني، شرح قانون العقوبات، القسم الخاص، ط 6، دار النهضة العربية القاهرة، د.س.ن

29. محمود مصطفى، شرح قانون العقوبات، قسم الخاص، ط 8، جامعة القاهرة، 1994

30. محمد الطيب عمور، السرقة الإلكترونية تكييفها الدرعي وطرف أثبتها مجال الاحياء، جامعه نسيبه بن بوعلي شلف، المجلد 19 العدد 22.

31. منير محمد الجنيبي، صعوبات التحقيق واستخراج الأدلة في جرائم المعلومات، ط1، دار الفكر الجامعي، الإسكندرية,2018

32. معز خليل العمر، جرائم مستحدثه، الطبعة الاولى، دار وائل للنشر والتوزيع، عمان 2012

33. محمد حسين منصور المسؤولية الالكترونية دار الجامعة الجديدة: الاسكندرية – مصر. 2009 .

34. نائلة عادل محمد فريد قوره، جرائم الحاسب الاقتصادية، دراسة نظرية وتطبيقية، دار النهضة العربية، القاهرة, 2004

35. نائلي لحسن، التحقيق في الجرائم المتصلة بتكنولوجيا المعلوماتية (بين النصوص التشريعية والخصوصية التقنية)، النشر الجامعي الجديد، الجزائر, 2017

36. نائلة عادل محمد بوره، جرائم الحاسب الالي الاقتصادي، الطبعة الاولى، منشورات الحلبي الحقوقية، بيروت، 2005

37. نهله عبد القادر المومن، جرائم المعلوماتية، الطبعة 2، دار الثقافة للنشر والتوزيع، عمان 2010

38. وسام فيصل محمود الشواورة، المسؤولية القانونية عن استخدام غير المشروع لبطاقات الوفاء، الطبعة الأولى، دار –وائل–للنشر، عمان, 2013

39. سليمان أحمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، القاهرة, 2007

40. عبد الرحمان عبد الله سند، الاحكام الفقهية للتعاملات الالكترونية (الحاسب الالي وشبكة المعلومات الانترنت)، دار الورق، الطبعة الأولى, 2004

41. محمد سعد، عالم القرصنة، حقوق الطبع والنشر, 2020

عبد الرحمن عبد الله السند الأحكام الفقهية للتعاملات الالكترونية الحاسب الآلي وشبكة المعلومات الانترنت، دار الورق، الطبعة الأولى 1424هـ، 2004

43- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، ط1، دار نشر، عمان

44- خالد عياد الحلبي، إجراءات التحري والتحقيق وجمع الأدلة في جرائم الحاسوب والانترنت، طبعة الأولى، دار الثقافة، الأردن, 2011

45- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، ط1، دار الفكر الجامعي، الإسكندرية، مصر ,2009

- **رسائل الدكتورة:**
- **رسائل الدكتورة المحلية**

43- رابحي عزيزة، أسرار المعلومات وحمايتها الجنائية. أطروحة ليني. شهادة الدكتوراه في القانون الخاص، جامعة أبو بكر بلقايد، تلمسان، 2018

44- فايز محمود راجع غلاب، الجرائم المعلوماتية في القانون الجزائري واليمني، أطروحة دكتورة كلية الحقوق جامعة الجزائر , 1 , 2009

45- البدري فيصل، مكافحة الجرائم الإلكترونية في القانون الدولي والداخلي. أطروحة للحصول على درجة الدكتوراه في القانون العام من جامعة الجزائر وحيد بني خدام. , 2018

46- بوري أحمد، الحماية القانونية لحق المؤلف والحقوق المجاورة في التشريع الجزائري والاتفاقيات الدولية. أطروحة لنيل درجة الدكتوراه في العلوم القانونية في القانون الجنائي، جامعة باتنة 2015

47- بدري فيصل، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة لنيل شهادة الدكتورة في قانون عام، جامعة الجزائر 1 بن يوسف بن خدة 2018

48- رابحي عزيزة، الاسرار المعلوماتية وحمايتها الجزائية، أطروحة لنيل شهادة الدكتورة قانون خاص، جامعة ابوبكر بلقايد، تلمسان,2018

49- هروال هبة نبيلة، جرائم الانترنت دراسة مقارنة، أطروحة دكتورة، جامعة ابي بكر بلقايد، تلمسان, 2014

- **مذكرات الماجيستر المحلية**

1. دحمان صبيحه خديجة، جرائم السرقة والاغتيال عبر الانترنت دراسة مقارنه بين الفقه الاسلامي والقانون الجزائري، مذكره الماجيستير، كليه العلوم الإسلامية، جامعه الجزائر يوسف بن خدام، 2013
2. در دور نسيم، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، مذكرة لنيل شهادة الماجستير في القاء جامعة منتوري، قسنطينة 2013
3. سوبر سفيان، جرائم المعلوماتية، مذكرة مقدمة للحصول على درجة الماجستير تخصص العلوم الجنائية وعلم الإجرام، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد تلمسان ,2010
4. سعيد علي نعيم، اليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة لنيل شهادة الماجيستر تخصص علوم جنائية كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، الجزائر, 2012
5. سعيد علي نعيم، اليات البحث والتحري عن الجرائم المعلوماتية في القانون الجزائري، مذكرة ماجيستر، جامعة الحاج لخضر باتنة، كلية الحقوق والعلوم السياسية، قسم الحقوق, 2012
6. سمية مزغيش، جرائم المساس بنظم المعلومات، مذكرة تكميلية لمتطلبات الحصول على درجة الماجستير في القانون الجنائي جامعة محمد خضر، بسكرة 2014.
7. صغير يوسف، الجريمة المرتكبة عبر الإنترنت: مذكرة للحصول على درجة الماجستير في قانون الأعمال الدولي، جامعة مولود معمري تيزي وزوو، 2013

8. صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة الماجيستر في القانون الدولي للأعمال، جامعة مولود معمري، تيزي وزوو

9. عبد الله دعش العجمي، المشكلات العملية والقانونية للجرائم الالكترونية دراسة مقارنة، رسالة استكملا للحصول على درجة الماجستير في القانون العام مجامعة الشرق الأوسط 2014

10. عبد الله ماجد عبد المطلب العكايلة، سرقة البيانات والمعلومات الإلكترونية، دراسة مقارنة، كلية العلوم والإنسانيات، جامعة الأمير سطام بن عبد العزيز

11. عمر علي نايت الملكية الفكرية في إطار التجارة الالكترونية. مذكرة مقدمة لنيل درجة الماجيستر في الأستاذة يسعد حورية. كلية الحقوق. جامعة مولود معمري تيزي وزوو تاريخ المناقشة 15/3/2014

12. فاطمة الزهراء خبازي، جرائم الدفع الالكتروني وسبل مكافحتها، أعمال الملتقى الوطني البات مكافحة الجرائم الالكترونية في التشريع الجزائري الجزائر 29 مارس 2017 جامعة الجيلالي بونعامة، خميس مليانة

13. فتيحة مهري، جريمة الدخول والدخول إلى أنظمة معالجة البيانات، تذكير للحصول على شهادة الماجستير في القانون الجنائي، وقائع جامعة العربي بن مهيدي، أم البواقي، 2016

14. معتوق عبد اللطيف الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن مذكرة مقدمة لنيل درجة الماجستير في العلوم القانونية تخصص القانون الجنائي جامعة باتنة 2012

15. ياسين بن عمر جرائم تقليد المصنفات الأدبية والفنية واليات مكافحتها. مذكرة مقدمة لنيل درجة الماجيستر. تخصص قانون جنائي إشراف الأستاذ بن محمد. كلية الحقوق جامعة ورقلة قاصدي مرباح. السنة الجامعية 2010/2011

- **رسائل الماجيستر الأجنبية**

1. تركي بن عبد العزيز بن تركي ال سعود، سرقه الإلكترونية بين الحذر والتعزيز، مذكره لنيل شهادة الماجستير الأكاديمية نايف العربية للعلوم الأمنية، الرياض، 2011

- **مقالات علمية**

1- ممدوح حسن مانع العدوان، نادر عبد الحليم السلامات، مشروعية وحجية الدليل المستخلص من التفتيش الالكتروني في التشريع الجزائري الأردني، مجلة دراسات علوم

الشريعة والقانون، كلية الشريعة والقانون، جامعة العلوم الإسلامية العلمية، المجلد 45، العدد 04, 2018

2- هشام رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي، مجلة الامن والقانون، دبي الامارات العربية المتحدة، العدد الثاني، 1999

3- صالح شتين، إجراءات التحري والتحقيق في جرائم تكنولوجيا الاعلام والاتصال في التشريع الجزائري، مجلة الدراسات القانونية، جامعة عبد الرحمان ميرة، بجاية، الجزائر، العدد 01.

4- أنسام سمير طاهر، جريمة السرقة الالكترونية، مجلة جامعية بابل العلوم الإنسانية، المجلد 27، العدد 5.

5- رحال بومدين، سعداني نورة، الحماية الجنائية الواقعة على اموال التجارة الالكترونية، جريمة السرقة والنصب، مجلة الواحات للبحوث والدراسات، المجلد 9، العدد 2، 2016.

6- عبد الصديق آل الشيخ، منع الجرائم الإلكترونية بموجب القانون رقم 04.09 يتضمن قواعد خاصة لمنع الجرائم المتعلقة بتقنيات الإعلام والاتصال ومكافحتها مجلة المعالم للدراسات القانونية والسياسية، المجلد الرابع، العدد الأول, 2020.

7- محمد نصير محمد مشكلات الحماية الجنائية لبرامج الحاسب الآلي (دراسة مقارنة)، مجلة قضائية، العدد الثامن، محرم 1425هـ.

8- ابراهيم رمضان ابراهيم، الجريمة الإلكترونية، سبل مواد في الشريعة الإسلامية والأنظمة الدولة، مجله كليه شريعة القانون موجب 30، العدد 2.

9- براهيمي جمال، مكافحة الجرائم الإلكترونية في التشريع الجزائري، مجلة النهضة، كلية العلوم والعلوم السياسية، جامعة مولود معمري، تيزي وزوو.

10- سالم بن حمزة المدني، مدى امكانيه تطبيق حدود على الجرائم الإلكترونية، مجله المجار العالمية المحكمة للدراسات الإسلامية والعربية، مجلد سته العدد 1، سنة، 2014.

11- هشام محمد رستم، الجرائم المعلوماتية اصول التحقيق الفني مجله الامن والقانون، دبي، العدد 2، 1999.

12- محمد موسى، تنازع الاختصاص في الجرائم الالكترونية، مجلة دفاتر السياسة والقانون، جامعة قاصدي مرباح، ورقلة، ال عدد2 سبتمبر 2009،

- **المواقع الالكترونية**

1- انظر موقع الكتروني: https://www.mlzamty.com/virus-damage يوم الاطلاع على الساعة 48:22 -23/4/2021.

2- معاني المعاجم, المقال منشور على الموقع: https://www.almaany.com تم نظر اليها يوم 22 ماي 2023 على الساعة 20:23 مساء

قائمة المحتويات

الفصل الثاني: التنظيم القانوني لجريمة السرقة الرقمية.

ملخص:

نتيجة للاستعمال الواسع لتكنولوجيا الاعلام والاتصال الحديثة في شتى مجالات الحياة خاصة مجال المعاملات المالية ،استحدثت جريمة السرقة الرقمية والتي اثارت جدلا فقهيا كبيرا حول طبيعتها و محل وقوعها، كما تميزت بخصائص جديدة لم تعرف في ظل جريمة السرقة التقليدية ، فبرزت سلبيات الوسائط الإلكترونية بأن اصبحت وسيلة لارتكاب المجرم المعلوماتي جرائم السرقة وعلى عكس هذا التطور السريع في أساليب ارتكابها فإن الحماية القانونية لجريمة السرقة الرقمية، لم تكن كذلك بل نجد أن موقف المشرع الجزائري كان غير واضح فلم ينص عليها صراحة الا انه أضفى حماية للمعلومات من خلال عدة قوانين كقانون 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها وبالتالي وفقا للمشرع الجزائري فان جريمة السرقة الرقمية هي جريمة السرقة المنصوص عليها في قانون العقوبات الجزائري ، أما فيما يخص الحماية الإجرائية فتظهر خصوصيتها من خلال تنظيم الاجراءات التقليدية للبحث والتحري وفقا لما يتماشى مع طبيعة محل هذه الجريمة، كما كرس المشرع حماية موضوعية ضد هذه الجريمة، وفق ألية مؤسساتية تتمثل في انشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال منصوص عليها في المرسوم الرئاسي 19-172.

-**الكلمات المفتاحية:** السرقة الرقمية , المجرم المعلوماتي ، الوسائط الالكترونية، المال المعلوماتي.

Summary:

As a result of the widespread use of modern information and communication technology in various areas of life, especially the field of financial transactions, the crime of digital theft was created, which sparked a major jurisprudential debate about its nature and the place of its occurrence. It was also characterized by new characteristics that were not known in light of the traditional crime of theft, so the negatives of electronic media emerged by becoming a means of committing Information criminal theft crimes. In contrast to this rapid development in the methods of committing them, there was no legal protection for the crime of digital theft. Rather, we find that the position of the Algerian legislator was unclear and did not explicitly stipulate it. However, he added protection for information through several laws, such as Law 09-04, which includes the rules. Special measures to prevent and combat crimes related to information and communication technology. Therefore, according to the Algerian legislator, the crime of digital theft is the crime of theft stipulated in the Algerian Penal Code. As for procedural protection, its specificity appears through the organization of traditional procedures for search and investigation in accordance with the nature of the subject, as well as The legislator has established objective protection against this crime, according to an institutional mechanism represented by the establishment of the National Authority for the Prevention of Crimes Related to Media and Communication .Technology, stipulated in Presidential Decree 19-172

Keywords: digital theft, information criminal, electronic media, information money