جامعة أكلي محند أولحاج – البويرة
كلية الحقوق والعلوم السياسية
قسم القانون الخاص

القواعد الخاصة بجريمة السرقة الإلكترونية

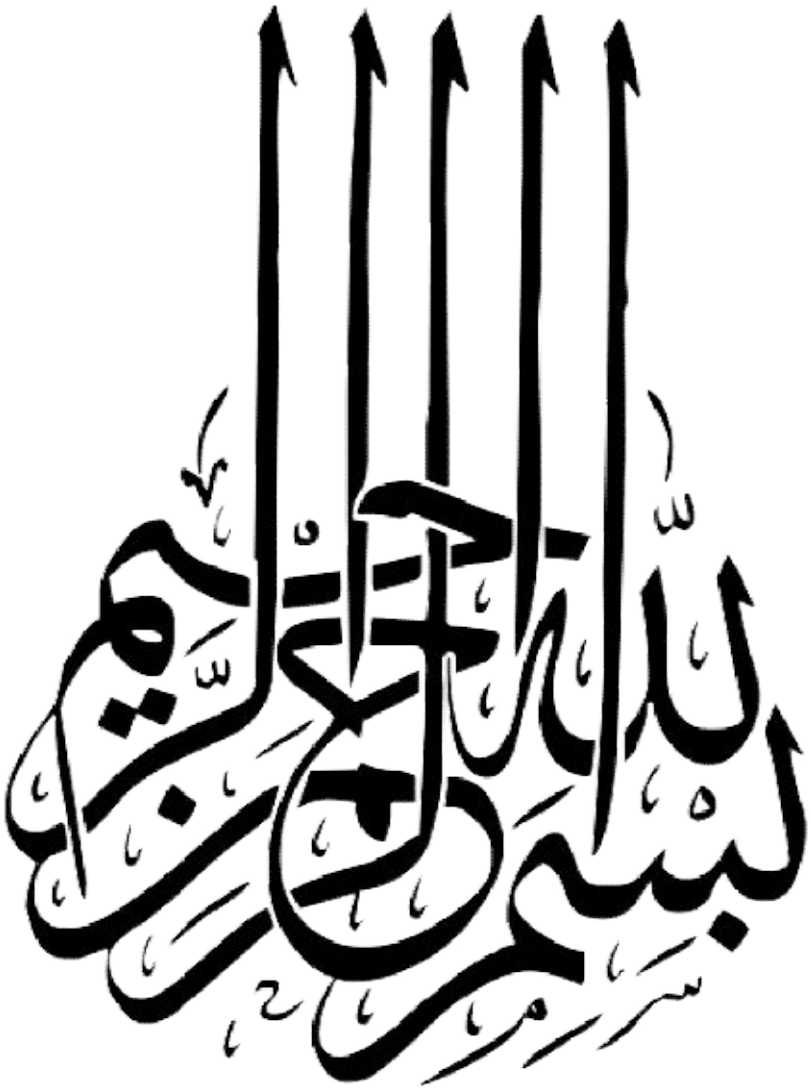
مذكرة لنيل شهادة ماستر في القانون العام
تخصص: القانون الجنائي والعلوم الجنائية

إعداد الطالبة: إشراف الأستاذ:
❖ طالب نبيلة – صغير يوسف

لجنة المناقشة

الأستاذ: خليفي سمير	رئيسا .
الأستاذة:- صغير يوسف	مشرفا ومقررا
الأستاذ: بوعمامة زكريا	ممتحنا

السنة الجامعية: 2021/2020.


بسم الله الرحمن الرحيم

شكر وعرفان

أحمد الله الذي أعطني القوة والصبر لإتمام هذا العمل المتواضع، فالحد الله حمدا كثيرا طيبا مبارك فيه، فسهل لي الصعوبات والعقبات.

كما لا يسعني إلا أن أتقدم بجزيل الشكر والامتنان إلى أستاذي الفاضل: صغير يوسف، الذي تكرم عليا بإشرافه وسديد توجهاته القيمة والإرشاد والنصح إلى غاية إتمام هذا البحث رغم مشاغله الكثيرة، واسأل الله أن يجزيه خير الجزاء،

كما اشكر أعضاء اللجنة الموقرة لقبولهم مناقشة هذه المذكرة وعلى تحملهم عناء مطالعة ومناقشة هذه المذكرة، كما اشكر جميع أساتذة كلية الحقوق والعلوم السياسية بجامعة البويرة على المجهدات التي بذلوها من أجلنا، وجزاهم الله كل خير.

وكل من يعمل بالإدارة، قدمت لهم من التقدير والاحترام والشكر وصادق وأطيب الدعوات.

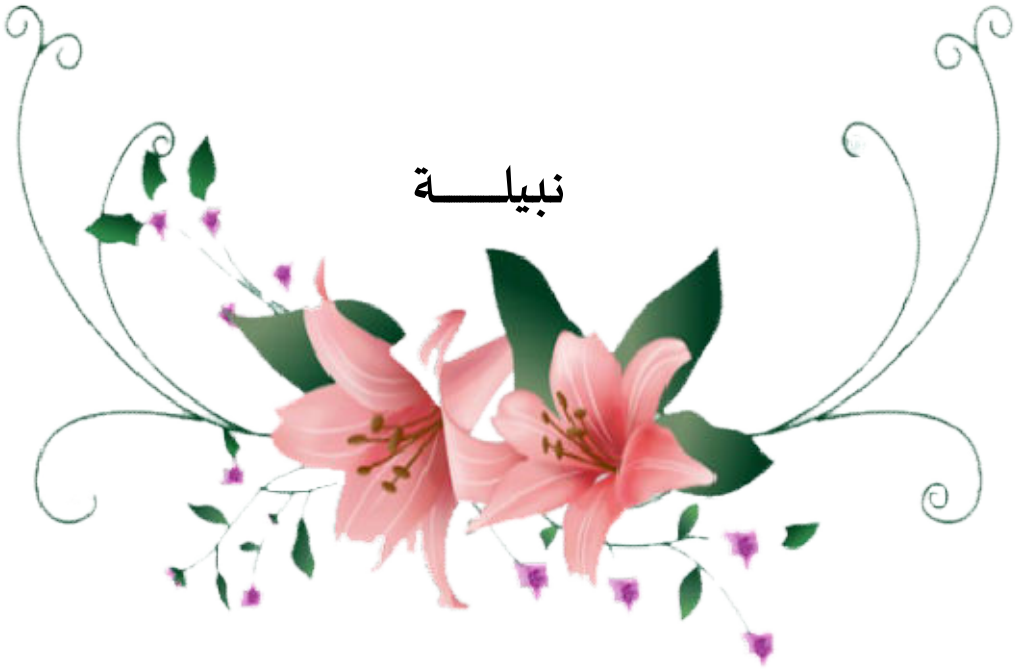
نبيلـــــة

الإهداء

الحمد لله وكفى والصلاة على الحبيب المصطفى وأهله وأما بعد: الحمد لله الذي وفقني لتكملة هذه الخطوة في مسيرتي الدراسية بمذكرتي هذه، هذه ثمرة الجهد والنجاح بفضله تعلى مهداة:

إلى من لا يمكن للكلمات أن توفي حقها و من أوصاني بهما ربي برا وإحسانا والداي العزيزين اللذان ضحيا كثيرا في سبيل نجاحي في مشواري الدراسي حفظهما الله وأدام صحتهما وعافيتهما، كما اهديه إلى إخواني وأختي الذين ساعدوني بنصائحهم وساعدوني بكتابة المذكرة رعاهم الله، وإلى عائلتي الكريمة سواء أحياء ومن غادروا هذه الدنيا إلى دار الحق رحمة الله عليهم، وإلى كل من ساندني و نصحني ولو بكلمة. وكل من يتمنى لي النجاح.

نبيلـــــة



مقدمة

مقدمة:

شهدت السنوات الأخيرة تطورا علميا وتقنيا في شتى مناحي الحياة، ومن بين ما يشهده العالم من مستحدثات تكنولوجية ما يعرف بالشبكة المعلوماتية. بحيث تسارع إيقاع التكنولوجي والتقني الهائل وظهور الفضاء الالكتروني ووسائل الاتصالات الحديثة كالفاكس والانترنت، وكل هذا بفضل اختراعات هائلة على المستوى التقني.

ولهذا يوصف العصر الذي نعشه بعصر التقنية المعلومات والاتصالات، وظهور انتشار استعمال الكمبيوتر واستحداث شبكات المعلومات. وبالمقابل نجد العلماء والصالحون يحاولون الاستفادة منها، وبالمقابل نجد أن المجرمين يحاولون الاستفادة أيضا من التقدم التكنولوجي، من اجل استغلال مرتكبو الجرائم الالكترونية في تنفيذ جرائمهم التي لم تعد تقتصر على إقليم الدولة واحدة، بل تجاوزت حدود الدول، وهي جرائم مبتكرة ومستحدثة تمثل ضربا من ضروب الذكاء الإجرامي.

وعلى الرغم من مزايا الكثيرة الناتجة عن التطور العلمي الهائل، إلا انه تترتب عليها مخاطر عدة. ناجمة عن إساءة استخدام شبكة المعلومات الدولية، لصالح المجرمين لممارسة نشاطاتهم الجرمية حيث أسهمت في ظهور طائفة جديدة من الجرائم المستحدثة، ومن بينها جريمة السرقة الالكترونية. وعليه ترتبط جريمة سرقة المعلومات ارتباطا وثيقا بمدى اعتماد المجتمع ومؤسساته المختلفة على المنظمة في القطاعات المختلفة، لهذا زادت فرص ارتكاب جريمة المعلوماتية، وقد تفننوا في ارتكاب المشروعة. مثل هذه الجرائم وذلك عن طريق ابتداع أساليب مبتكرة لتنفيذ جرائمهم. بحيث يستغلون، في هذا المجال قدراتهم ومعرفتهم من اجل القيام بنشاطاتهم الإجرامية الغير، وتمتاز خطورة هذه الجريمة ذات الخصائص متعددة، لا تتوفر في جريمة التقليدية، الأمر الذي يهدد مصالح الأفراد والمؤسسات المالية والأمن القومي والسيادة الوطنية وفقدان الثقة بالتقنيات الحديثة. وأيضا العديد من الأشخاص يتعرضون لهذا النوع من القرصنة على المواقع التواصل الاجتماعي.

كلما زاد استخدام الانترنت في الحياة الشخصية أو المهنية ازدادت مخاطرها، وبما أنا ظاهرة الإجرام الالكتروني تتعلق بكل سلوك غير مشروع أو غير مسموح، فانه اوجب تطوير البنية التشريعية الجنائية، الوطنية بذكاء تشريعي مماثل تعكس فيه الدقة الواجبة على المستوى القانوني. إن جرائم سرقة الالكترونية المخزنة في الحاسب الآلي تعتبر من الجرائم التي تتميز

بالحداثة، وذلك نظرا لارتباطها بتكنولوجيا متطورة هي تكنولوجيا المعلومات، الأمر الذي جعلها تتسم بمجموعة من الخصائص والسمات الخاصة.

أهمية الموضوع:

- يعد موضوع البحث من الموضوعات المهمة والجديدة والذي لا يزال محل دراسة وتمحيص على الصعيد الفقهي.
- وما لا يمكن إنكاره هو الآثار التي تخالفها هذه الجريمة من سلبيات وتكمن خطورتها كونها تمس كثيرا من مصالح المجتمع.
- بحيث أصبحت ظاهرة عالمية تهدد الأفراد والدول وتهدد الأنشطة الفردية والدولية. وتعد هذه الجريمة من الجرائم المعلوماتية الحديثة التي تفرض نفسها على المستوى الوطني والدولي، على حد سواء.

أسباب اختيار الموضوع:

إن اختيار موضوع **جريمة** السرقة الالكترونية جاء بسبب عدة أسباب منها ذاتية وأخرى موضوعية تتمثل فيما يلي:

الأسباب الذاتية:

تتمثل في ميولي ورغبتي بدراسة هذا النوع من المواضيع وبدقة الاطلاع وكسب المعرفة اللازمة في مجال الجرائم المستحدثة.

الأسباب الموضوعية:

تظهر أهمية هذا الموضوع كونها من الجرائم الخطيرة الأكثر انتشارا تحتاج الكثير من البحث والدراسة.

محاولة إعطاء فكرة عامة حول مدى انطباق نصوص الجريمة التقليدية عليها.

تعتبر من الجرائم المستحدثة وما تتمتع به من صبغة تقنية وعلمية تجعلها دخيلة على رجال القانون.

الإشكالية:

هل النصوص المنظمة لجريمة السرقة الواردة في قانون العقوبات الجزائري تكتفي لمواجهة سرقة الالكترونية أم أنها عاجزة أمام القيد الذي يفرضه؟

التساؤلات:

- ما هي جريمة السرقة الالكترونية؟
- وما هي التعاريف التي أوردها الفقه القانوني لها؟
- وما هي الخصائص المميزة لها؟
- إذا كان يعاقب قانون العقوبات الجزائري لجريمة السرقة الالكترونية، فما هي هذه العقوبات؟
- إذا كانت تتكون من مراحل ما هي هذه المراحل؟

النهج المتبع:

للإجابة على هذه الإشكالية على هذه الإشكالية ونظرا لطبيعة البحث اتبعت منهجين:

المنهج التحليلي: الذي يتناسب مع طبيعة الموضوع وذلك بتحليل النصوص القانونية المنظمة لجريمة السرقة.

والمنهج الوصفي: نظرا لما يحتويه هذا البحث من مصطلحات متعلقة بجريمة سرقة الالكترونية وذلك وفقا الخطة التالية:

اعتمدت على خطة ثنائية، بحيث قمت بتقسيم الخطة إلى فصلين، كالتالي:

- الفصل الأول: ماهية الجريمة السرقة الالكترونية الذي قسمته إلى مبحثين، وفي المبحث الأول نبين فيه مفهوم جريمة السرقة الالكترونية، ونتطرق إلى دوافع وتقنيات ارتكاب مجرمي جريمة السرقة الالكترونية وأصنافها في المبحث الثاني.
- الفصل الثاني الجوانب القانونية لجريمة السرقة الالكترونية وآليات مكافحتها، الذي قسمته إلى المبحثين. نتطرق فيه إلى أركان جريمة السرقة الالكترونية وتطبيقاتها في المبحث الأول، وفي المبحث الثاني نبين فيه عقوبة جريمة السرقة الالكترونية والوقاية منها.

الفصل الأول

ماهية جريمة السرقة الإلكترونية

الفصل الأول: ماهية جريمة السرقة الالكترونية

لقد شهد في الآونة الأخيرة تطور ملحوظ في مجال التقنية، مما نتج عن استعمال الحاسب الآلي وشبكة الانترنت في جميع الميادين، بحيث يتم استخدام هذه الوسائل بالطرق الغير المشروعة، الأمر الذي أدى إلى ارتكاب الجرائم لها علاقة بهذا المجال، ما يعرف بجريمة الالكترونية. ونظرا لحداثة الجريمة فان دراستنا تتمحور على جريمة السرقة الالكترونية فهي جزء من ظاهرة إجرامية حديثة، ظاهرة إجرام معلوماتي. فالمجرم المعلوماتي فهو يسرق بذكاء وله قدرات ومهارات لتنفيذ النشاط الإجرامي، بحيث أصبحت هذه الجريمة منتشرة وسريعة بكثرة في دول العالم.

وهذا ناتج عن التطور التكنولوجي الذي ساعد مرتكبي جريمة بمهاجمة الحاسب الآلي بطرق مختلفة وسهلة، وليس فقط المحترفين في القرصنة الذين يقومون بهذه الجريمة بل أصبح في وقتنا الحلي لأي شخص عادي بالقيام بالسرقة الالكترونية عبر وسائل التواصل الاجتماعي وهذا راجع إلى الدروس المنتشرة في قنوات يوتيوب والموجودة بكثرة والتي تعلم كيفية إدخال الفيروسات للحاسوب وغيرها.

وعلى ضوء ذلك قسمت الفصل الأول إلى ماهية الجريمة السرقة الالكترونية، وفي هذا الفصل سنحول دراسة مفهوم جريمة السرقة الالكترونية في المبحث الأول، وعليه نستعرض فيه ثلاثة مطالب، أما المبحث الثاني نتطرق إلى دوافع وتقنيات ارتكاب مجرمي جريمة السرقة الالكترونية وأصنافها، بحيث نستعرض فيه مطلبين.وانطلاقا من هذا سنحاول دراسة المفصلة في المبحثين المواليين.

المبحث الأول: مفهوم جريمة السرقة الالكترونية

إن جريمة السرقة الالكترونية تصنف من الجرائم المستحدثة لان الدليل يصعب إيجاده فالسارق في هذه الجريمة يسرق باحترافية لا يترك أي إثر وراءه فهي عكس الجريمة التقليدية الذي يكون الدليل ملموس،ويمكن أن يكون له شهود يشهدون بان فلان هو الذي سرق،وأما الجاني في السرقة الالكترونية يسرقك دون رؤيته، بمعنى أخر انه يسرق عن بعد.

وسنحاول في هذا المبحث الذي قمت بتقسيمه إلى ثلاثة مطالب، بحيث نبين في المطلب الأول تعريف السرقة الالكترونية وصورها، وأما صور جريمة السرقة الالكترونية وتميزها عن القرصنة البريد الالكتروني في المطلب الثاني، ونبين في: مراحل السرقة الالكترونية.

المطلب الأول: تعريف جريمة السرقة الالكترونية وصورها

سنتناول في هذا المطلب المقصود بجريمة السرقة الالكترونية في الفرع الأول، وأما خصائص المميزة لجريمة السرقة الالكترونية في الفرع الثاني، وأخيرا صور جريمة السرقة الالكترونية وتميزها عن القرصنة البريد الالكترونية في الفرع الثالث.

الفرع الأول: المقصود بجريمة السرقة الالكترونية

أولا: تعريف السرقة لغة

السرقة بفتح السن وكسر الراء، من سرق يسرق وهي اخذ الشيء من الغير على وجه الخفية،والسارق هو من جاء مستترا إلى حرز فاخذ مالا لغيره.[1]

ثانيا: تعريف السرقة اصطلاحا:

أ-تعريف السرقة التقليدية اصطلاحا:

نجد تعريفات مختلفة عند المذاهب الفقهية في تعريف السرقة تبعا لاختلافهم في شروطها وأرائهم.

تعريف الحنفية: القول بان السرقة هي اخذ العاقل البالغ نصابا محررا أو ما قيمته نصاب ملكا للغير لا شبهة له فيه على وجه الخفية.[2]

---

[1]- محمد طيب عمور-السرقة الالكترونية: تكيفها الشرعي وطرق إثباتها، مجلة الإحياء، المجلد :19، العدد 22، كلية العلوم السياسية -جامعة حسيبة بن بوعلي - الشلف. ص 405

[2]- محمد الطيب عمور، مجلة الإحياء، المرجع السابق، ص 406.

تعريف المالكية: بقولهم هي اخذ مال الغير مستترا من غير أن يؤتمن عليه[1].

تعريف الشافعية: السرقة هي اخذ المال خفية ظلما من حرز مثله بشروط[2].

تعريف الحنابلة: هي اخذ مال خفية محترم لغيره وإخراجه من حرز مثله لا شبهة له فيه على وجه الاختفاء[3].

من خلال التعريفات الفقهية للمذاهب الأربعة نلاحظ بان تعريف السرقة التقليدية اختلفت عبارات المذاهب الفقهية تبعا لاختلافهم. ويمكن تعريفها بأنها: كل شخص يقوم بأخذ شيء بدون علم الغير مستترا أو خفية من اجل امتلاكه، فهو يعتبر سارق في نظر الفقه والقانون، إضافة إلى ذلك تعتبر جنحة في قانون الجزائري كقاعدة عامة.

ب- تعريف السرقة الالكترونية اصطلاحا:

يمكن بوجه عام تعريف جريمة السرقة المعلوماتية بأنها: اخذ المعلومات والبرامج المخزنة في الحاسب الآلي أو المنقولة عبر وسائل الاتصال، باستخدام أدوات تقنية المعلومات.[4] وتتم سرقة المال المعلوماتي عن طريق اختلاس، البيانات والمعلومات والإفادة منها باستخدام السارق للمعلومات الشخصية مثل الاسم، الأرقام السرية، الخاصة بالمجني عليهم[5]. السرقة الالكترونية هي عبارة عن أفعال غير مشروعة، يكون الحاسب الآلي محلا لها أو وسيلة لارتكابها[6].

وهناك من يعرف السرقة المعلوماتية بأنها: هي نوع من أنواع الجرائم المعلوماتية التي ترتكب بواسطة الكمبيوتر، ويمكن تعريفها بوجه عام بأنها: "**أخذ المعلومات والبرامج المخزنة في الحاسب الآلي أو المنقولة عبر وسائل الاتصال، باستخدام أدوات تقنية المعلومات**"[7].

---

[1]- د/ إبراهيم رمضان إبراهيم عطايا، الجريمة الالكترونية وسبل مواجهتها في الشريعة الإسلامية والأنظمة الدولية (دراسة تحليلية تطبيقية)، طنطا، 2015، ص 387.

[2]- إبراهيم رمضان إبراهيم عطايا،المرجع نفسه، ص 387.

[3]- دحمان صبايحية خديجة، جرائم السرقة والاحتيال عبر الانترنت دراسة مقارنة بين الفقه الإسلامي والقانون الجزائري، مذكرة لنيل شهادة الماجستير، شريعة والقانون، الجزائر، 2013، ص 8.

[4]- احمد محمد عبد الرؤف المنفي، السرقة الالكترونية وحكمها في الإسلام، شبكة الالوكة، اليمن، ص31. موقع الالكتروني:www.alukah.net

[5]- صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة الماجستير في القانون، تخصص القانون الدولي للأعمال، جامعة مولود معمري، تيزي وزو،2013، ص 74.

[6]- أنسام سمير طاهر، جريمة السرقة الالكترونية، مجلة جامعة بابل للعلوم الإنسانية، المجلد 27، العدد 5، 2019، ص134.

[7]- أحمد محمد عبد الرؤوف المنيفي، المرجع السابق، ص 33.

من خلال ما سبق نستنتج بان السرقة الالكترونية تعتبر من التعريفات الحديثة لما وصلت به التكنولوجيا في التقدم والتطور في عصرنا هذا، فهي سطو أو اختلاس على البرامج المخزنة في الكومبيوتر، سواء كان مال بنكي أو بيانات شخصية وما شبه في ذلك. فالسرقة الالكترونية هي عبارة عن أفعال غير مشروعة، فلجاني يقوم بسرقة في مكان بعيد عن مكان الجريمة فهي صعبة الإثبات، عكس السرقة التقليدية التي تتطلب على الجاني بان يكون في مسرح الجريمة.

وطبقا للمادة 350 قانون العقوبات التي تنص على **(كل من اختلس شيئا غير مملوك له يعد سارقا ويعاقب بالحبس من سنة (1) إلى خمس (5) سنوات وبغرامة من 100.00دج إلى 500.000دج.** نلاحظ هذه المادة لم تحصر لنا هذه الأشياء، وعليه يمكن استخدامها لمعاقبة مرتكبي السرقة الالكترونية، **(يجوز أن يحكم على الجاني علاوة على ذلك بالحرمان من حق أو أكثر من حقوق الواردة في المادة 9 مكرر 1 لمدة سنة (1) على الأقل وخمس (5) سنوات على الأكثر، وبالمنع من الإقامة طبقا للشروط المنصوص عليها في المادتين 12و13 من هذا القانون).**

ونلاحظ من خلال نص المادة 350 قانون عقوبات بان المشرع الجزائري، أدرج جريمة السرقة بأنه كل من قام باختلاس أشياء ولم يحدد لنا ما هي هذه الأشياء (معنوية أو مادية)، بحيث اعتبره سارقا فهو في نظر القانون يعد مجرم قام باعتداء على أملاك الغير،وإلى ذلك نجد الفقهاء في تعريفاتهم بان السرقة هي اخذ شيء دون علم صاحبه، ما جعل المشرع لم يغفل فيها بل قام بنص المادة أعلاه بمعاقبة وتجريم كل من يقوم بسرقة.

الأمر رقم 66-156 المؤرخ في 18صفار عام 1386 الموافق 8 يونيو سنة 1966، الذي يتضمن قانون العقوبات، المعدل والمتمم

الفرع الثاني: الخصائص المميزة لجريمة السرقة الالكترونية

ومن أهم خصائص جريمة السرقة الالكترونية هي:

- عابرة للحدود: سهولة في حركة المعلومات عبر أنظمة التقنية الحديثة مما جعل بالإمكان ارتكاب جريمة عن طريق حاسوب موجودة في دولة معينة بينما يتحقق الفعل الإجرامي

في دولة أخرى[1]. وبما أننا في عصر التكنولوجيا المتطورة فان سرقة الالكترونية عبرت الحدود، بحيث نجد الجاني متواجد في دولة معينة ويسرق خارج دولته.

- تقع السرقة الالكترونية في مجال المعالجة الآلية للمعلومات وتستهدف المعنويات لا الماديات.[2] وعليه تعتبر السرقة الالكترونية من الجرائم المستحدثة، الأكثر انتشارا في الشبكة المعلوماتية، بحيث الجاني المعلوماتي هدفه ليس أشياء مادية مثلما هو في السرقة التقليدية، فالسرقة الالكترونية تستهدف المعنويات.
- تتميز جريمة السرقة المعلوماتية بان تنفيذها يتم عن بعد والجاني في مكان بعيد عن مكان الجريمة[3]. وعليه فان السرقة تطورت بتطور التكنولوجيا، ويدل ذلك على أن السرقة التقليدية فالمجرم يقوم بتخطيط والتحضير أولا وبعد ذلك يباشر في تنفيذ جريمة السرقة بوجوده في مكان الجريمة، أما فيما يخص السرقة الالكترونية فالجاني المعلوماتي يسرق بذكاء بحيث يستعمل مهاراته أو مكتسباته القبلية أو إذا كان محترفا وله الخبرة فيذلك بتنفيذ تقنيات حديثة لارتكاب جريمة السرقة عن بعد.

وهي بالتالي اقل عنفا وأكثر صعوبة في الإثبات، لان الجاني مرتكب الجريمة لا يترك وراءه أي أثرا مادي خارجي ملموس[4].

إذن السرقة الالكترونية تعتبر جريمة اقل عنفا عكس السرقة التقليدية التي يتخذ فيها المجرم استعمال العنف أو السلاح، فهي ترتكب خفية، ولا يمكن رؤية الجاني يسرق كما هو في السرقة التقليدية،وعليه فالسرقة التقليدية المجرم الذي يرتكب الجريمة يمكن أن يشهد الشهود ضده أي وجود دليل ضده سواء كانت أدلة مادية أو عن طريق الشهود، بينما السرقة الالكترونية تعتبر جريمة خطيرة لأنها يصعب إثباتها.

---

[1]– سمية مزغيش، جرائم المساس بالأنظمة المعلوماتية، مذكرة مكملة من متطلبات نيل شهادة الماستر، قانون جنائي، جامعة محمد خضر، بسكرة، 2014، ص 19.

[2]– أنسام سمير طاهر، المرجع السابق، ص 135.

[3]– احمد محمد عبد الرؤوف، المرجع السابق، ص 32.

[4]– أنسام سمير طاهر، المرجع السابق، ص 136.

المطلب الثاني: تميز جريمة السرقة الالكترونية عن جريمة قرصنة البريد الالكتروني

جريمة السرقة الالكترونية هي سرقة ولكن بطرق متطورة ومستحدثة، وعليه نجد أيضا البريد الالكتروني يمكن قرصنته، والتي تشكل خطرا على المجتمع بحيث تعتبر جريمة خطيرة باستعماله للبريد الالكتروني المسروق، ويدل ذلك على انه قام بانتحال شخصية وأيضا تعتبر جريمة، ومن هنا سنحاول تميز بين جريمة السرقة الالكترونية وقرصنة البريد الالكتروني.

نتطرق في هذا الفرع الأول إلى تعريف جريمة قرصنة البريد الالكتروني، والفرع الثاني نتطرق إلى أوجه التشابه والاختلاف بين الجريمتين.

الفرع الأول: تعريف جريمة قرصنة البريد الالكتروني

تعريف البريد الالكتروني (ايمايل):

يعتبر من الاستخدامات الشائعة التي توفر إمكانية الاتصال بملاين البشر حول العالم كبديل للبريد التقليدي، البريد الالكتروني عبارة عن رسالة لكنها تتم بطريقة الكترونية. بحيث يتيح البريد الالكتروني إمكانية نقل الرسائل بطريقة سريعة للغاية[1]. وفي تعريف أخر إنها صندوق البريد الذي يتم بواسطة إرسال الرسائل الالكترونية إلى المرسل إليه عبر شبكة المعلومات، ولكل شخص أن يقوم بإنشاء هذا البريد تحت عنوان خاص به[2]. فلا يمكن اختراق البريد الالكتروني شخص إلا بمعرفة كلمة السر الخاصة به أو من خلال طرق فنية معقدة لا يجدها إلا محترفي عمليات اختراق شبكات الحاسوب[3].

تعريف قرصنة البريد الالكتروني:

وقد عرف القانون العربي النموذجي عند حديثة عن مكافحة جرائم الكمبيوتر والانترنت، جريمة قرصنة البريد الالكتروني باعتبارها جريمة الدخول غير المصرح به لنظام البريد الالكتروني[4].

---

[1]– نهلا عبد القادر مومني، الجرائم المعلوماتية،عمان، الطبعة الثانية، دار الثقافة للنشر والتوزيع، 2010، ص 29.

[2]– أيمن عبد الله فكري، الجرائم المعلوماتية دراسة مقارنة في التشريعات العربية والأجنبية، معهد الإدارة العامة الطبعة الأولى، الرياض، 2014، ص 51.

[3]– رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة لنيل شهادة الدكتورة قانون خاص، جامعة أبو بكر بلقايد، تلمسان، 2018، ص 84.

[4]– أنسام سمير طاهر، المرجع السابق، ص 137.

وعلى الصعيد الفقه المقارن والعرقي فلا يوجد تعريف البريد الالكتروني وإنما يوجد تعريف القرصنة بصورة عامة، بحيث تعددت الاتجاهات الفقهية التي تناولت تعريف الجريمة المعلوماتية بشكل عام وجريمة القرصنة بشكل خاص[1].

ويتضح من خلال التعريفات أن هناك بعض التعريفات للبريد الالكتروني بصفة عامة، بحيث يعتبر هي الوسيلة تواصل بين شخص ما أو عدة أشخاص، فهي أسرع من البريد التقليدي، وأما فيما يخص تعريف جريمة قرصنة البريد الالكتروني، ولم تضع تعريفا خاص به، بحيث اكتفت التشريعات بوضع النصوص القانونية التي تعرف الدخول غير المشروع وبشكل عام. ونشير في هذا الصدد أن المشرع الجزائري تناول في القانون العقوبات في القسم السابع مكرر[2] بأنظمة المعالجة الآلية، في المادة 394 مكرر بأنها تنص على معاقبة الدخول والبقاء الغير المشروع في نظام المعالجة الآلية.

وإضافة إلى ذلك نجده انه تبنى التعريف الذي جاءت به اتفاقية الدولية للإجرام المعلومات. بموجب أحكام المادة 2/ب من قانون 04/09، وأطلق عليه تسمية (منظومة معلوماتية)[3].

بحيث تنص على القواعد الخاصة بالوقاية من جرائم الإعلام والاتصال.

إذن تجدر بنا الإشارة إلى أن جريمة قرصنة البريد الالكتروني يمكن تطبيق عليها العقوبات المنصوص عليه في المادة 394 مكرر قانون العقوبات الجزائري.

وعليه يمكن أن نستخلص أن تعريف جريمة قرصنة البريد الالكتروني: بأنها الدخول الغير المشروع إلى نظام البريد الالكتروني دون علم صاحبه لغرض الاستيلاء والنسخ وجمع المعلومات وما شابه ذلك إلى المنظومة المعالجة الآلية.

الفرع الثاني: أوجه التشابه والاختلاف بين الجريمتين

إن أفعال جريمة سرقة المعلومات وجريمة قرصنة البريد الالكتروني تعد أفعال مجرمة في معظم التشريعات، لذلك نجد أوجه الاختلاف والتشابه بينهما.

---

[1]– أنسام سمير طاهر، المرجع نفسه، ص 138.

[2]– قانون رقم 09–04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[3]– أنسام سمير طاهر المرجع السابق، ص 138.

أ-أوجه التشابه:

- كلا الجريمتين من الجرائم المعلوماتية المستحدثة التي يصعب إثباتها وترتكب في الخفاء.
- وتعتمد كلا الجريمتين على النشاط التقني دون بذل أي مجهود عضلي.
- وهما من الجرائم العمدية.
- والتي يتعين لتوافرها القصد الجرمي العام والخاص، ووجوب توافر إرادة عمدية متجهة لارتكاب الفعل المجرم[1].

نستنتج من خلال ما تقدم بان هناك أوجه التشابه، بين السرقة الالكترونية وقرصنة البريد الالكتروني.

ب-أوجه الاختلاف:

- أن جريمة قرصنة البريد الالكتروني تتم دون رضا صاحب البريد الالكتروني. ويكون الدخول الأشخاص بقصد النسخ أو الاستيلاء على المعلومات.
- وتقع جريمة السرقة المعلومات أيا كان وجودها، أما جريمة قرصنة البريد الالكتروني فإنها تقتصر فقط على البريد الالكتروني.
- وينقسم مرتكبو جرائم قرصنة إلى فئتين هم الهاكر والمحترفون وهناك صنفين من القرصنة. يطلق على الصنف الأول الهواة والصنف الثاني المحترفون، بينما جريمة السرقة المعلومات تتم من قبل جميع الأشخاص المتمتعين بالخبرة التقنية[2].

بما أن جريمة السرقة الالكترونية وقرصنة البريد الالكتروني هناك أوجه التشابه فيما بينهما، وكما نجد أيضا أوجه اختلاف بين جريمتي السرقة الالكترونية وقرصنة البريد الالكتروني.

المطلب الثالث: مراحل السرقة الالكترونية

إن جريمة السرقة الالكترونية تتم وفق مراحل وخطوات التي يقوم بها المجرم من اجل الوصول إلى هدفه وأصبحت هذه الخطوات يتبعها القراصنة بوجه عام لدخول إلى نظام الحاسب الآلي. وتتكون هذه المراحل من أربع مراحل وهي:

---

[1]- أنسام سمير طاهر المرجع السابق، ص 138.

[2]- أنسام سمير طاهر المرجع السابق، ص 138.

- مرحلة الاستطلاع وجمع المعلومات.
- مرحلة مسح.
- مرحلة الدخول إلى الحاسب الآلي.
- مرحلة نسخ البيانات والمعلومات.

وانطلاقا من هذا قمت بتقسيم هذا المطلب الثالث إلى فرعين، نستعرض في الفرع الأول مرحلة الاستطلاع وجمع المعلومات ومرحلة المسح، وبينما في الفرع الثاني نستعرض مرحلة الدخول ومرحلة نسخ البيانات والمعلومات.

الفرع الأول: مرحلة الاستطلاع وجمع المراجع ومرحلة المسح

في هذا الفرع نتطرق إلى مرحلتين وهما: مرحلة الاستطلاع أو جمع المعلومات المتواجدة في الكمبيوتر بحيث تعتبر هذه المرحلة هي مرحلة بدائية التي يبحث فيها ويجمع المعلومات عن المنظومة المعلوماتية المراد اختراقها، فهي مهمة بالنسبة للجاني المعلومات التي يجمعها،وعليه سنحاول دراستها أولا،وتليها ثانيا مرحلة مسح وهذه المرحلة فيها يقوم الجاني بمسح المعلومات من اجل سهولة طريق الدخول إلى المنظومة.

أولا: مرحلة الاستطلاع أو جمع المعلومات

يقصد بمرحلة الاستطلاع جمع المعلومات عن المنظمة الهدف أو بالتحديد شبكة المنظمة، سواء كان هذه المنظمة بنك أو شركة ...الخ[1]

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[2] ولقد أدرج المشرع نص **المادة 394 مكرر 2 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).**

[1]– احمد محمد عبد الرؤوف المينيفي، المرجع السابق، ص 37.

[2]– احمد محمد عبد الرؤوف المنيفي، المرجع نفسه، ص37.

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[1].

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 لجريمة من الجرائم الماسة بالأنظمة المعلوماتية[2].

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[3].

---

[1]– محمد سعد، عالم القراصنة، حقوق الطبع والنشر 2020، ص 34.

[2]– صغير يوسف، المرجع السابق، ص 111.

[3]– احمد محمد عبد الرؤوف المنيفي، المرجع السابق، ص 38.

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 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 "**IP**".

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].

---

[1]– احمد محمد عبد الرؤوف المنيفي، المرجع السابق، ص 51.

[2]– رابحي عزيزة، المرجع السابق، ص 115 و116.

[3]– احمد محمد عبد الرؤوف المنيفي، المرجع نفسه، ص 54.

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[1].

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[2].

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 المكالمات من الفاتورة قبل طبعتها وإرسالها، ومثل قيام أحد الطلاب بتغيير درجاته المسجلة على الكمبيوتر في مادة معينة أو تغيير معدلة الفصلي أو العام[3].

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 اقر المشرع بتضاعف العقوبة إذا ترتب ذلك الحذف أو تغير لمعطيات المنظومة أو تخريب في المادة 394 مكرر».

---

[1]– محمد سعد، المرجع السابق، ص 40.

[2]– محمد نصير محمد، مشكلات الحماية الجنائية لبرامج الحاسب الآلي (دراسة مقارنة)، مجلة قضائية، العدد الثامن، محرم 1425هـ، ص 227.

[3]– فاطمة الزهراء خبازي، جرائم الدفع الالكتروني وسبل مكافحتها، أعمال الملتقى الوطني: آليات مكافحة الجرائم الالكترونية في التشريع الجزائري، الجزائر 29 مارس 2017، جامعة الجيلالي بونعامة، خميس مليانة، ص 33

الفرع الثاني: مرحلة الدخول ومرحلة نسخ البيانات والمعلومات

في هذا الفرع سنستعرض فيه مرحلتين، بحيث نتطرق أولا إلى مرحلة الدخول التي يحاول الجاني بقيام كسر كلمة السر من اجل استكمال مهمته، والتي تتمثل في مرحلة التي تلي مرحلة الدخول، وهي مرحلة الأخيرة المتمثلة في مرحلة نسخ المعلومات والبيانات.

أولا: مرحلة الدخول إلى الحاسب الآلي

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[1]. 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]– ابن شهرة شول، آليات مكافحة الجريمة المعلوماتية (مواقع التجارة الالكترونية نموذجا)، مجلة دراسات، العدد 13، 2016 دار المنظومة، الجزائر، ص 215. الرابط:Http : seach.mandumah.com/record/300501

[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، المرجع السابق، ص 157.

[4]– احمد محمد عبد الرؤوف المنيفي، المرجع نفسه، 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 لثغرات البرمجية وهذه الطريقة أصعب. ولكن إتباع الطريقة الأولى أو الطريقة الثانية فهي طبعا تؤدي إلى أثار 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، المرجع السابق، ص 108.

[2]- بدري فيصل، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة لنيل شهادة الدكتورة في قانون عام، جامعة الجزائر 1، بن يوسف بن خدة، 2018، ص 161.

[3]- بدري فيصل، مرجع نفسه، ص 144.

[4]- الأمر رقم 03-05 مؤرخ في 19 جمادي الأولى عام 1412 الموافق 19 يوليو سنة 2003 يتعلق بحقوق المؤلف والحقوق المجاورة.

ثانيا: مرحلة نسخ البيانات والمعلومات

نسخ البرامج والبيانات هي مرحلة النهائية في جريمة السرقة الالكترونية، وهو الهدف المقصود منها، وتتم عملية النسخ مع بقاء أصل المسروق لدى المجني عليه، فلا ينتقل هذا الأصل إلى الجاني، وإنما تنتقل إليه نسخة فقط، وهذا يعد من أهم خصائص السرقة الالكترونية[1]. وتتمثل مرحلة إخراج البيانات، مثل ذلك سرقة بعض البيانات الالكترونية أو معلومات الآلية المتعلقة بمراقبة مخزون إحدى الشركات أو إفشاء معلومة متعلقة بإحدى الشركات أو إفشاء معلومة متعلقة بإحدى العملاء[2].

إن احتفاظ بنسخة قد يتم التواصل إلى المعلومات السرية الالكترونية بكل سهولة مما يتم نسخها بسرعة فائقة، والخطورة تكمن هنا في إمكانية استخدام تلك المعلومات السرية الخاصة في المستقبل من اجل تحقيق أغراض غير مشروعة[3]. وتعتبر **قرصنة البرمجيات** هي عملية نسخ أو تقليد لبرامج إحدى الشركات العالمية على اسطوانات وبيعها للناس بسعر اقل،وجريمة نسخ المؤلفات العلمية والأدبية بالطرق الالكترونية المستحدثة،وعليه أن المعلومة الأدبية والفكرية ذات قيمة أدبية ومادية إلى جانب ذلك براءات الاختراع التي تخول لملكها حق معنوي وآخر مالي[4].

وإضافة إلى ذلك يتم نسخ البيانات الالكترونية لبطاقة الصراف الآلي بحيث يستخدمها لصرف أموال من حساب الضحية، وقد ينشئ صفحة انترنت مماثلة جدا لموقع أحد البنوك، أو المؤسسات المالية الضخمة لتطلب من العميل إدخال بياناته أو تحديث معلوماته بقصد الحصول على بياناته المصرفية وسرقتها[5].

وهناك طريقتين لنسخ البرنامج الحاسب الآلي والمتمثلة في صور الاعتداء لها:

النسخ الحرفي للبرامج: وتعتبر اشد صور الاعتداء على البرامج، بحيث يقوم بإعادة إنتاج البرنامج وملحقاته بشكل كامل أو تقليده دون زيادة أو نقصان أو تعديل. وأما النسخ الغير

---

[1]– احمد محمد عبد الرؤوف المنيفي، المرجع السابق، ص 76.

[2]– فاطمة الزهراء خبازي، المرجع السابق، ص 33.

[3]– رابحي عزيزة، المرجع السابق، ص 51.

[4]– سورية ديش، أنواع الجرائم الالكترونية وإجراءات مكافحتها، مجلة الدراسات الإعلامية، المركز الديمقراطي العربي، العدد الأول، يناير 2018، جامعة جيلالي ليابس، سيدي بلعباس، الجزائر، ص 245.

[5]– سورية ديش، المرجع سابق، ص 243 و244.

الحرفي للبرامج: يقصد به الانتحال، بالمعنى الاستحواذ على الغير، ويتجلى الاعتداء في حالة وجود نسخة مأخوذة عن الأصل لها بشدة ومطابقة والسبب في ذلك يعود ذلك إلى الاستعارة الدقيقة لبعض العناصر،وكلما كان الناسخ يتمتع بقدرة كبيرة أن يظهر الاستعارة هذا يكون أفضل، بحيث تزداد الفرصة لينتج مصنفا أو شيئا جديد[1].

وعليه تتحقق السرقة بمجرد اخذ نسخة من الأصل مع بقاء هذا الأصل في حيازة صاحبه مادام أن هذا الأخذ تم دون موافقة صحبه[2].

نص المشرع العربي في المادة الرابعة عشر (14) على سرقة المعلومات بتجريم كل من عمليات نسخ ونشر لمصنفات الفكرية أو الأدبية، أو الأبحاث العملية، أو ما في حكمهما إذا ما ارتكب دون وجه حق، بعقوبة الحبس الذي يترك تقديرها وفقا لقانون كل دولة ودون الاختلال بنصوص الخاصة بالملكية الفكرية لكل بلد[3]. من خلا ما سبق نشير إلى مرحلة نسخ البيانات والمعلومات، هي مرحلة نهائية التي يقوم بها الجاني، كما تتم عملية نسخ البرامج والبيانات بانتقال النسخة طبق الأصل إلى الجاني (السارق) وتبقى النسخة الأصلية لدى المجني عليه (الضحية).

ونلاحظ بان المشرع الجزائري حصر الأفعال التي يعاقب عليها في المادة 394 مكرر 1 وهي الإدخال أو التعديل أو المحو، بينما فعل النسخ لم يذكره، وبما أن السرقة تتحقق بمجرد قيام بنسخ طبق الأصل على البرامج والمعلومات، إذن يمكن تطبق على هذه المرحلة على نص المادة 350 قانون العقوبات.

إن كلمة "الشيء" الواردة في المادة 350 قانون العقوبات، تشمل الأشياء المادية وغير المادية[4]. وفيما يخص استنساخ برامج المؤلف بأي أسلوب في شكل نسخ مقلدة، بحيث يعد هذا السلوك الإجرامي من أشهر البرامج وأخطر عمليات التقليد والقرصنة المعلوماتية لسهولة

---

[1]– عبد الرحمان جميل محمود حسين، الحماية القانونية لبرامج الحاسب الآلي دراسة مقارنة، الأطروحة استكمالا لمتطلبات درجة الماجستير في قانون الخاص، بكلية الدراسات العليا في جامعة النجاح الوطنية في نابلس، فلسطين، 2008، ص 13.

[2]– محمد نصير محمد، المرجع السابق، ص 223.

[3]– سمية مزغيش، المرجع السابق، ص 51.

[4]– العمري ابتسام، جريمة سرقة المعطيات المعلوماتية، مذكرة لنيل شهادة الماستر في قانون الجنائي للأعمال، جامعة العربي بن مهدي، أم البواقي،2018، ص 30.

القيام بها، وقلة تكاليفها وارتفاع مداخيلها واستنساخ البرمجيات قد يتم في عدة أشكال وصور باختلاف الدعامة والمصدر الذي تتواجد فيه هذه البرمجيات[1].

إن المشرع الجزائري قد فصل جيدا حدود الاستنساخ بالنسبة للبرمجيات المؤلف وحددها في حالات استثنائية معينة[2].

[1]– بدري فيصل، المرجع السابق، ص 144 و145.

[2]– بدري فيصل، مرجع نفسه، ص 146.

المبحث الثاني: دوافع وتقنيات ارتكاب مجرمي جريمة السرقة الالكترونية وأصنافها

نستعرض في هذا المبحث الدوافع التي أدت إلى ارتكاب جريمة السرقة الالكترونية، بحيث نجد أن هناك عدة دوافع لارتكابها ومنها الدوافع الشخصية والمادية وغيرها، نتطرق فيها في المطلب الأول مع استعراض أساليب وتقنيات المتبعة لارتكاب الجريمة الخطيرة التي تمس المعلومات والأبحاث العلمية والصور والفيديوهات وغيرها من الأمور الشخصية الموجودة في الحاسب الآلي، وأما فيما يخص المطلب الثاني سنستعرض فيه أصناف القراصنة وأطرافها.

المطلب الأول أساليب ارتكاب جريمة السرقة الالكترونية ودوافعها

قسمت المطلب هذا إلى فرعين: ففي الفرع الأول نتطرق فيه إلى دوافع التي أدت لارتكاب جريمة السرقة الالكترونية، وبينما في الفرع الثاني نتطرق إلى أساليب وتقنيات لارتكاب هذه الجريمة. حيث أن مجرمي الانترنت يسعون من خلال ارتكابهم جريمة لتحقيق أغراض شخصية أو معنوية أو قد تكون ذات كيان مادي، والمجرم عند ارتكابه الجريمة فهو يتبع أساليب وهذه الأساليب تختلف بين جريمة المرتكبة عبر الانترنت عن جريمة التقليدية. وبفضل تطور السريع الذي في الفترة الخيرة، تطورت معها أساليب ارتكاب الجريمة. وسنحاول التفصيل في الفرعين المواليين أساليب والدوافع لارتكاب جريمة السرقة الالكترونية[1].

الفرع الأول: دوافع ارتكاب جريمة السرقة الالكترونية

وبما أننا في عصر التكنولوجيا بحيث الدافع هو الذي يحرك إرادة الجاني لارتكاب الجريمة، وعليه نجد عدة أسباب تدفع لارتكاب الجرائم المستحدثة، ونوجزها كالتالي:

أولا: الرغبة في قهر النظام والتفوق على تعقيد وسائل التقنية

قد تكون الدوافع لارتكاب الجريمة مجرد شغف بالإلكترونيات والرغبة في تحدي وقهر النظام والتفوق على تعقيد وسائل تقنية[2]. وعلى صعيد أخر قد يكون الدافع وراء ارتكاب الجريمة هو الرغبة في قهر النظام الالكتروني والتغلب عليه، لإظهار تفوقهم على وسائل

---

[1]– بدري فيصل، مرجع نفسه، ص 146.

[2]– سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة لنيل شهادة الماجستير في العلوم القانونية الجنائية، جامعة الحاج لخضر، باتنة، 2013، ص 61.

التكنولوجيا الحديثة[1]. وقد يكون الداعي إلى ارتكاب الجريمة هو من اجل إثبات شخصية ضعاف النفوس الذين يجدون في شخصياتهم خللا ما، ولإكمال النقص المغروس في نفوسهم[2]. ويتزايد شيوع هذا الدافع لدى فئة صغار السن، الذين يمضون وقتا طويلا أمام حواسيبهم الشخصية في محاولة لكسر حواجز الأمن لأنظمة الحواسيب والشبكات المعلومات لإظهار تفوقهم على وسائل التقنية[3].

وأقوى دافع الذي يدفعه إلى ارتكاب الجريمة هو من اجل قهر النظام، بحيث يتزايد شيوع هذا الدافع لدى فئة صغار السن، بحيث يحاولون بيان تفوقهم ومستوى ارتقاء براءتهم، وهناك دافع أخر والذي يتمثل في التسلية واللهو ويكون عدد غير قليل من المحترفين يعتبرون أن الدخول إلى الحواسيب الآخرين دون علمهم واختراقها هو تسلية ومرح من عملهم هذا بحيث يقضوا أكبر أوقاتهم في أنظمة الحواسيب.

ثانيا: الربح وكسب المال

إن الرغبة في تحقيق مكاسب مادية، قد يكون من أكثر البواعث التي تؤدي إلى إقدام مجرمي المعلوماتية على اختراق جرائمهم[4] بحيث يعمد الجاني رغبة منه في تحقيق الثراء والكسب المادي إلى التلاعب بأنظمة المعالجة الآلية للبنوك والمؤسسات المالية إن كان أحد موظفيها، فيعمل على استغلالها وبرمجتها لتحويل مبالغ مالية إن كان أحد شركائه أو لحسابهم، كما يمكن الحصول على مكاسب المادية من خلال المساومة على البرامج أو المعلومات المتحصل عليها بطريق الاختلاس من جهاز الحاسوب[5]. يكون الدافع منها تحقيق أرباح

---

[1]– سالم محمد سالم بني مصطفى، جريمة السرقة المعلوماتية، رسالة استكمالا لمتطلبات الحصول على درجة الماجستير في قانون عام، جامعة جدار، 2011، ص 34.

[2]– سعدات محمد فتوح محمد، خصائص الجرائم المعلوماتية وصفات مرتكبها في ظل مجتمع المعلوماتية، المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية، كلية العلوم الحاسب والمعلومات، جامعة الإمام محمد بن سعود الإسلامية،الرياض، دار المنظومة 2016، ص 39.

[3]– لعاقل فريال، الجريمة المعلوماتية في ظل التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون الجنائي، جامعة أكلي محند أولحاج، البويرة، 2015، ص 26.

[4]– سالم محمد سالم بني مصطفى، المرجع السابق، ص 33.

[5]– سعيداني نعيم، المرجع السابق، ص 61.

ومكاسب مادية كاستخدام شبكة الانترنت للإعلان عن صفقات تجارية غير مشروعة[1] والدافع الذي يتمثل في كسب الأرباح الطائلة دون تعب وإرهاق ودون رأسمال، هذا السبب هو الذي يدفع إلى اختراق الأنظمة المعلوماتية بغرض التلاعب فيها أو استخدام الغير المشروع لبطاقات الائتمان. بالدخول إلى حسابات المصرفية.

ثالثا: الانتقام من رب العمل وإلحاق الضرر به

يتوافر هذا الدافع نتيجة فصل الموظف من عمله، كما يعتبر هذا الدافع أخطر الدوافع التي يمكن أن تدفع الشخص إلى ارتكاب الجريمة، ذلك انه غالبا ما يملك معلومات كبيرة عن المؤسسة أو الشركة التي يعمل فيها[2] وعليه الباعث على ارتكاب الجريمة قد يكون في الانتقام من شخص ما، أو حتى من بعض الأنظمة السياسية في بعض الدول أو من رب العمل[3]. أي أن الحقد على رب العمل الدافع المحرك لارتكاب الجريمة[4]. لوحظ أن العاملين في قطاع التقنية أو المستخدمين لها في نطاق قطاعات العمل الأخرى، يتعرضون على النحو كبير لضغوطات نفسية ناجمة عن ضغط العمل، والمشاكل المالية، وكل هذه الأمور قد تدفع إلى النزعة نحو تحقيق الربح، لكنها في حالات كثيرة تدفع بعض العاملين إلى ارتكاب جرائم الحاسوب، هدفها الانتقام من رب العمل أو المنشأة[5].

ونجد دافع أخر التي تدفعه إلى ارتكاب جريمة السرقة الالكترونية هو الدافع الشخصي، والتي تدفع العامل إلى الانتقام بالدخول في أنظمة الكترونية التي تسهل عليه الانتقام بحيث يقوم بتخريب فيها والعبث في محتوياتها.

---

[1]– سعيد بن سالم البادي، زيدان بن حمد الجنيبي، يوسف الشيخ حمزة، محمد احمد العطاء، الجريمة الالكترونية في المجتمع الخليجي وكيفية مواجهتها، مجمع البحوث والدراسات أكاديمية السلطان قابوس لعلوم الشرطة نزوى، سلطنة عمان،2017، ص29.

[2]– نايري عائشة، الجريمة الالكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون الإداري، جامعة احمد دراية، أدرار، 2017، ص 13.

[3]– سالم محمد سالم بني مصطفى، المرجع السابق، ص 34.

[4]– رابحي عزيزة، المرجع السابق، ص 101.

[5]– لعاقل فريال، المرجع السابق، ص 25.

رابعا: الرغبة في تعلم القرصنة المعلوماتية

الرغبة الشديدة في تعلم كل ما يتعلق بأنظمة الحاسوب والشبكات الالكترونية قد يكون الدافع وراء ارتكاب الجرائم المعلوماتية[1]. وكثيرا ما نجد أن قراصنة الأنظمة يعلنون أن هدفهم من الوصول للمعلومات ودخولهم للشبكات والحواسيب الالكترونية هو التعلم فقط[2]. ويشير الأستاذ (ليفي) مؤلف كتاب قراصنة التي تركز على أساسين:

1- إن الدخول إلى أنظمة الحاسوب يمكن أن يعلمك كيف يسير العالم.

2- إن عملية جمع المعلومات يجب أن تكون غير خاضعة للقيود[3].

يعتبر حب التعلم والاستطلاع من الأسباب الرئيسية التي تدفع إلى ارتكاب الجريمة، لان المخترق يعتقد أن أجهزة الحاسوب والأنظمة هي ملك للجميع من اجل الاستفادة والتعلم[4]. باعث هذه الفئة هو حب التعلم كل ما يخص بالحاسوب والانترنت،وعليه فان رغبتهم الشديدة وشغف الالكترونيات لأجل التعلم وقد تدفعه إلى ارتكاب الجريمة.

الفرع الثاني: أساليب وتقنيات ارتكاب جريمة السرقة الالكترونية

نتطرق في هذا الفرع إلى تقنيات التي يتبعها المجرم المعلوماتي في ارتكاب جريمة السرقة الالكترونية، حيث أصبح من السهل انتهاك هذه المنظومة المعلوماتية التي انتشرت في هذه الفترة الأخيرة الكثير من الكتب وخاصة اليوتيوب، هناك بحيث تتيح معرفة مختلف الوسائل والتقنيات التي يمكن معرفتها لارتكاب السرقة وانتهاك سرية المعلومات. وهذه الأساليب تتمثل في:

- الاختراق أولا.
- الفيروسات ثانيا.

---

[1]- حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، علم الإجرام والعقاب، جامعة الحاج لخضر، باتنة، 2012، ص 47.

[2]- سعيد بن سالم البادي وأخرن، المرجع السابق، ص 28.

[3]- نهلا عبد القادر المومنى، المرجع السابق، ص 89 و90.

[4]- مهني محمد شريف، استخدام القرصنة الالكترونية في السياسة الروسية (بين التجريم الدولي وحتمية التخابر)، مذكرة تخرج لاستكمال متطلبات لنيل شهادة الماستر في ميدان حقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، 2018، ص 13.

أولا: الاختراق

المخترق هو شخص لا علم له بأي لغة من لغات البرمجة إنما تتم عمليات الاختراق التي يجربها عن طريق برامج اختراق موجودة بكثرة على الشبكة مجانية[1]. بحيث ارتبط ظهور القرصنة واختراق رموز أنظمة الحاسوب مع ظهور أول الحواسيب الالكترونية إلا أن تاريخ القرصنة واختراق رموز أنظمة الحاسوب يشمل الهجوم السيئ على شبكات الحاسوب من قبل مخترقي نظم الحاسوب[2].

القرصنة:

هي عملية اختراق لمنظومات حاسوبية أو شبكية يتم خلالها نسخ المعلومات المراد قرصنتها بهدف استغلالها لأغراض شخصية سواء منها الربح المالي، أو لأغراض أخرى كالتشهير أو التجسس الأمني أو التحيل أو غير ذلك أو غير ذلك من الأعمال الإجرامية، المشابهة والواقعة في الحياة اليومية في المجالات المختلفة كالتزوير والسرقة والتنصت وغير ذلك[3] تتم اغلب الاختراق عن طريق زرع برنامج معين في جهاز الضحية[4].

يشير القرصنة ببساطة إلى فعل استغلال ضعف موجود في نظام كمبيوتر أو شبكة[5] إن عملية الاختراق الالكتروني تتم عن طريق تسريب البيانات الرئيسية والرموز الخاصة ببرامج الشبكة الانترنت، وهي عملية تتم من أي مكان في العالم، ولا تزال نسبة الاختراقات لم تكتشف بعد بسبب التعقيد الذي يتصف به النظام تشغيل الحاسب الآلي[6]، الاختراق بشكل عام هو القدرة على الوصول لهدف معين بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بالهدف أو الوصول إلى البيانات الموجودة على الأجهزة الشخصية بوسائل غير مشروعة[7]. فيكون الاختراق على وصول هدف معين عن طريق ثغرات في النظام الحماية

---

[1]– بشرى حسين الحمداني، القرصنة الالكترونية أسلحة الحرب الحديثة، دار أسامة للنشر والتوزيع، الأردن، عمان، الطبعة الأولى، 2014، ص 14 و 15 .

[2]– بشرى حسين الحمداني، المرجع السابق، ص 20.

[3]– زايد محمد، الجريمة والقرصنة في مجال المعلوماتية والشبكات، المجلة العربية العلمية للفتيان، تونس، المجلد 10، العدد 19، 2016 دار المنظومة، ص 57. الرابط:http://search.mandumah.com/record/100968

[4]– مهني محمد شريف، المرجع السابق، ص 15.

[5]– محمد سعد، المرجع السابق، ص 6.

[6]– عبد الرحمان عبد الله سند، المرجع السابق، ص 284.

[7]– سعيداني نعيم، المرجع السابق، ص 56.

الخاصة، وتتم عن طريق برنامجين الأول الخادم وهو بجاهز الضحية إذ ينفذ المهام الموكلة إليه، والثاني يوجد بجهاز المخترق ويسمى بالبرنامج المستفيد[1].

وعليه نستدرج أنواع الاختراق فيما يلي:

1- اختراق المزودات أو الأجهزة الرئيسية للشركات والمؤسسات أو الجهات الحكومية وذلك باختراق الجدران النارية التي عادة توضع لحمايتها، وغالبا ما يتم ذلك باستخدام المحاكاة **Spoofing** وهو مصطلح يطلق على عملية انتحال شخصية، للدخول إلى النظام حيث أن حزم الـ**IP** تحتوي على عناوين للمرسل والمرسل إليه وهذه العناوين هي ذاتها نجح بها مخترقي الهوتميل في الولوج إلى معلومات النظام قبل فترة قريبة من الزمان[2].

2- الاختراق الأجهزة الشخصية والعبث بما تحتويه من معلومات وهي طريقة للأسف شائعة لسذاجة أصحاب الأجهزة الشخصية من جانب ولسهولة تعلم برامج الاختراقات وتعددها من جانب أخر[3].

3- اختراق متواجد بكثرة في مواقع التواصل الاجتماعي، بحيث تتم عن طريق القراصنة مخترقي الأنظمة على مواقع التواصل الاجتماعي، حيث يتبادل أفراد هذه الطائفة المعلومات فيما بينهم بغية الاطلاع على مواطن الضعف في الأنظمة المعلوماتية[4].

4- قرصنة موقع الويب: يعني قرصنة موقع ويب التحكم غير المصرح به في خادم الويب والبرامج المرتبطة به مثل قواعد البيانات والوجهات الأخرى[5].

يتضح بأن اختراق الحاسوب ظهر منذ ظهور أول كمبيوتر، ويطلق عادة على استخدام غير القانوني للحاسوب، من خلال استخدام شبكة الانترنت، وبالإضافة بعض البرامج المعدة خصيصا لهذا الغرض،ويعتبر في وقتنا الحالي الاختراق على انه تعطيل أنظمة الأمن على

---

[1]- روان بن عطية الله الصحفي، الجرائم السيبرانية، المجلة الالكترونية الشاملة متعددة التخصصات، العدد الرابع والعشرون، شهر 5، 2020، المملكة العربية السعودية، جدة، ص 15.

[2]- محمد إسماعيل محمد، الاختراق 1، دون طبعة النشر، دون سنة النشر، ص4.

[3]- انظر الموقع الالكتروني:https://shella4ever.yoo7.com/t81-topic يوم الاطلاع: 2021/4/23،على الساعة 09:00.

[4]- احمد حسن عبد العليم حسن الخطيب، الجرائم المعلوماتية الواقعة عبر التواصل الاجتماعي قراءة في قانون مكافحة جرائم التقنية المعلومات المصري رقم 175 لسنة 2018 ونظام مكافحة جرائم المعلوماتية السعودي 1428هـ، مجلة دراسات الإفريقية وحوض النيل، العدد السادس أكتوبر، تشرين الأول، 2019، مجلد 2، المركز الديمقراطي العربي، ألمانيا، برلين، ص 116.

[5]- انظر الموقع الالكتروني: http ://www.jsecuritylab.com/2020/10/blog-post_94.html يوم الاطلاع: 2021/5/25، على الساعة: 15:15.

المنظومة المعلوماتية المراد اختراقها، فهو عمل غير قانوني يحاسب عليه القانون. وقد تستخدمها أيضا بعض الدول لمعرفة أسرار الدول المعادية لها، بحيث يصل المهاجم الذي يخترق ويتعدى على الحاسوب لهدف معين بطريقة غير شرعية.

ثانيا: الفيروسات (البرامج الخبيثة)

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 أخر عن طريق الملفات المتبادلة بين المستخدمين[5].

وهناك أنواع عديدة من الفيروسات ومنها ما يلي:

* **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[1].

---

[1]– أيمن عبد الله فكري، المرجع السابق، ص 45.

[2]– عبد الرحمان عبد الله سند، المرجع السابق، ص 345.

[3]– أسامة فتحي، فيروسات الحاسوب، دون بلد النشر، دون سنة النشر، ص 3.

[4]– احمد محمد عبد الرؤوف المنيفي، فيروسات الحاسب الآلي، اليمن، 2019، ص4.

[5]– عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الالكترونية دراسة مقارنة، رسالة استكملا للحصول على درجة الماجستير في القانون العام،جامعة الشرق الأوسط،2014، ص 7.

[6]– انظر موقع الكتروني:https://www.mlzamty.com/virus-damage/ يوم الاطلاع على الساعة 48:22، 2021/4/23.

* **الدودة:** وهي عبارة عن برمجية تقوم بالانتقال من حاسوب إلى أخر، دون حاجة إلى تدخل إنساني لتنشيطها، فهي تتمتع بخاصية التنشيط الذاتي وبهذا تختلف حصان طروادة[2].
* **فيروسات خفية:** هذه الفيروسات تفلت من الرقابة بواسطة قدرتها على التنكر، مما يجعل اكتشافها صعب[3].
* **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 البرنامج الرئيسي، فهو لا يزال الفيروس نشطا في الذاكرة في انتظار فرصة للعثور على ملفات الأخرى وتصيبها حتى بعد الرئيسية تم إنهاء البرنامج (المضيف)[4].

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.

المطلب الثاني: أصناف مجرمي السرقة الالكترونية وأطرافها

جريمة السرقة الالكترونية بما أنها تعتبر من أحد الجرائم المعلوماتية، نظرا لتطور السريع في مجال التكنولوجيا، ظهرت جرائم جديدة مستحدثة، وتطورت طريقة ارتكابها، ومن هذا المنبر نشير إلى أصناف مجرمي السرقة الالكترونية، بحيث نجد الجاني المعلوماتي (السارق) والمجني عليه (المسروق)، إضافة إلى ذلك نجد هناك العديد من الطوائف للقراصنة، وسنتطرق

---

[1]– إبراهيم السنوسي نصر، مقدمة للإنترنت، البرنامج التمهيدي للتدريب على استخدام الحاسوب والانترنت، جامعة سبها، مكتب التدريب، 2015، ص 20.

[2]– طرق الخن، جرائم المعلوماتية، منشورات الجامعية الافتراضية السورية، الجمهورية العربية السورية، 2018، ص 45. على الرابط: http://pedia.svuonline.org

[3]– دردور نسيم، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، مذكرة لنيل شهادة الماجستير في القانون الجنائي، جامعة منتوري، قسنطينة، 2013، ص 45.

[4]– محمد سعد، المرجع السابق، ص 75.

إلى طائفتين أساسيتين، وهما الهاكرز والكراكرز. وعليه قسمت المطلب الثاني إلى فرعين: بحيث نتطرق إلى أطراف مجرمي السرقة الالكترونية في فرع الأول، بينما أصناف قراصنة الالكترونية في فرع الثاني.

الفرع الأول:أطراف مجرمي السرقة الالكترونية

أطراف الجريمة المعلوماتية هي كأي جريمة لا بد لها من فاعل (الجاني)وواقع عليه الفعل (المجني عليه)، والذي غالبا يهيئ الفرصة المناسبة لاستغلال الوسيلة المعلوماتية،وهي نوع جديد من السلوكيات المنحرفة التي يتعرض لها كل من النظام المعلوماتي ومكوناته من البيانات أو المعطيات من خلال أشخاص مؤهلين وذوي خبرة علمية وعملية، بل له أثره أيضا على تميز المجرم ألمعلوماتي عن غيره من المجرمين التقليدين.

ونستعرض فيه الجاني المعلوماتي أولا، ثم المجني عليه ثانيا.

أولا: الجاني في جريمة المعلوماتية

المجرم المعلوماتي هو كل شخص سواء، طفل، رجل، أنثى، يأتي أفعالا إرادية تشكل سلوكا ايجابيا أو سلبيا باستخدام تقنية المعلوماتية، لإحداث نموذج إجرامي بالاعتداء على حق أو مصلحة،وسمات المجرم المعلوماتي تشبه في كثير من الأحيان، سمات المجرمين ذوي الياقات البيضاء[1]. فالمجرم المعلوماتي ينتمي في أكثر الحالات إلى وسط اجتماعي متميز كما انه على درجة من العلم والمعرفة، وان لم يكن من الضروري أن ينتمي إلى مهنة يرتكب من خلالها الفعل الإجرامي[2] يتميز المجرم المعلوماتي عن غيره من المجرمين العاديين الذين جنحوا إلى السلوك الإجرامي النمطي بعدة خصائص ومنها: المجرم المعلوماتي لا يلجأ إلى العنف في تنفيذ جرائمه، ومتخصص ومحترف[3].

يتميز المجرم المعلوماتي بمجموعة من السمات والتي تساعد التعرف عليها في مواجهة هذا النمط الجديد، ومن أهم هذه الصفات:

---

[1]– حمزة بن عقون، المرجع السابق، ص 28.

[2]– لعاقل فريال، المرجع السابق، ص 20.

[3]– نمديلي رحيمة، خصوصية الجريمة الالكترونية في القانون الجزائري والقوانين المقارنة، أعمال المؤتمر الدولي الرابع عشر: الجرائم الالكترونية، طرابلس 24–25 مارس 2017، جامعة محمد لمين دباغين، سطيف 2، الجزائر، ص 7.

* **مجرم ذكي:** حيث يمتلك هذا المجرم من المهارات ما يؤهله للقيام بتعديل وتطوير في الأنظمة الأمنية حتى لا تستطيع أن تلاحقه وتتبع أعماله الإجرامية من خلال الشبكات أو داخل أجهزة الحاسوب[1].
* **المجرم متخصص:** له قدرة فائقة في المهارة التقنية ويشتغل مداركه ومهارته في اختراق الشبكات وكسر كلمات المرور أو الشفرات ويسبح في عالم الشبكات ليحصل على كل غالي وثمين من البيانات والمعلومات الموجودة على أجهزة الحواسيب ومن خلال الشبكات[2].
* **المجرم لا يستخدم العنف:**يعد مرتكبي جرائم المعلوماتية من المجرمين الذين لا يلجؤون إلى العنف مطلقا في تنفيذ جرائمهم، لان هذا النوع من الجرائم لا يستلزم أي قدرة من العناء للقيام بذلك[3]. كالسرقة الالكترونية فالمجرم هنا لا يستعمل العنف بل يلجأ إلى الحيلة والذكاء فهي جريمة عكس جرائم التقليدية.
* **المجرم يسيطر على النظام:** فمعظم مجرمي المعلوماتية لهم سلطة مباشرة أو غير مباشرة في مواجهة المعلومات محل الجريمة، وقد تشمل هذه السلطة في الشفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات، والتي تعطي الفاعل مزايا متعددة كفتح الملف أو محوها أو قراءتها أو كتابتها[4].

من خلال ما تقدم يتضح بان المجرم المعلوماتي يختلف عن المجرم التقليدي العادي،ويختلفان سواء في الأهداف أو الطريقة ارتكاب الجريمة، والمجرم المعلوماتي له صفات تميزه عن المجرم العادي.

ثانيا: المجني عليه

وفقا لتقرير صندوق النقد الدوالي، فانه من المستحيل أن نحدد على نحو دقيق نطاق الجرائم المعلوماتية، حيث انه من المتصور أن يقع ضحية هذه الجرائم جميع الأشخاص، سواء

---

[1]– إسراء جبريل رشاد مرعي، الجرائم الالكترونية «الأهداف، الأسباب، طرق الجريمة ومعالجتها»، مجلة الدراسات الإعلامية، المركز الديمقراطي العربي، العدد الأول يناير، 2018، ص429.

[2]– مرابطن حياة، الجريمة الالكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون الجنائي والعلوم الجنائية، جامعة عبد الحميد بن باديس، مستغانم، 2019، ص 24.

[3]– سعدات محمد فتوح محمد، المرجع السابق، ص 45.

[4]– ريم ساسي، الحماية الجنائية لسرية المعلومات الالكترونية، مذكرة لنيل شهادة الماستر تخصص قانون جنائي للأعمال، جامعة العربي بن مهيدي، أم البواقي، 2016، ص 21.

الطبيعية أو المعنوية، العامة أو الخاصة[1]. من الصعب تحديد نطاق ضحايا هذه الجرائم ومن بينهم جريمة السرقة الالكترونية، لأنهم لا يعلمون بها إلا بعد وقوعها وعند علمهم يفضلون عدم الإبلاغ عن انتهاك نظامهم المعلوماتي وهذا ما يساعد على زيادة ارتكابها[2].

أن الغالبية العظمى من المجني عليهم هم إما مؤسسات مالية كالبنوك والمصارف وشركات الصرافة، وإما شركات المعلومات بصرف النظر عن نوع هذه المعلومات أو قيمتها إذ قد تكون بالغة الأهمية كالمعلومات العسكرية والمخابراتية، وقد تكون معلومات رياضية أو فنية أو اجتماعية بسيطة[3]. نلاحظ بان الجاني المعلوماتي يهاجم المعلومات التي يستفيد منها سواء كانت مادية كالأموال أو معنوية، بحيث يكون المجني عليه شركات أو مؤسسات أو يكون شخص طبيعي بسرقته البريد الالكتروني، وعليه فان لصد هذه الجرائم على المجني عليهم بالإبلاغ عن انتهاك النظام المعلوماتي.

الفرع الثاني: أصناف القراصنة المعلومات

نستعرض في هذا الفرع صنفين أساسيين للقراصنة، بحيث هذه الظاهرة انتشرت بكثرة في وقتنا الحالي، يمكن تصنيف قراصنة المعلومات إلى قسمين:

1- قراصنة الهواة (الهاكر)

2- قراصنة المحترفون (الكراكر)

أولا: قراصنة الهواة (الهاكر)

الهاكر هو اللفظ العربي للكلمة الانجليزية وهي تحمل عدة معان، إلا أننا معنيون بمعنى واحد وهو المخترق أو الهاتك[4]. تضم هذه الطائفة الأشخاص الذين يستهدفون من الدخول إلى أنظمة الحاسبات الآلية غير المصرح لهم بالدخول إليها، وكسر الحواجز الأمنية الموضوعية لهذا الغرض. وذلك بهدف اكتساب الخبرة أو بدافع الفضول أو لمجرد إثبات القدرة، على اختراق هذه الأنظمة[5]. يرون في اختراق لأنظمة المعلوماتية تحديا لقدراتهم الذاتية، هذه

---

[1]- عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية وأزمة الشرعية الجزائية، جامعة الكوفة، كلية القانون، العدد السابع، 2008، ص 118.

[2]- عيشة خلدون، الطبيعة الخاصة للجريمة الالكترونية وصورها، مجلة دراسات وأبحاث، جامعة الجلفة، الجزائر، 2016 دار المنظومة، ص 120. الرابط: http://search.mandumah.com/record/458394

[3]- عبد الله دغش العجمي، المرجع السابق، ص 34.

[4]- ربحي عزيزة، المرجع السابق، ص 106.

[5]- موقع الالكتروني:/https://www.alukah.net/culture/0/52639 يوم الاطلاع 2021/4/28، على الساعة 05: 23

الطائفة غالبا ما تكون من هواة الحاسوب، بحيث يقومون بأعمالهم هذه لمجرد إظهار أنهم قادرون على اقتحام المواقع الأمنية أو لمجرد ترك بصماتهم التي تثبيت وصولهم إلى تلك المواقع[1]. وهو مستخدم حاسوب غرضه التوصل إلى الدخول غير المصرح به إلى نظم الحاسوب[2].

فالهاكرز يعد شخصا بارعا في استخدام الحاسب الآلي ولديه فضول في استخدام حسابات الآخرين بطرق غير مشروعة[3].

وعليه يمكن القول بان "الهاكرز" هم الهواة أو المبتدئين الذين يكون هدفهم من اختراقهم للأنظمة الالكترونية التعلم والتسلية، فهم في الغالب لا يكون لديهم دوافع حاقدة أو تخريبية، الهدف هو اكتساب الخبرة والتحدي وإثبات الذات، أو بدافع الفضول.

وهناك أصناف مختلفة والذي يتم تصنيفهم حسب مجال خبرتهم وحسب الاتجاهات وهم ثلاثة نماذج:

أ-**قراصنة ذو القبعات البيضاء:** وهي مجموعات ذات المصلحة من المنظومات المعلوماتية، بحيث يقوم أفراد هذه المجموعة باختبارات في الاختراقات بالاتفاق مع أصحاب المنظومة لتحسين جودة الحماية لهذه المنظومات، فهؤلاء باحثين في اكتشاف نواقص برمجيات الحماية، وتحليل المنظومات والبروتوكولات، بهدف إدخال تحسينات في الحلول الوقائية ضد تهديدات القراصنة الآخرين[4].

ب- **قراصنة ذو القبعة السوداء:** هو الشرير أو الرجل السيئ، حيث تعود إلى اختراق الذي يقتحم الشبكات أو الحواسيب أو يصنع فيروسات الحاسوب للتخريب أو الحصول على المال[5].

ج- **القراصنة ذو القبعة الرمادية:** هم الأشخاص الذين يقع بين القبعة البيضاء وقبعة سوداء، يعتبر هذا النوع من المتسللين، قد يستخدم مهارته سواء للدفاع أو أغراض مسيئة[1].

---

[1]- نهلا عبد القادر المومني، المرجع السابق، ص 83.

[2]- هروال هبة نبيلة، جرائم الانترنت دراسة مقارنة، أطروحة دكتورة، جامعة أبي بكر بلقايد، تلمسان، 2014، ص52.

[3]- عبد الله دغش، المرجع السابق، ص 21.

[4]- زايد محمد، المرجع السابق، ص 75.

[5]- يشرى حسين الحمداني، المرجع السابق، ص 19.

ثانيا: الكراكرز (المحترفين)

ويطلق على المجرمون المحترفون في الجريمة المعلوماتية "الكراكرز" فهو الشخص الخبير في مجال الحاسب الآلي ولكنه يقوم بأنشطة غير قانونية كالتدمير الأنظمة المعلوماتية[2]، ويتميز هؤلاء بقدراتهم التقنية الواسعة وخبرتهم في مجال أنظمة الحاسوب والشبكات، وهم أكثر خطورة من الصنف الأول[3]، كما تتميز بالتنظيم والتخطيط للأنشطة التي ترتكب من قبل أفرادها[4]، والبعض الأخر يدخل من اجل تحقيق أغراض سياسية، وغالبا أعمار هؤلاء تكون بين 25 و40 سنة[5]. إن أهداف هذا الفريق أكبر وأخطر من الفريق السابق، فأهدافهم المصاريف وسحب الأموال من حسابات العملاء أو الولوج إلى أخطر المواقع وأكثرها حساسية، ببياناتها أو تدميرها[6]. ويتضح بان الكراكرز هم المحترفون المخترقون الذين يكونوا دخولهم إلى الحواسيب من اجل تحقيق أهدافهم، وعليه فان هذه الفئة أخطر من الأولى.

---

[1]– محمد سعد، المرجع السابق، ص 6.

[2]– بن منصور صالح وكوش أنيسة، السلوك الإجرامي للمجرم المعلوماتي، مذكرة لنيل شهادة الماستر في العلوم الجنائية، جامعة عبد الرحمان ميرة، بجاية، 2015، ص 38.

[3]– ريم ساسي، المرجع السابق، ص 25.

[4]– نايري عائشة، المرجع السابق، ص 21.

[5]– عبد الله دغش العجمي، المرجع السابق، ص 22.

[6]– الموقع الالكتروني: https://www.alukah.net/culture/0/52639 يوم الاطلاع 2021/4/28، على الساعة 05: 23

خلاصة:

وفي الأخير بعد تناولنا في هذا الفصل ماهية جريمة السرقة الالكترونية، أين بينا مختلف الآراء الفقهية في تعريف جريمة السرقة الالكترونية، انتهينا بأنها نوع من أنواع الجرائم المعلوماتية التي ترتكب بواسطة الكمبيوتر، بحيث يرتكب الجاني السرقة عن بعد، فهي تنطوي بوجه عام على ذات الصفات والخصائص التي تتمتع بها، ومع ذلك فان جريمة السرقة الالكترونية تتميز عن بقية الجرائم المعلوماتية الأخرى، بأنها تقع على المعلومات التي لها قيم مالية، ولذلك تعتبر جريمة خطيرة وسريعة ومتطورة .تبيان تميز بين سرقة الكترونية وقرصنة البريد الالكتروني والمراحل التي تمر بها لارتكاب الجريمة، وفي الأخير تم إبراز دوافع التي أدت بالجاني لارتكاب تلك الجريمة الخطيرة، والأساليب والتقنيات التي يستخدمها لدخول إلى المنظومة المعلوماتية. وفئات القراصنة المعلوماتية. ولذا سنحاول من خلال الفصل الموالي إبراز أركان وعقوبات جريمة السرقة الالكترونية، ونبين التطبيقات التي يقوم بها المجرم ووسائل المكافحة، جريمة السرقة الالكترونية باعتبارها جريمة خطيرة فهي في تزايد مستمر بسبب استخدام تلك التقنيات.

الفصل الثاني

الجوانب القانونية لجريمة السرقة الإلكترونية وآليات مكافحته

الفصل الثاني: الجوانب القانونية لجريمة السرقة الالكترونية وآليات مكافحتها

وفيما يخص الجوانب القانونية نطرق إلى العقوبات بحيث نستعرض أراء الفقهاء فيما يخص جريمة السرقة الالكترونية، بين معارض ومؤيد عن تطبيق القانون السرقة التقليدية. وهناك بعض التطبيقات يقوم بها المجرم المعلوماتي بمهاجمة الحاسوب بهدف قرصنة سواء البرامج أو معلومات شخصية وغيرها. وبما أن جريمة السرقة الالكترونية هي جريمة مستحدثة وتشكل خطرا وضرر على المجتمع، ولابد من مكافحتها، وحمايتها بطرق وسائل الوقاية من القرصنة. وسنحاول في هذا الفصل نتطرق الجوانب القانونية لجريمة السرقة الالكترونية وآليات مكافحتها، والتي قمت بتقسيمها إلى مبحثين، وعليه نستعرض في المبحث الأول أركان جريمة السرقة الالكترونية وتطبيقات التي يستخدمها الجاني لمهاجمة المنظومة المعلوماتية، وثانيا نتطرق فيه إلى العقوبات جريمة السرقة الالكترونية. وأما فيما يخص المبحث الثاني نستعرض فيه الوسائل الوقاية من الجريمة وطرق مكافحاتها.

المبحث الأول: أركان جريمة السرقة الالكترونية وتطبيقاتها

قمت بتقسيم هذا المبحث إلى مطلبين، بحيث نتطرق بالتفصيل إلى أركان جريمة السرقة الالكترونية صور وعناصرها بالتفصيل في المطلب الأول، ثم يليها تطبيقات التي يقوم بها الجاني لسرقة والتقاط غير المشروع للبيانات والمعلومات في المطلب الثاني، نستعرض أركان جريمة السرقة وهي: الركن المادي والذي يتمثل في فعل الاختلاس وعناصره،وتسليم المعلومات، وسنحاول التطرق أيضا إلى محل السرقة المعلوماتية والتي ندرس فيها طبيعة المال في المعلوماتية، ثم طبيعة المنقول في المعلوماتية، تليها ملكية الغير للمال المعلوماتي. وأخيرا الركن المعنوي بحيث ندرس فيه القصد العام والخاص.

وفي المطلب الثاني نستعرض فيه تطبيقات جريمة السرقة الكترونية والتقاط غير المشروع للبيانات، التي يقوم بها الجاني لمهاجمة الحاسوب لغرض شخصي، وأما فيما يخص تطبيقات فهي، سرقة البيانات المالية للهوية الشخصية، وسرقة الودائع،ونسخ المعلومات، ونسخ البرامج، أما فيما يخص التقاط غير مشروع للبيانات فالجاني يتبع هذه الأساليب والطرق والمتمثلة في التجسس الالكتروني، وأسلوب الخداع،وتقنية تفجير أو تدمير المواقع.

المطلب الأول: أركان جريمة السرقة الالكترونية

نتطرق في هذا المطلب إلى أركان جريمة السرقة الالكترونية، من حيث وجود ركنين أساسين والتي قمت بتقسيمه، نستعرض في الفرع الأول نتطرق إلى محل السرقة في المعلوماتية والتي ندرس بالتفصيل طبيعة المال في المعلوماتية،ثم طبيعة المنقول في المعلوماتية،وتليها ملكية الغير لمال المعلوماتي، بينما في الفرع الثاني نستعرض الركن المادي بحيث نتطرق فيه إلى فعل الاختلاس وعناصره وأما الركن المعنوي في الفرع الثالث نتطرق في هذا إلى القصد العام والقصد الخاص.

الفرع الأول: محل السرقة المعلوماتية

هناك خلاف فقهي عن سرقة المعلومات إذا كان المال محل الجريمة، ولذلك نشير في هذا الصدد إلى أراء الفقهاء بين مؤيد ومعارض عن محل السرقة المعلوماتية، ونتطرق أولا إلى طبيعة المال في المعلوماتية، ثم تليها طبيعة المنقول في المعلوماتية، وثالثا ملكية الغير للمال المعلوماتي.

أولا: طبيعة المال في المعلوماتية

تنقسم الأموال في المعلوماتية إلى عنصرين إما يكون مال مادي وهي العناصر المادية للحاسب، والتي تحتوي على كيان مادي ملموس ولا خلاف فيها بين الفقهاء، بحيث يرى الرأي المؤيد بصلاحية البرامج والبيانات لان تكون محلا لجريمة السرقة[1].

واستندوا في ذلك: بان المختلس لهذه المعلومات يمكنه نقلها على دعامة مادية، وأيضا البيانات والبرامج والمعطيات المخزنة بالحاسب الآلي لها كيان مادي يترجم إلى أفكار على شاشة الكمبيوتر، وبحيث أن المعلومات يمكن أن تقبل قياس سرقة البيانات والبرامج الكمبيوتر على سرقة الكهرباء[2]. وهناك رأي معارض يرى عكس ذلك بحيث ذهب رأي منهم إلى المعلوماتية لا تصلح بان تكون محلا لجريمة السرقة،بان المعلومات لا تصلح أن تكون مالا أو محلا للسرقة إلا إذا اقترنت بالمادية لذلك فان التعدي عليها بالسرقة لا يعتد به، إلا في حالة وجودها مسجلة على دعامات أو اسطوانات فهي تصبح في ذلك أموالا تصلح محلا للسرقة[3].

ثانيا: طبيعة المنقول في المعلوماتية

هناك من يرى بان المعطيات المعلوماتية منقولا، وهناك جانب من الفقه من يرى بأنها ليست منقولا.

ونشير إلى حجج التي استندوا فيها أنصار الرأي المعارض: بان المعلومات المخزنة سواء في النظام المعلوماتي أو في أي وسيط لا تعتبر في حد ذاتها أشياء مادية فلا يتصور انتزاعها وحيازتها ولا تكون محلا للسرقة[4].

أما الرأي المعارض يرى عدم اعتبار المعلوماتية منقولا وذلك للأسباب التالية، بان القيمة المعلوماتية أكبر بكثير من القيمة المالية للدعامة، وأن عدم اعتبار شاشة الكمبيوتر شيء وبالتالي فلا تصلح لان تكون محلا لجريمة السرقة[5].

---

[1]– دحمان صبايحية خديجة، جرائم السرقة والاحتيال عبر الانترنت دراسة مقارنة بين الفقه الإسلامي والقانون الجزائري، مذكرة لنيل شهادة الماجستير في العلوم الإسلامية، الجزائر، 2013، ص 55.

[2]– دحمان صبايحية خديجة، مرجع سابق، ص 55.

[3]– رابحي عزيزة، المرجع السابق، ص 184.

[4]– العمري ابتسام، المرجع السابق، ص 29.

[5]– دحمان صبايحية خديجة، المرجع السابق، ص 56.

ثالثا: ملكية الغير للمال المعلوماتي

تشترط القواعد العامة للسرقة لوقوع الجريمة شرطين: فالأول: يتمثل في عدم ملكية المال محل السرقة، بينما الشرط الثاني: يتمثل في ملكية المال محل السرقة[1]، واستنادا لنص المادة 350 قانون العقوبات الجزائري يجب أن يكون محل الاختلاس ملكا للجاني، فإذا كان ملكا للغير فلا جريمة لان الغاية من التجريم هو حماية حق الملكية وليس تسليط العقوبة[2]. إذن المعلوماتية تصلح بان تكون محلا للملكية باعتبار أن التحليل المنطقي الذي لا يمكن إنكاره هو ملكيتها لشخص ما وبالتالي فهي ليست ملكا للسارق بل يقوم بالاستحواذ عليها، كشيء ليس مملوكا له وهذا هو جوهر الاختلاس في السرقة[3].

الفرع الثاني: الركن المادي

في الركن المادي سنحاول دراسة فعل الاختلاس وعناصره بحيث نتطرق إلى أراء الفقهاء المختلفة للنظام المعلوماتي أولا، ثم نتطرق إلى تسليم المعلومات ثانيا. وعلى ضوء هذا ندرس بالتفصيل:

أولا: فعل الاختلاس وعناصره في الانترنت

العنصر الموضوعي (الاستيلاء على المعلوماتية): لقد اختلف الفقهاء إلى رأيين، رأي يؤيد وجود الاختلاس في الاستيلاء على المعلوماتية، ورأي آخر معارض.

وبما أن الاختلاف موجود هناك أربع صور والمتمثلة في: "الطبيعة المعلوماتية، المعلوماتية المخزنة في النظام، سرقة وقت النظام المعلوماتي، المعلومات المخزنة على دعامات"[4].

الصورة الأولى: الطبيعة المعلوماتية

هناك تنازع فقهي حول الطبيعة المعلوماتية بان تكون محلا لاختلاس بين مؤيد ومعارض.

---

[1]– سالم محمد سالم بني مصطفى، المرجع السابق، ص 58.

[2]– دحمان صبايحية خديجة، مرجع نفسه، ص 56.

[3]– رابحي عزيزة، المرجع السابق، ص 189.

[4]– دحمان صبايحية خديجة، المرجع السابق، ص 50.

أولا: الرأي المؤيد

فقد ذهب جانب من الفقه إلى القول بإمكان اختلاس برامج الحاسب باعتبارها خلقا فكريا، وبالتالي فانه يمكن الوقوع فعل اختلاس عليها في الصورة تتناسب وطبيعة هذه البرامج[1] بحيث استندوا في ذلك إلى: أن المادة 350 قانون العقوبات الجزائري من "اختلس شيئا غير مملوك له يعد سارقا" بحيث كلمة "شيء" فإنها يمكن بان تكون معنوي يمكن الاستيلاء عليه[2] وكذلك يمكن اختلاس المعلوماتية باعتبارها خلق فكري، وبما أن معلومات قابلة للتحديد والقياس مثل: الطاقة الكهربائية[3].

ثانيا: الرأي المعارض

ذهب أنصار هذا الاتجاه بالقول إن المعطيات المعلوماتية لا تخضع لفعل الاختلاس، بحيث استندوا إلى حجج التالية:

بان معطيات المعلوماتية تتعارض مع اعتبارها من قبيل الأشياء، بحيث تتم الحصول عليها إما عن طريق السمع أو بالقراءة أو بطريق إعادة النسخ للبرامج على دعامات، كما أن المعطيات المعلوماتية هي ليست أموال[4] وأن الاختلاس اللازم لوقوع السرقة بمعناها المعروف غير متحقق لأنه ينطوي على تبديل الحيازة بحيث تنحصر في الحصول المنفعة الشيء فقط، دون أصل حيازة صاحبه، فسرقة منفعة بشرط وجود نص بهذا الأمر، وفي حالة عدم وجود نص فلا سرقة في الأمر[5] ويرجع السبب لعدم وجود قوانين خاصة بسرقة المعلومة بحد ذاتها وفي بعض الحالات يستحيل تطبيق نصوص السرقة على سرقة المعلومات اللامادية[6].

الصورة الثانية: سرقة (قرصنة) المعلوماتية المخزنة في النظام المعلوماتي

يوجد حالتين للصورة قرصنة المعلوماتية المخزنة في النظام المعلوماتي وهما: بحيث تتمثل الحالة الأولى في نسخ ونقل المعلوماتية من النظام المعلوماتي، والحالة الثانية هي التقاط

---

[1]– اختير مسعود، الحماية الجنائية لبرامج الكمبيوتر أساليب وثغرات، دار الهدى عين مليلة، الجزائر، طبعة 2010، ص51.

[2]– دحمان صبايحية خديجة، مرجع سابق، ص 51.

[3]– رابحي عزيزة، المرجع السابق، ص 191.

[4]– العمري ابتسام، المرجع السابق، ص 49.

[5]– سالم محمد سالم بني مصطفى، المرجع السابق، ص 61.

[6]– رابحي عزيزة، المرجع السابق، ص 191.

الذهني والسمعي للمعلوماتية من النظام المعلوماتي. وعلى ضوء هذا نتطرق بالتفصيل فيما يلي:

الحالة الأولى: نسخ ونقل المعلوماتية من النظام المعلوماتي

هناك رأي يرى عدم صلاحية المعلومات المخزنة في النظام للنسخ ورأي أخر يرى عكس ذلك بأنها تصلح للنسخ.

رأي معارض: استندوا بان النسخ وإتلاف الأصل لا يمكن أن يشكل تقليدا لبرامج لان العبرة في وجود التقليد[1].

فالجاني عند قيامه بنسخ ونقل المعطيات لم يستولي على أصل المال، بل نقل صورة عنها ولذلك يعتبر هذا الفعل وبدون ادني شك غير مشروع إلا انه لا يدخل في جريمة السرقة فقد يكون ذلك تقليدا أو سرقة منفعة حتى ولو تم تدميرها وإتلافها[2]. هذا الاتجاه ينكر صلاحية نسخ المعطيات من النظام المعلوماتي كمحل للاختلاس.

ويرى **رأي المؤيد:** بان فكرة الاستيلاء الاحتيالي لنسخ ونقل المعلوماتية هي إحدى صور التفسير الواسع للاختلاس، وأيدت المحكمة ذلك في قضية التي أدنت إحدى العمال بالسرقة عن حالة النسخ الفوتوغرافي للمستندات السرية حيث إن هذه المستندات تم الاستيلاء عليها احتيالا وانه وفق لرأي فقهاء المعلوماتية بان سرقة المعلوماتي تختفي وراء سرقة الأوراق والمستندات[3]. والمشرع الجزائري في تعريفه للسرقة اخذ بالمفهوم الواسع لها ولم يأخذ بالمفهوم الضيق، وبالتالي بإمكانية أن يكون المال محل السرقة معنوي غير مادي[4].

الحالة الثانية: الالتقاط الذهني والسمعي للمعطيات المعلوماتية

بحيث يذهب رأي مؤيد إلى قولهم إن الاستيلاء على البرامج بوجه مستقل ودون الاستعانة بالدعامة التي تحتويها، فان الاختلاس على البرامج بشأنها لا يمكن أن يتحقق إلا بنشاط ذهني يتم بموجبه ومن خلال السمع مثلا أو البصر التقاط المعلومات وحفظها[5].

---

[1]– محمد حماد مرهج الهيتي، التكنولوجيا الحديثة والقانون لجنائي، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2004، ص 243.

[2]– العمري ابتسام، المرجع السابق، ص 51.

[3]– سالم محمد سالم بني مصطفى، المرجع السابق، ص 63.

[4]– دحمان صبايحية خديجة، المرجع السابق، ص 52.

[5]– محمد حماد مرهج الهيتي، المرجع السابق، ص 206.

ويمكن الحصول على البرامج والمعلومة بتشغيل الجهاز ورؤية المعلومة على الشاشة فان المعلومة تنتقل من الجهاز إلى ذهن الملتقى وحيث إن موضوع حيازتها المعلوماتية غير مادي فان واقعية الحيازة تكون من نفس الطبيعة غير مادية "ذهنية "وبالتالي إمكانية حيازة المعلوماتية عن طريق الالتقاط الذهني عن طريق البصر أو السمع[1].

وبينما يرى فقهاء الرأي عكس ذلك بان المعطيات والبيانات غير صالحة للالتقاط الذهني والسمعي بحيث أن الصورة التي تظهر على شاشة النظام المعلوماتي ولو أنها تبدو كنشاط إنساني يمكن تقديرها بالجهد الفني الذي يبذله المختص إلا انه لا تعتبر مكتوبة ولا تصلح للسرقة[2] وعدم وجود نشاط مادي ملموس في هذه الحالة كدليل يقع على المختلس المعلوماتي[3].

الصورة الثالثة: سرقة وقت النظام المعلوماتي

لقد اختلف الفقهاء بين معارض ومؤيد على مدى صلاحية سرقة وقت النظام المعلوماتي بان تكون محلا للسرقة.

رأي المؤيد: بالنسبة لأصحاب هذا الرأي استندوا إلى المبررات التالية:فالسرقة وقت النظام المعلوماتي لا تحتاج للإثبات، حيث تعتبر مجرد تشغيل غير مشروع فهو سرقة لوقت العمل إذن هي تخضع لنصوص السرقة، وبحيث اعتبروا أن وقت استخدام المكونات المادية للنظام المعلوماتي يمكن أن تقوم بالمال أو أي قيمة مادية، وعليه إن استيلاء على وقت النظام المعلوماتي يعد استيلاء مادي وكما انه يمنع باقي المستخدمين بالاستفادة من هذا الوقت[4].

ويرى بعض الفقهاء بان سرقة وقت الآلة فهي من طائفة جرائم المعلوماتية، بحيث يلجاء العاملين بالنظام المعلوماتي لاستخدامه في أعمال خاصة بهم،وعليه تكون واقعة السرقة منصبة على وقت الجهاز الذي يمكن تقويمه ماليا، وتجدر أن واقعة السرقة لا تكمن في الشيء

---

[1]– سالم محمد سالم بني مصطفى، المرجع السابق، ص 64.

[2]– سام محمد سالم بني مصطفى، مرجع نفسه، ص 63.

[3]– دحمان صبايحية خديجة، المرجع السابق، ص 53.

[4]– العمري ابتسام، المرجع السابق، ص 54.

المسروق لضالة قيمته، بالمقارنة بما تحتويه هذه المكونات المادية من معلومات تقدر خسارتها بأموال طائلة[1].

والرأي المعارض: يذهب الفقهاء في رأيهم بعدم صلاحية سرقة وقت النظام المعلوماتي، بحيث استندوا في ذلك إلى اعتبارها سرقة منفعة أصل، بل تشكل جريمة نصب في حالة انتحال الشخص اسم أخر لكي يستطيع أن يستخدم الكمبيوتر أو ادعاءاته لصفة غير صحيحة، وفي هذه الحالة يعد المستخدم خائن للأمانة إذا استخدم الجهاز دون علم صاحبه[2]. نلاحظ بان في الركن المادي والذي يتمثل في اختلاس نظام المعلوماتي، والذي تطرقنا فيه إلى صورها، بحيث رأينا بان كل الصور لها أراء الفقهاء بين المعارض والمؤيد، وبما أننا في عصر تكنولوجيا الحديثة وفي تطور مستمر، نؤيد الرأي القائل بصلاحية المعلوماتية صالحة للاختلاس. بحيث المشرع الجزائري استحدث بعض النصوص القانونية لحماية المنظومة المعلوماتية من اعتداء وانتهاكها.

ثانيا: تسليم المعلومات

انقسمت الآراء القائلة فيما يتعلق بالتسليم فيما يخص المعلوماتية وأثره بالنسبة لجريمة السرقة، بينما كانت الآراء الفقهية والقضائية تتعلق بالتسليم الصادر من الحاسب الآلي لتوزيع النقود، في حين أننا نود أن نتحدث عن تسليم المعلومات الموجودة داخل الحاسوب لمختلسها ذلك يقتضي من وجهة نظرنا تطبيق القواعد العامة المتعلقة بالتسليم في جريمة السرقة التقليدية[3].

الفرع الثالث: الركن المعنوي

جريمة السرقة صنفها المشرع من الجنح، وبما أنها جريمة عمدية عبر الانترنت بحيث يتطلب لقيامها توافر القصد العام والخاص، ومن هذا المنبر نشير أولا إلى القصد العام، ثم نتطرق إلى القصد الخاص. بحيث القصد العام هو العلم والإرادة، بينما القصد الخاص هو النية في ارتكاب الجريمة، وعليه نتطرق بالتفصيل فيما يلي:

---

[1]– سوير سفيان، جرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، جامعة أبو بكر بلقايد، تلمسان، 2011، ص 40.

[2]– دحمان صبايحية خديجة، المرجع السابق، ص 54.

[3]– رابحي عزيزة، المرجع السابق، ص 196.

أولا: القصد العام لقيام جريمة السرقة يجب أن يعلم الجاني بان البرامج و البيانات مملوكة للغير، وإذا تحصل على المعلومات والبيانات بدون قصد "خطاء" بالبرامج ، فلا يكون مرتكبا لجريمة السرقة لانتفاء عنصر العلم[1] إن المجرم المعلوماتي مرتكب لجريمة سرقة المعلومات، يسعى بإرادته إلى الاستحواذ عليها بتشغيله ويعلم أنها مملوكة للغير وفي قيامه باختلاسها أو نسخها يعتبر قد توافر لديه عنصر القصد العام[2] بالإضافة إلى العلم يجب أن تتجه إرادة السارق إلى إخراج الشيء محل السرقة من حيازة المجني عليه وإدخاله في حيازته و تكون إرادة حرة بحيث إذا اكرهه شخص أخر لإخراج المال من حيازة صاحبه تخلفت لديه إرادة ارتكاب الاستيلاء وامتنع قيام السرقة[3].

ثانيا: القصد الخاص إلى جانب عنصر القصد العام والذي يتمثل في العلم والإرادة، يضاف عنصر القصد الخاص والذي يتمثل في النية الاستحواذ على الشيء.

يجب لقيام جريمة السرقة أن تتجه لدى الجاني نيته إلى تملك الشيء المختلس فإذا لم تتجه نيته إلى تملكه فلا تقوم الجريمة في هذه الحالة[4].

وعند ما ينتهك الجاني النظام المعلوماتي الخاص، الذي له كلمة السر ونظام أنمني خاص يدل على وجود قصد وسوء النية من مرتكب الفعل، ويتوفر فيها القصد العام والخاص ويظهر القصد الخاص في فترة البقاء غير المشروع إلا أن المشكلة التي تعترض ذلك هي كيفية إثبات سوء النية[5].

المطلب الثاني: تطبيقات جريمة السرقة الالكترونية والتقاط غير المشروع للبيانات

قمت بتقسيم هذا المطلب إلى فرعين، بحيث في الفرع الأول نستعرض تطبيقات جريمة السرقة الالكترونية والتي تتمثل أولا في سرقة البيانات المالية للهوية الشخصية، وثانيا سرقة الودائع، وثالثا نسخ المعلومات، ورابعا نسخ البرامج. وبينما في الفرع الثاني نتطرق فيه إلى التقاط غير المشروع للبيانات، والتي تتمثل في قيام الجاني بالتجسس الالكتروني، وأسلوب الخداع، وأخيرا تقنية تفجير أو تدمير المواقع. كل هذه الأساليب هي خطيرة وتهدد النظام

---

[1]– دحمان صبايحية خديجة، المرجع السابق، ص 56.

[2]– رابحي عزيزة، مرجع سابق، ص 197.

[3]– سالم محمد سالم بني مصطفى، المرجع السابق، ص 46.

[4]– دحمان صبايحية، مرجع سابق، ص 56.

[5]– رابحي عزيزة، مرجع سابق، ص 198.

المعلوماتي والمجتمع وخاصة التجسس الالكتروني الذي قد يمس اعتداء على أسرار الدولة وعلى ضوء هذا نستعرض بتفصيلها في الفروع.

الفرع الأول: تطبيقات جريمة السرقة الالكترونية

التطبيقات التي يقوم بها المجرم المعلوماتي بالدخول إلى النظام المعلوماتي من اجل سرقة البيانات والمعلومات والمتمثلة في:

أولا: سرقة البيانات المالية للهوية الشخصية

مع بداية استخدام البطاقات الائتمانية خلال شبكة الانترنت واكبت ظهور الكثير من المتسللين للسطو عليها، فالبطاقات الائتمانية تعد نقودا الكترونية والاستيلاء عليها يعد استيلاء على مال الغير، بحيث الاستيلاء على بطاقات الائتمان أمرا ليس بصعوبة مكان وذلك فان اللصوص يستطيعون سرقة مئات الآلاف من أرقام البطاقات في يوم واحد من خلال شبكة الانترنت[1] يقوم سارق استعمال البطاقة الائتمانية للحصول على السلع والخدمات أو سحب مبالغ مالية بموجبها من أجهزة التوزيع الآلي أو السحب باستخدام بطاقات مزورة[2].

وتعتبر البيانات المالية الخاصة بالهوية الشخصية من أكثر البيانات التي تتعرض للنسخ والسرقة وتتضمن هذه البيانات رقم بطاقة الائتمان،ورقم الحساب الضمان الاجتماعي، ويمكن الجاني من الاستيلاء على هذه البيانات ارتكاب جرائم اقتصادية متنوعة، بحيث يمكن للجاني ببيع هذه البيانات وتحقيق الربح منها، ويمكن أيضا استخدامها لارتكابها في عدة جرائم[3].

ثانيا: سرقة الودائع

سرقة الودائع الالكترونية تتم عن طريق الدخول إلى النظام الحاسب الآلي في البنوك، ومن ثم القيام بعمليات تحويل ونقل ودائع مالية من حساب إلى أخر، بحيث يقوم الجاني بإجراء قيود كتابية من حساب إلى أخر، وعليه يعتبر إجرائها عملية سرقة لودائع مالية، بحيث يتم من خلال أساليب الاختراق المختلفة والتي تتحقق السرقة بمجرد نقل الوديعة وإخراجها من حساب أخر[4] إن السطو على البنوك هو الهدف المفضل لقراصنة انترنت الذين يتلاعبون في كشوف

---

[1]– رصاع فتيحة، الحماية الجنائية للمعلومات على شبكة الانترنت، مذكرة لنيل شهادة ماجستير في قانون عام، جامعة أبي بكر بلقايد، تلمسان، 2012، ص 80.

[2]– سوير سفيان، المرجع السابق، ص 37.

[3]– احمد محمد عبد الرؤوف المنيفي، السرقة الالكترونية، المرجع السابق، ص 116.

[4]– احمد محمد عبد الرؤوف المنيفي، السرقة الالكترونية، مرجع نفسه، ص 117.

وحسابات العملاء ونقل الأرصدة من حساب لأخر، ونظرا لخطورة جريمة السطو[1] بحيث يقومون بإضافة أرقام أو أصفار إلى أرقام ما في هذا الحساب[2].

ثالثا: نسخ المعلومات

تشمل المعلومات المقالات والأبحاث والكتب والصوت والصورة والفيديو، وتخزن هذه الأنواع المختلفة من المعلومات في أنظمة الكمبيوتر داخل قواعد بيانات، وقد كانت قواعد بيانات، وقد كانت البيانات التقليدية تخزن النصوص فقط، أما التطبيقات الحديثة لقواعد البيانات فبإمكانها، أيضا تخزين الصوت والصورة في موقع اليوتيوب الذي يخزن الصوتيات ومقاطع الفيديو[3] ومع أن كثير من المعلومات متاح للتحميل والنسخ مجانا من الانترنت، إلا أن منها ما يقتضي رسوما مالية مقابل السماح بنسخة[4] نسخ البيانات أو المعلومات أو التصاميم العائدة للمجني عليه والتي يحصل عليها الجاني بالنسخ مع بقاء النسخة الأصلية في حيازة المجني عليه[5]. وسرقة المعلومات المخزنة في جهاز الحاسوب أو المتبادلة عبر الشبكة العالمية للمعلومات (الانترنت) تعتبر من أكثر أساليب انتشارا في مجال الاعتداء على المعلومات، ويطلق البعض على هذه الجريمة: "**جريمة قرصنة المعلومات**" والتي تجري هذه العملية –السرقة– من خلال وصول الأفراد الغير المرخص لهم إلى المعلومات والبيانات وبرامج الحاسوب[6].

من خلال ما تقدم نستخلص بان المعلومات المتواجدة داخل الكمبيوتر يمكن نسخها من طرف الأشخاص الغير المصرح بهم بالدخول إليها بحيث يقوم القراصنة بنسخ الغير المشروع على المعلومات والبيانات،ورغم انه لا يأخذ النسخة الأصلية إلا أن هناك بعض المعلومات لا يمكن نسخ لأنها تحمل حقوق الطبع والنشر للمؤلف، والتي أطلق عليها **جريمة قرصنة المعلومات** بحيث انتشرت بكثرة في الأواني الأخيرة.

---

[1]– مرابطن حياة، المرجع السابق، ص 18.

[2]– رصاع فتيحة المرجع السابق، ص 48 .

[3]– احمد محمد عبد الرؤوف المنيفي، السرقة الالكترونية، المرجع السابق، ص 118.

[4]– مرجع نفسه.

[5]– طارق الخن، المرجع السابق، ص 34.

[6]– نهلا عبد القادر المومني، المرجع السابق، ص 99.

رابعا: نسخ البرامج

إن الاقتحام أو التسلل هي النسخ الغير المشروع لنظام الحاسب الآلي أو البرنامج معين من برامج الحاسب الآلي المختلفة، أدت قرصنة البرامج إلي خسائر مادية باهظة جدا والتي وصلت في عام 1988م إلى احد عشر مليار دولار أمريكي في مجال البرمجيات طبقا لبعض الإحصاءات التي أجريت في هذا الشأن[1] يتطلب نسخ البرامج أولا كسر كلمة المرور الخاصة به، ومن ثم ينتقل إلى جهاز الجاني، هو نسخة البرامج فقط، أما الأصل يبقى لدى المجني عليه، ومع ذلك فان نسخ برنامج معين يفقد المصنف له حقه في بيع هذه البرنامج والحصول على أرباح منه[2]، وأكثر البرامج التي تتعرض للنسخ هي برامج الألعاب، وبرامج الأعمال والتجارة، والسبب في ذلك هو ارتفاع تكلفة هذه البرامج، وذلك يقوم الجناة بنسخها[3].

من خلال ما سبق نلاحظ بان نسخ الغير المشروع للبرامج يؤدي إلى خسائر كبيرة، بحيث يقوم الجاني بكسر كلمة السر ليدخل للنظام المعلوماتي، والتي يتم بتطبيق الخطوة الأخيرة وهي النسخ برنامج معين وقد تكون هذه البرامج هي برامج تعليمية مثلا،أو برامج العاب، أو غيرها من البرامج، فهي تؤدي إلى فقدان المصنف له حقه في بيع برنامج، لأنه أصبح البرنامج ليس ملكه وحده بل توجد نسخة لدى الجاني بحيث يمكن لهذا الأخير ببيعها اقل ثمن أو يزيد الثمن.

الفرع الثاني: التقاط غير مشروع للبيانات

يقصد بالالتقاط المشاهدة أو الحصول على ما هو مرسل عبر الشبكة المعلوماتية، والمجرم المعلوماتي يقوم بالتقاط البيانات بعد الدخول غير المشروع إلى النظام أو البقاء فيه[4]. بحيث تتمثل هذه الطرق في التجسس الالكتروني أولا، ويليها أسلوب الخداع ثانيا، وثالثا تقنية تفجير أو تدمير موقع الكتروني.

---

[1]– العيهار فاطمة الزهراء وبراشد منال، جريمة سرقة المال المعلوماتي عبر الانترنت، مذكرة لنيل شهادة الماستر في قانون عام، المركز الجامعي بلحاج بوشعيب، عين تموشنت، 2017، ص 24.

[2]– احمد محمد عبد الرؤوف المنيفي، السرقة الالكترونية، المرجع السابق، ص 119.

[3]– احمد محمد عبد الرؤوف المنيفي، مرجع نفسه، ص 118.

[4]– عبد الله ماجد المطلب العكايلة، سرقة البيانات والمعلومات الالكترونية دراسة مقارنة، كلية العلوم والدراسات الإنسانية، جامعة الأمير سطام بن عبد العزيز، ص 2189.

أولا: التجسس الالكتروني

يقوم القراصنة الحاسب الآلي باستخدام البرامج التي تنتج لهم الاطلاع على البيانات الخاصة بالشركات والمؤسسات العامة على شبكة انترنت وبالتالي يتمكنوا من الحصول على ما يردوا من المعلومات مختلفة[1] بحيث يكمن الخطر الحقيقي في عمليات التجسس التي تقوم بها الأجهزة الاستخبارية، للحصول على أسرار ومعلومات الدولة ثم إفشائها لدولة أخرى، والتي تكون عادة معادية، أو استغلالها بما يضر المصلحة الوطنية[2].

ولقد نص المشرع الجزائري على جريمة التجسس في **المادة 64 من قانون العقوبات،** والتي اشتملت في النص بصفة أساسية على التجسس الذي يستهدف امن الدولة،والملاحظ أن المشرع قد راعى أخطار التجسس المعلوماتي الذي يتم بوسائل تقنية معلوماتية، وهذا ما نص عليه في **المادة 63 فقرة 2 من قانون العقوبات: (...الاستحواذ بأية وسيلة كانت على مثل المعلومات أو الأشياء أو المستندات أو التصميمات بقصد تسليمها إلى دولة أجنبية أو أحد عملائها).**[3]

نلاحظ بان التجسس الالكتروني هو أسلوب خطير يستعمله القراصنة الحاسوب سواء للاطلاع أو جمع المعلومات وأسرار الشركات أو المؤسسات، أو قد تكون معلومات تخص دولة معينة وإفشاء أسرارها لدى دولة أخرى والتي تشكل خطر على امن الدولة،وبالنسبة للمشرع الجزائري فقد نص في قانون العقوبات **في مادة 64 (يرتكب جريمة التجسس ويعاقب بالإعدام كل أجنبي يقوم بأحد أفعال المنصوص عليها في الفقرات 2 و3 و4 من المادة 61 وفي المادتين 62 و62).** نلاحظ بان المشرع الجزائري في هذه المادة شدد العقوبة والتي تمثلت في الإعدام إذا كان لشخص الأجنبي بالاستحواذ على المعلومات وغيرها من الأفعال.

ثانيا: أسلوب الخداع

وذلك بإنشاء موقع وهمي تشبه المواقع المشهورة فيدخل لها المشتري ويدخل بياناته فيأخذها القرصنة ويستخدمونها لمصالحهم[4] ويعتبر أسلوب الخداع المتبع من قبل قراصنة

---

[1]– مرابطن حياة، المرجع السابق، ص 19.

[2]– رصاع فتيحة، المرجع السابق، ص 77.

[3]– بن زرت أسيا، إثبات الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في قانون الجنائي، جامعة عبد الحميد بن باديس مستغانم، 2019، ص 15.

[4]– دحمان صبايحية خديجة، المرجع السابق، ص 50.

الكمبيوتر للحصول على البيانات والمعلومات أقرب إلى وصف لاحتيال، بحيث يقوم المجرم المعلوماتي بإتباع سلوك لإيهام المجني عليهم بوجود مشروع كاذب بغرض الحصول على معلومات واستغلالها بصورة غير مشروعة[1].

ويتحقق هذا الأسلوب بإنشاء مواقع وهمية على شبكة الانترنت المشابهة تماما لمواقع الشركات والمؤسسات التجارية الأصلية الموجودة على هذه الشبكة، ولإنشاء هذا الموقع يقوم القراصنة بالحصول على كافة بيانات الموقع الأصلي، من الانترنت مع تعديل بياناته، والذي يصبح يستقبل كافة المعاملات المالية والتجارية التي يقدمها الموقع الأصلي لأغراض تجارية ومن بينها البيانات الخاصة ببطاقات الائتمان والرسائل الالكترونية[2].

هدف قراصنة الحاسوب من استخدام أسلوب الخداع هو من اجل حصول على المعلومات والبيانات الأشخاص بإنشاء مواقع وهمية لأغراض تجارية وعليه يحصل المجرم المعلوماتي على البيانات بصورة غير مشروعة.

ثالثا: تقنية تفجير أو تدمير المواقع

يقصد بتدمير المواقع به: الدخول الغير المشروع على نقطة ارتباط أساسية أو فرعية متصلة بالانترنت من خلال نظام ألي أو مجموعة نظم مرتبطة شبكيا بهدف تخريب نقطة أو النظام[3] يعتمد هذا الأسلوب على ضخ كميات كبيرة من الرسائل الالكترونية من جهاز الحاسب الآلي للجاني إلى الجهاز المستهدف، بحيث يشكل هذا الكم من الرسائل الالكترونية ضغط يؤدي في النهاية إلى تفجير الموقع العامل على الشبكة لتشتيت المعلومات والبيانات المخزنة فيه لتنتقل بعد ذلك إلى الجهاز الخاص بالمجرم[4]، أو تمكنه من حرية التجول في الموقع المستهدف بسهولة ويسر، فيستولي بذلك على ما يشاء من أرقام و بيانات خاصة ببطاقات ائتمانية مملوكة لغيره[5].

---

[1]– حمزة بن عقون، المرجع السابق، ص 138.

[2]– هروال هبة نبيلة، المرجع السابق، ص 289 .

[3]– عبد الرحمان عبد الله سند، المرجع السابق، ص 283.

[4]– حمزة بن عقون، مرجع نفسه، ص 141.

[5]– هروال هبة نبيلة ، المرجع السابق ، ص 290 .

المبحث الثاني: عقوبة جريمة السرقة الالكترونية وآليات مكافحتها

أضحى بان السرقة هي جريمة يرفضها المجتمع والقانون، بحيث اجمع الفقهاء والقضاء وبعض التشريعات بدراسة هذه الظاهرة، ونشير في هذا في المبحث إلى عقوبات ومواقف التشريعات من جريمة السرقة الالكترونية، ومن جهة أخرى موقف تشريع الجزائري، ثم نستعرض آليات الوقاية والمكافحة من هذه الجريمة التي تشكل خطرا على المجتمع.

المطلب الأول: موقف التشريعات من جريمة السرقة الالكترونية

نبين في هذا المطلب نتطرق إلى مواقف تشريعات الغربية والعربية في الفرع الأول من جريمة السرقة المعلوماتية، وأما الفرع الثاني نتطرق موقف التشريع الجزائري.

الفرع الأول: موقف تشريعات الغربية من السرقة عبر الانترنت

سنبين في هذا الفرع موقف التشريع الفرنسي من السرقة عبر الانترنت وموقف تشريعات العربية.

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 المادة311-2 إذ اعتبر أن اختلاس الطاقة أضرارا بالغير يعد سرقة[1]. فالتشريع الفرنسي نص قانون العقوبات الجديد على تجريم سرقة المال المعلوماتي متمثلا في المعلومات والبرامج، وذلك بموجب الفقرة الأولى من المادة 307، إذ تقرر المادة أن كل من التقط بطريق الاختلاس والتحايل برامج أو معلومات أو أي عنصر من عناصر نظام المعالجة الآلية للبيانات، تعاقب بالحبس مدة ثلاث سنوات وبغرامة مقدارها مليون فرنك[2]. 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 اقره الفقه والقضاء الانجليزي في الكثير من القضايا[3].

---

[1]- هروال هبة نبيلة، المرجع السابق، ص 187.

[2]- أنسام سمير طاهر، المرجع السابق، ص 146.

[3]- هروال هبة نبيلة، مرجع نفسه، ص 188.

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. ويعد من الأموال المنقولة في حكم قانون العقوبات الطاقة الكهربائية وجمع أنواع الطاقة ذات القيمة الاقتصادية"[1] 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 نكون أمام الجريمة فلابد أن يكون الاعتداء واقعا على منقول له صفة المال بالإضافة إلى حيازة الغير له[2] فهي اكتفت بتطبيق قوانينها العقابية التقليدية الخاصة بجريمة السرقة[3]. 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...).**[4]

ومن خلال ما سبق نلاحظ بان مواقف التشريعات هناك من استحدث نصوص لتجريم جرائم التي ترتكب على الحاسب الآلي وهناك بعض التشريعات اكتفت بالقوانين التقليدية.

الفرع الثاني: موقف التشريعات الجزائري من جريمة السرقة عبر الانترنت

تناول المشرع الجزائري السرقة في القسم الأول من الفصل الثالث المعنون بالسرقات وابتزاز الأموال **في المواد 350 إلى 369 من قانون العقوبات الجزائري**، بحيث عرف السرقة في **المادة 350 من قانون العقوبات**، بأنها: "**اختلاس شيء مملوك للغير**" وإن عدم تحديد طبيعة الشيء محل السرقة هو الذي دفع المشرع لإمكانية تجريم اختلاس المياه والكهرباء على

---

[1]– هروال هبة نبيلة، المرجع السابق، ص 189.

[2]– عبد الله ماجد عبد المطلب العكايلة، المرجع السابق، ص 2163.

[3]– هروال هبة نبيلة، مرجع نفسه، ص 189.

[4]– أنسام سمير طاهر، المرجع السابق، ص 147.

الرغم من أنها ليست طبيعة مادية،وعليه يمكن اعتبار الأفكار والمعلومات طاقة ذهنية يصدق عليها المعنى وتقبل التملك والحيازة من خلال الدعامة التي توجد عليها[1].

ونلاحظ مما تقدم أنه يمكن استخدام النصوص التقليدية فيما يخص جريمة السرقة الالكترونية، لان المشرع الجزائري لم يحدد في نص **المادة 350 قانون العقوبات** مصطلح "الشيء" إذا كان مادي أو الشيء معنوي.

وفي هذا الشأن أيضا نحن نقترح أن يستخدم المشرع الجزائري في حين تصديه للسرقة المعلوماتية بنص خاص بها أن يعبر عنها بمصطلح القرصنة هذا للتفرقة بين السرقة التقليدية وبين السرقة المعلوماتية[2].

المطلب الثاني: مكافحة جريمة السرقة الالكترونية في إطار القوانين الخاصة

نشير في هذا المطلب إلى مكافحة عن جريمة التي انتشرت بسرعة، والتي تعتبر أخطر جريمة مستحدثة بسبب انتشار تقنيات القرصنة ولهذا نتطرق إلى بعض العقوبات التي يمكن للقاضي أن يعاقب بها المجرم المعلوماتي، من اجل الحماية والتصدي لهذه الجريمة والتي نستدرجها في فرعين المواليين، بحيث نتطرق في الفرع الأول العقوبات المنصوص في **الأمر رقم 03-05 المتعلق بحق المؤلف والحقوق المجاورة**، وفي الفرع الثاني نتطرق إلى العقوبات المنصوص عليها في **قانون 09-04 المتضمن قانون العقوبات.**

الفرع الأول: العقوبات المنصوص في الأمر رقم 03-05 المتعلق بحق المؤلف والحقوق المجاورة

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 جويلية 2003 فيما يخص براءة الاختراع **(لا تعد من قبيل الاختراعات في مفهوم هذا الأمر برامج الحاسوب)** فالمشرع قد تبنى نظام حق المؤلف كبيئة لحماية البرامج دون نظام البراءة[3] 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

---

[1]- هروال هبة نبيلة، المرجع السابق، ص 189.

[2]- رابحي عزيزة، المرجع السابق، ص 199.

[3]- خثير مسعود، المرجع السابق، ص 76.

والتي أصبح لها قانون خاص، في قانون العقوبات المادة 393 تقر الغرامة كعقوبة للاعتداء على حق المؤلف، بينما الأمر 93-17 والأمر 03-05 يقرران عقوبتي الحبس والغرامة[1].

والغي هذا الأمر كذلك بموجب الأمر 03-05 حيث نجد عقوبات أصلية وعقوبات تكميلية.

- **عقوبات أصلية:**

نصت المادة 153 من الأمر 03-05 الصادر في 1003/07/19 المتعلق بحق المؤلف والحقوق المجاورة المعدل و المتمم 73-14 على عقوبة التقليد بقولها **(يعاقب مرتكب جنحة تقليد مصنف أو أداء كما هو المنصوص عليه في المادتين 151 و152 أعلاه بالحبس من ستة أشهر (6) إلى ثلاثة (3) سنوات و بغرامة مالية من خمسمائة ألف دينار (500.000دج) إلى مليون دينار (1.000.000دج) سواء كان النشر قد حصل في الجزائر أو في الخارج)** وكما نصت المادة 154 ق.ح.ح.م كذلك: **(يعد 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)**[2] 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 أخر خرقا للحقوق المعترف بها[3].

- **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 العتاد الذي تم ضبطه وحجزه والذي استعمل في إنتاج النسخ المقلدة[4]. وفي **المادة 156 من الأمر رقم 03-05** منح للجهة القضائية حق غلق المؤسسة التي يستغلها

---

[1]- صغير يوسف، المرجع السابق، ص 107.

[2]- خثير مسعود، المرجع السابق، ص 99.

[3]- خثير مسعود، مرجع نفسه، ص 100.

[4]- بواري احمد، الحماية القانونية لحق المؤلف والحقوق المجاورة في التشريع الجزائري والاتفاقيات الدولية، أطروحة لنيل درجة الدكتورة في العلوم القانونية في قانون جنائي، جامعة باتنة 1، 2015، ص 130 و301.

المقلد أو شريكه كمؤسسات التوزيع والبيع بالتجزئة لكن بشرط أن تقوم بإنذار المخالف بواسطة السلطة العمومية[1].

الفرع الثاني: الحماية في قانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بالتكنولوجيا الإعلام والاتصال 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[2] ولذلك اوجد 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 القضائية، وهذا تحت طائلة العقوبات المنصوص عليها في ذات القانون[3]. وكما أنشاء هيئة وطنية للوقاية من الإجرام المتصل بتكنولوجيات الإعلام والاتصال ومكافحته وسن أحكام خاصة بالتعاون والمساعدة القضائية الدولية[4].

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[5].

---

[1]– بواري احمد، مرجع سابق، ص 302.

[2]– سمية مزغيش، مرجع نفسه، ص 65.

[3]– عبد الصديق شيخ، الوقاية من الجرائم الالكترونية في ظل القانون رقم 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مجلة معالم للدراسات القانونية والسياسية، المجلد 4، العدد1، 2020، ص 197.

[4]– سوير سفيان، المرجع السابق، ص 22.

[5]– براهيمي جمال، مكافحة الجرائم الالكترونية في التشريع الجزائري، المجلة النقدية، كلية والعلوم السياسية، جامعة مولود معمري، تيزي وزو، ص 154.

الفرع الثالث: العقوبات المنصوص في قانون 04-15 المتضمن قانون العقوبات

سعى المشرع الجزائري في تعديله الأخير لقانون العقوبات من الأمر 66-165 إضافة قسم سابع مكرر عنونه "المساس بأنظمة المعالجة الآلية للمعطيات" ويشمل المواد من 394 مكرر إلى 394 مكرر 7.[1] 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 من 50.000دج إلى 200.000دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك).**[2]

ويقصد بفعل الدخول هنا هو الركن المادي لجريمة الاعتداء على نظام المعالجة الآلية للمعطيات، ذلك الدخول المعنوي أو الالكتروني باستعمال الوسائل الفنية والتقنية إلى النظام المعلوماتي، ولا يعد فعل الدخول بحد ذاته سلوكا غير مشروع وإنما يتخذ وصفه الإجرامي انطلاقا من كونه قد تم دون وجه حق أو دون ترخيص[3]. 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 لمعطيات المنظومة. وإذا ترتب عن أفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة (6) أشهر إلى سنتين (2) والغرامة من 50.000دج إلى 150.000دج). وأورد المشرع ظرفين لتشديد عقوبة الدخول غير المشروع إلى المنظمات المعلوماتية، وهو حذف أو تغيير المعطيات وظرف ثاني هو تخريب نظام اشتغال المنظومة[4].

- **الاعتداء على المعطيات الداخلية:** وحدد المشرع عقوبة الاعتداء العمدي على المعطيات الموجودة داخل النظام في **المادة 394 مكرر 1 "بالحبس من ستة أشهر إلى ثلاث**

---

[1]- خثير مسعود، المرجع السابق، ص 108.

[2]- فتيحة مهري، جريمة الدخول والبقاء إلى أنظمة المعالجة الآلية للمعطيات، مذكرة لنيل شهادة الماستر في قانون جنائي أعمال، جامعة العربي بن مهيدي، أم البواقي،2016، ص 36.

[3]- براهيمي جمال، المرجع السابق، ص 126.

[4]- صغير يوسف، المرجع السابق، ص 108.

سنوات وبغرامة من 500000دج إلى 2000000دج. كل من ادخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها"[1] ويقصد بالأفعال المنصوص عليها في المادة:

- **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)[2].
- **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[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[4].

كما أن أفعال الإدخال والمحو والتعديل وردت على سبيل الحصر، ومنه لا يقع تحت طائلة التجريم أي فعل أخر غيرها حتى ولو تضمن اعتداء على المعطيات الموجودة داخل نظام المعالجة الآلية للمعطيات[5].

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 التحصل

---

[1]– الأمر رقم 04–15 المؤرخ في 10 نوفمبر 2004 المتمم والمعدل للأمر 66–156 المتضمن قانون العقوبات.

[2]– بدري فيصل المرجع السابق، ص 175 و176.

[3]– بدري فيصل، مرجع نفسه، ص 176.

[4]– بدري فيصل، المرجع سابق، ص 176.

[5]– سوير سفيان، المرجع السابق، ص 94.

عليها من إحدى الجرائم الماسة بالأنظمة المعلوماتية بنص **المادة 394 مكرر 2 بالحبس من شهرين إلى ثلاث سنوات وبغرامة من 1000000دج إلى 5000000دج**[1].

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**[2] 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**[3] 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 للأشخاص الطبيعيين بصفتهم فاعلين أو شركاء في نفس الجريمة.[4]

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[5]. نلاحظ 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 156/66 المتضمن قانون العقوبات**، والذي استحدث

---

[1]- بدري فيصل، مرجع نفسه، ص 197.

[2]- سوير سفيان، المرجع السابق، ص 38.

[3]- قانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل و المتمم للأمر 156/66 المتضمن قانون العقوبات.

[4]- صغير يوسف، المرجع السابق، ص 111.

[5]- رابحي عزيزة، مرجع نفسه، ص 250.

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[1].

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.**[2] 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)**[3].

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[4].

المطلب الثالث: وسائل وطرق التصدي للحماية من برامج الفيروسات

يعتبر الحاسب الآلي، والهواتف الذكية أكثر عرضة لاختراق والسرقة وتدميرها من طرف القراصنة، وما جعل الخبراء في هذا المجال التقنية بالمكافحة والحماية للبرامج والبيانات المتواجدة لحماية الحاسب الآلي من أي اختراق ونشر الفيروسات بحيث قاموا بإنشاء برمجيات مضادة للفيروسات من اجل حماية البرامج والبيانات من القرصنة، باستعمال الطرق للوقاية منها. وعليه قمت بتقسيم المطلب إلى فرعين:نتطرق في الفرع الأول إلى وسائل التصدي عن

---

[1]– سوير سفيان، المرجع السابق، ص 22.

[2]– رابحي عزيزة، المرجع السابق، ص 247.

[3]– رابحي عزيزة، مرجع نفسه، ص 247.

[4]– صغير يوسف، مرجع سابق، ص 110.

طريق برامج مكافحة الفيروسات، بينما نتطرق في الفرع الثاني إلى طرق الوقاية من برامج الفيروسات.

الفرع الأول: وسائل التصدي عن طريق برامج مكافحة الفيروسات

نشير في هذا الفرع إلى الوسائل التي يجب إتباعها وهي عبارة عن برامج لمكافحة فيروسات التي تدخل إلى الكمبيوتر أو الهواتف الذكية وبذلك قد تكون هذه على شكل إعلان تظهر على شاشة كمبيوتر أو قد تكون مواقع العاب وغيرها،ومن اجل تفادي السرقة يجب إدخال برمجيات مخصصة لمكافحة هذه الفيروسات من اختراق وهي كالتالي:

- البرمجيات المضادة للفيروس والديدان: وهي برمجيات صممت وأنجزت للتعرف على الفيروس أو الدودة وإبطال مفعولها بتجميدها. وان لم تستطيع حذفها من الجهاز أو المنظومة. وقد اختصت عدة شركات في تصميم وانجاز تلك البرمجيات المضادة، لكن القرصنة والمخربين لا يكفون عن تطوير منتجاتهم مما يجعل شركات الحماية والسلامة مضطرة إلى تحديث منتجاتها كي تحد من مفعول البرمجيات الخبيثة. بحيث وصل منتجو البرمجيات إلى تصميم برمجيات أخرى لمكافحة الفيروسات[1].
- برامج كاشفة: تستطيع التعرف إلى ملفات التجسس وتقوم بإزالتها من الجهاز، لكن هناك بعض ملفات التجسس قد لا تستطيع برامح مكافحة الفيروس اكتشافها، ولهذا لا بد من تجنب وضع قوائم بكلمات السر أو الاستخدام على الجهاز، وخصوصا أرقام الحسابات البنكية، وبطاقات الائتمان، مع التقليل من الدخول على الحسابات البنكية عبر الانترنت ما أمكن وعدم الاحتفاظ بتقارير سرية تحتوي أرقاما مهمة على قرص الصلب[2].
- تشفير البيانات: هو عملية تحويل المعلومات المرسلة عبر الشبكة إلى رموز سرية بحيث تصبح غير قابلة للقراءة أو الفهم إلا من الأشخاص الصرح لهم، وهي عملية تعميمية المعلومات كوسيلة للحفاظ على امن المعلومات في بيئة غير أمنة.وهناك نوعين وهي تشفير متماثل: الذي يستخدم فيه مفتاح شفرة واحدة لكل من عمليتي التشفير وفك الشفرة،

---

[1]– زايد محمد، المرجع السابق، ص 79.

[2]– عبد الرحمان عبد الله سند، المرجع السابق، ص 400.

وهناك تشفير الغير متماثل: والذي يستخدم فيه مفتاحان أحدهما في التشفير والأخر في فك التشفير، يستخدم لحماية البيانات ضد الاطلاع على المعلومات[1].

- الجدار النارية: هي مجموعة أنظمة توفير أساليب أمنية بين الانترنت وشبكة المؤسسات أو الشركات وغيرها، لكي تجبر جميع عمليات الدخول إلى الشبكة، الخروج منها أن تمر خلال الجدار الناري الذي يقوم بصد اختراقات المستخدمين المتطفلين، وهو يوفر في ذات الوقت حواجز أمنية قبل الدخول إلى الموقع المعني، مثل التحقق من المستخدمين المحليين والخارجيين ونظام الدخول والخروج[2] تتمثل في أجهزة مختصة في تقصي البرمجيات هذه المنظومات سواء على حواسيب منفردة أو على شبكات، بحيث تعمل هذه المنظومات على مراقبة كل المعطيات النافذة وتقوم بتحليلها حسب المعلومات والأوامر التي تلقاها على شكل ملفات وعناصر تركز عليها[3]، وكما تحمي الموقع على شبكة الانترنت، أو على الشبكة الخاصة من محاولات الدخول العشوائية، كما يمكن استخدام بعض الوسائل المساعدة تتبع محاولات الدخول إلى النظام و معرفة مرتكبها[4].
- الحماية عن طريق أنظمة التشغيل: ظهر حديث في الأسواق العالمية نظم التشغيل مؤمنة من خلال القابلية للتحكم وتحقيق السلامة والتكامل والقابلية للفحص كالأتي:

أ- القابلية للتحكم: تسمح هذه الخاصية لمدير النظام بالتحكم الكامل في الصلاحيات وتساعده في القدرة على التحكم في معرفة المستفيدين الذين يحق لهم استخدام النظام ومقدرة ذلك الاستخدام[5].

ب- السلامة والتكامل: وهذا بمقدرة نظام التشغيل على حماية نفسه واستطاعته فرض استخدام القواعد والسياسات الأساسية وحماية المستفيدين من بعضهم البعض.

---

[1]- سالم بن حامد بن علي البلوى، التقنيات الحديثة في التحقيق الجنائي ودورها في ضبط الجريمة، رسالة استكمالا لمتطلبات الحصول على درجة الماجستير في العلوم الشرطية، جامعة نايف للعلوم الأمنية، كلية الدراسات العليا،الرياض،2009، ص162.

[2]- رابحي عزيزة، المرجع السابق، ص 131.

[3]- زايد محمد، المرجع السابق، ص 80.

[4]- عبد الرحمان عبد الله سند، المرجع السابق، ص 398.

[5]- سالم بن حامد بن علي البلوي، المرجع السابق، ص 158.

ج- القابلية للفحص: تتحقق هذه الخاصية مقدرة نظام التشغيل على إخراج التقارير التي تلفت نظر الإدارة إلى أي سلوك غير مادي واستخدام التقارير في تصحيح ما يلزم وتعمل وظائف نظام التشغيل على عدد من الوظائف وهي كما يلي:

- التأكيد من شخصية المستفيد بجمع دلائل تؤكد شخصيته مثل: "كلمة المرور، أو بطاقة ممغنطة أو بصمة الإصبع ".
- تدمير المستفيد: يقصد بهذا قدرة النظام على التعرف إلى المستفيدين عن طريق اسم المستفيد أو رقم خاص به.
- تسجيل الوقائع وهي نظام يسجل حالات الفشل في الدخول إلى النظام وتكرار المحاولات الخاطئة لإدخال كلمة المرور[1].
- إخراج التقارير: عن طريق تحليل وترتيب البيانات التي تسجل عن الوقائع الأمنية وإخراجها في شكل تقارير واضحة يسهل فهم وقائعها.
- الإنذار: يقصد به إصدار إنذارات مثل رسالة تعرض على وحدة الكونسول لتنبيه المسؤول إلى التدخل السريع واتخاذ الإجراء الذي يصحح الأوضاع.[2]

ظاهرة السرقة عبر الانترنت انتشرت بسرعة في الفترة الأخيرة، وعليه فالمختصين في هذا المجال قاموا بإنشاء برمجيات مضادة للفيروسات من اجل تصدي من كل قرصنة. وباستعمالها تتفادى مشاكل الاختراق وعدم دخول أي فيروسات.

ونستنتج مما سبق أن التقنيات الحديثة المستخدمة لحماية الحاسب الآلي هناك الحماية عن طريق برامج مكافحة الفيروسات،والحماية عن طريق أنظمة التشغيل.

الفرع الثاني: طرق الوقاية من الفيروسات

للوقاية من فيروسات التي تدمير الحواسيب والهواتيف، يجب بقيام ببعض من الطرق للوقاية وتجنب الاختراق وعليه لا بد من اتباع تقنيات التالية:

- عمل نسخ احتياطية من البيانات المهمة، وعدم فتح الملفات المرفقة بالبريد الالكتروني من شخص لا تعرفه، ويجب استخدام برنامج لمكتفحة الفيروسات لتحفض الاقراص بصفة دورية، وعدم نسخ ملفات من مصدر مجهول (مواقع الانترنت)، اضافة الى ذلك

[1]- سالم بن حامد بن علي البلوي، مرجع نفسه، ص 159.

[2]- سالم بن حامد بن علي البلوي، مرجع سابق، ص 160.

يجب فحص الاقراص القابلة للازلة قبل استخدامها، وتجنب زيارة المواقع الغير الامنة بشبكة الانترنت[1].

- عند اكتشاف برامج ملوثة ضمن برامج التطبيقات يجب إزالتها فورا فإذا تم الاكتشاف في الوقت المناسب فيمكن أن تحل محلها النسخة النظيفة من البرنامج المحفوظة لدى المؤسسة، أما إذا تم اكتشافها عند فوات الأوان فمن الضروري في هذه الحالة فحص مكتبة البرامج كلها بعناية وإزالة برامج دخيلة[2].
- بعد حدوث أي حالة تخريب، يجب فحص قائمة البرامج الموجودة في الأجهزة المختلفة ومقارنتها بالقائمة السابقة على عملية التخريب لاكتشاف أي برامج دخيلة وذلك بالتأكيد من أسماء البرامج وأحجامها وتاريخ أخر تعديل عليها، أما إذا كان التخريب الذي وقع في شكل تضمن كود مدسوس في بعض البرامج المشروعة فان وسيلة اكتشاف ذلك هي استخدام برامج اختبار خاصة أو بمقارنة الكود الموجود بعد التخريب مع نسخة سابقة نظيفة[3].
- وضع كلمة السر على النحو التالي: يجب أن يتم تبديل كلمات السر بصورة دورية لتجنب إمكانية الاطلاع عليها من قبل الآخرين، بحيث يمكن التبديل مرة كل ثلاثين يوما، ويفضل عدم إعادة كلمة السر القديمة قبل مرور سنة على الأقل بعد التخلي عنها، يجب أن تكون كلمات السر من خمسة أحرف على الأقل ويفضل أن تكون ثمانية أحرف وذلك يجعل مهمة صعبة بالنسبة للقرصان[4].
- فحص جميع الأقراص الغريبة أو التي استخدمت في أجهزة أخرى قبل استعمالها، وعدم تنفيذ أي برنامج مأخوذ من الشبكات العامة مثل الانترنت قبل فحصه،وفيما يخص برامج الألعاب لا يجب تشغيلها على الجهاز الذي يتضمن البيانات والبرامج الهامة،

---

[1]– إبراهيم السنوسي نصر، المرجع السابق، ص 21.

[2]– هيئة التحرير (معد)، مكافحة جرائم الحاسب الآلي الأمن والحياة، أكاديمية نايف العربية للعلوم الأمنية، مجلة16، العدد 175، السعودية، ذي الحجة 1417هـ، ص21.

[3]– هيئة التحرير، مرجع سابق، ص 21.

[4]– رابحي عزيزة، المرجع السابق، ص 132.

وعدم ترك الأقراص اللينة في السواقة عندما يكون الجهاز متوقفا عن العمل، ويجب التأكد من خلو سواقة الأقراص اللينة قبل إعادة إقلاع الجهاز[1].

- تجهيز الكمبيوتر ببرامج مضادة للفيروسات واستخدمه بشكل دوري
- تحديث برامج مضاد للفيروسات بشكل دائم لضمان كشف الفيروسات الجديدة
- الانتباه للأقراص اللينة ضد الكتابة لمنع الفيروسات من الانتقال إليها
- الاحتفاظ بنسخة ملف نظيفة من الفيروسات ومحمية ضد الكتابة لاستخدامها عند الإصابة
- إغلاق الجهاز نهائيا وإعادة تشغيله عند ظهور عبارة "Non bootable diskette".[2]

[1]– زهير هشام المرشدي، أنواع الفيروسات في الحاسب الآلي، تخصص هندسة اتصالات، جامعة سبا، اليمن، 2014، ص10.

[2]– زهير هشام المرشدي، مرجع سابق، ص 11.

خلاصة:

وفي الأخير نخلص في هذا الفصل الذي استعرضنا فيه الجوانب القانونية لجريمة السرقة الالكترونية، والتي قمنا بإشارة إليها في المطالب، وبحيث تطرقنا إلى أركان السرقة المعلوماتية وقد تطرقنا إلى مواقف التشريعات وموقف التشريع الجزائري من جريمة السرقة المعلوماتية، ومن خلال ما سبق استنتجنا بان السرقة المعلوماتية يمكن تطبيق النصوص السرقة التقليدية، واستدرج المشرع بعض القوانين لمكافحة الأشخاص الذين يقومون بالاعتداء على النظام المعلوماتي، وهناك طرق يعتمدها الجاني لمهاجمة النظام بإتباع بعض الأساليب والتي تتمثل في تدمير المواقع، والتجسس الالكتروني، وإتباع أسلوب الخداع، بحيث معظم تطبيقات السرقة تتمحور على سرقة البنوك ونسخ المعلومات والبرامج إضافة إلى ذلك سرقة هوية الائتمان، ويعتمد الجاني في استخدام برامج الفيروسات من اجل استيلاء على ما يريد، ومن اجل حماية الهاتف الذكي والكمبيوتر وتجنب السرقة يجب إتباع بعض طرق لتصدي من برامج الفيروسات خاصة.

خاتمة

خاتمة:

وفي الأخير نخلص إلى القول بان التطور التكنولوجي رغم أنها لها ايجابيات وما قدمته للعالم بأكمله إلا انه لم يمر هذا التطور على العالم بسلام. وعليه نشير إلى أن دراسة موضوع السرقة الالكترونية تكتسي أهمية كبيرة كونها ظاهرة إجرامية في المجتمع والتي انتشرت بكثرة بفعل التطور في تقنيات الحاسب الآلي والاتصال، بحيث تعتبر هذه الجريمة عابرة للحدود. وتشكل هذه الجريمة خطرا كبيرا على المجتمع خاصة إذا تعرضوا إلى السطو على أموال بنكية أو معلومات والبيانات الخاصة بالشخص في الحاسب الآلي من طرف القراصنة.

وقد تكون السرقة بريد الكتروني حيث هذه الظاهرة منتشرة والتي تتمثل في انتحال شخصية شخص المسروق وقد تؤدي إلى مشاكل كبيرة خاصة إذا كان البريد يستعمل في أعمال بين الشركات، أو قد يقوم القراصنة بسرقة البرامج قد تكون برامج الألعاب أو برامج تعليمية أو غيرها من البرامج، بحيث أحدثت مخاطر والتي تتمثل في استغلال هذه التقنية في الولوج عن بعد إلى الحواسب الآلية الخاصة بالأفراد وبالمؤسسات والتخريب فيها والنسخ الغير المشروع، وعليه فجريمة السرقة الالكترونية هي في تتطور مستمر بإتباع تقنيات والأساليب القرصنة بسبب استغلال وسائل الاتصال الحديثة، وعلى وجه الخصوص بطاقات الائتمان والسحب من الأرصدة بواسطة البطاقة الممغنطة. فنظريا ينطبق جريمة السرقة المعلوماتية على مجموعة من الأموال، والمعلومات سواء كتاب أو صور أو فيديوهات...، أو ينقل هذه البيانات بطرق غير مشروعة.

وتعد محاربة الجريمة المعلوماتية أمرا مفروضا على الدول العالم، لأنها تشكل خطورة على المجتمع والمنظومة المعلوماتية، وخاصة جريمة السرقة الالكترونية والتي ترتكب عبر الانترنت وانتشرت بسرعة فائقة وتطورت بالتطور التكنولوجي، بحيث أصبح المجرم يستخدم تقنيات وإتباع طرق جديدة للقرصنة والاستيلاء والاختلاس عكس خطوات التي يتبعها الجاني في السرقة التقليدية.

وما جعل المشرع الجزائري رغبته والتصدي للجرائم المنتشرة والوقاية ومكافحة هذه الجرائم الالكترونية ومن بينها جريمة السرقة الالكترونية، بحيث سعى التشريع الجزائري من محاولة منع حدوث الجريمة قبل وقوعها والتصدي للعوامل المؤدية لها.

وكما أن المشرع تبنى مبدأ الوقاية من الجرائم المتصلة بالتكنولوجيا الإعلام والاتصال ومكافحتها في قانون 09-04 بحيث استحدث القسم السابع مكرر بعنوان المساس بأنظمة المعالجة للمعطيات في الفصل الثالث من باب الثاني من الكتاب الثالث من مواد 394 مكرر إلى 394 مكرر 7 من قانون العقوبات.

ومن اجل تفادي جريمة السرقة على الكمبيوتر أو على الهواتف الذكية، توجد برامج مضادة للفيروسات. بحيث تجرم كل الأفعال المخالفة للقانون التي ترتكب عبر وسائل الإعلام والاتصال.والملاحظ فيما يخص السرقة الالكترونية –التي ترتكب عبر الانترنت– فالمشرع الجزائري يطبق أحكام السرقة التقليدية طبق للنص المادة 350 قانون العقوبات التي لم تحدد مصطلح الشيء إذا كان مادي أو معنوي، من المفروض التشريع الجزائري يخصص نصوص قانونية تجريم وتعاقب جريمة القرصنة، من اجل مكافحتها.

ويمكن حماية النظام المعالجة الآلية للبيانات ضد الإصابة من الفيروسات وبالتالي حماية البرامج والبيانات سواء عن طريق الحماية ببرامج مكافحة الفيروسات أو عن طريق استعمال حماية التشغيل من اجل تفادي جريمة السرقة الالكترونية والحرص على معلومات الشخصية والحاسب الشخصي.

وذلك بوضع برامج الحماية المناسبة، وتجنب فتح أي رسالة الكترونية مجهولة المصدر بل المسارعة إلى إلغائها، والحذر وعدم تصديق كل ما يصل من إعلانات والتأكيد من مصداقيتها عن طريق محركات البحث الشهيرة، من اجل الوقاية والتصدي من الاختراقات.

قائمة المراجع

أولا: الكتب

1- إبراهيم **رمضان إبراهيم عطايا**، الجريمة الالكترونية وسبل مواجهتها في الشريعة الإسلامية والأنظمة الدولية دراسة تحليلية تطبيقية، العدد الثلاثون، الجزء الثاني، طنطا، 2015.

2- أحمد **عبد الرؤوف المنيفي**، فيروسات الحاسب الآلي، اليمن، 2019.

3- **أحمد محمد عبد الرؤوف المنيفي**، السرقة الالكترونية وحكمها في الإسلام، شبكة الالوكة، اليمن. متوفر على الموقع التالي: www.alukah.net

4- أسامة **فتحي**، فيروسات الحاسوب، دون بلد النشر، دون سنة النشر.

5- **أيمن عبد الله فكري**، الجرائم المعلوماتية دراسة مقارنة في التشريعات العربية والأجنبية، معهد الإدارة العامة، الطبعة الأولى، الرياض، 2014.

6- بشرى **حسين الحمداني**، القرصنة الالكترونية أسلحة الحرب الحديثة، دار أسامة للنشر والتوزيع،الأردن،عمان، الطبعة الأولى، 2014.

7- خثير **مسعود**، الحماية الجنائية لبرامج الكمبيوتر أساليب وثغرات، دار الهدى، عين مليلة، الجزائر، طبعة 2010.

8- عبد **الرحمان عبد الله سند**، الأحكام الفقهية للتعاملات الالكترونية (الحاسب الآلي وشبكة المعلومات الانترنت)، دار الورق، الطبعة الأولى 1424،2004.

9- محمد **إسماعيل محمد**، الاختراق 1، دون طبعة النشر، دون سنة النشر.

10- محمد **حماد مرهج الهيني**، التكنولوجيا الحديثة والقانون الجنائي، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2004.

11- **محمد سعد**، عالم القرصنة، حقوق الطبع والنشر 2020.

12- نهلا **عبد القادر مومني**، الجرائم المعلوماتية، طبعة الثانية، عمان، دار الثقافة للنشر والتوزيع، 2010.

ثانيا: الرسائل والمذكرات الجامعية

أ- الرسائل الجامعية:

13- **بدري فيصل**، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة لنيل شهادة الدكتورة في القانون عام، جامعة الجزائر 1 بن خدة، 2018.

14- بواري **احمد**، الحماية القانونية لحق المؤلف والحقوق المجاورة في التشريع الجزائري والاتفاقيات الدولية، أطروحة لنيل شهادة الدكتورة في العلوم القانونية في القانون الجنائي، جامعة باتنة 1، 2015.

15- **رابحي عزيزة**، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة لنيل شهادة الدكتورة قانون خاص، جامعة أبو بكر بلقايد، تلمسان، 2018.

16- هروال **هبة نبيلة**، جرائم الانترنت دراسة مقارنة، أطروحة دكتورة، جامعة أبي بكر بلقايد، تلمسان، 2014.

ب- مذكرات الماجستير:

17- حمزة **بن عقون**، السلوك الإجرامي للمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، علم الإجرام والعقاب، جامعة الحاج لخضر، باتنة، 2012

18- **دحمان صبايحية خديجة**، جرائم السرقة والاحتيال عبر الانترنت دراسة مقارنة بين الفقه الإسلامي والقانون الجزائري، مذكرة لنيل شهادة الماجستير، شريعة والقانون، الجزائر، 2013.

19- دردور**نسيم**، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، مذكرة لنيل شهادة الماجستير في القانون الجنائي، جامعة منتوري، قسنطينة، 2013.

20- **رصاع فتيحة**، الحماية الجنائية للمعلومات على شبكة الانترنت، مذكرة لنيل شهادة الماجستير في قانون عام، جامعة أبي بكر بلقايد، تلمسان، 2012.

21- سالم **بن حامد بن علي البلوى**، التقنيات الحديثة في التحقيق الجنائي ودورها في ضبط الجريمة، رسالة استكمالا لمتطلبات الحصول على درجة الماجستير في العلوم الشرطية، جامعة نايف العلوم الأمنية، كلية الدراسات العليا، الرياض، 2009.

22- **سالم محمد سالم بني مصطفى**، جريمة السرقة المعلوماتية، رسالة استكمالا لمتطلبات الحصول على درجة الماجستير في قانون عام، جامعة جدار، 2013.

23- **سعيداني نعيم**، آليات البحث والتحري عن الجريمة المعلوماتية في قانون الجزائري، مذكرة لنيل شهادة الماجستير في العلوم الجنائية، جامعة الحاج لخضر، باتنة، 2013.

24- **سوير سفيان**، جرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، جامعة أبو بكر بلقايد، تلمسان، 2011.

25- **صغير يوسف**، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة الماجستير في القانون الدولي للأعمال، جامعة مولود معمري، تيزي وزو، 2013.
26- **عبد الرحمان جميل محمود حسين**، الحماية القانونية لبرامج الحاسب الآلي دراسة مقارنة، الأطروحة استكمالا لمتطلبات درجة الماجستير في قانون الخاص، بكلية الدراسات العليا في جامعة النجاح الوطنية في نابلس، فلسطين، 2008.
27- **عبد الله دغش**، المشكلات العملية والقانونية للجرائم الالكترونية دراسة مقارنة، رسالة استكمالا للحصول على درجة الماجستير في القانون العام، جامعة الشرق الأوسط، 2014.

ج- مذكرات الماستر:

28- بن **زرت أسيا**، إثبات الجريمة المعلوماتية في التشريع، مذكرة لنيل شهادة الماستر في قانون الجنائي، الجامعة عبد الحميد بن باديس، مستغانم، 2019.
29- **بن منصور صالح، كوش أنيسة**، السلوك الإجرام للمجرم المعلوماتي، مذكرة لنيل شهادة الماستر في العلوم الجنائية، جامعة عبد الرحمان ميرة، بجاية، 2015.
30- ريم **ساسي**، الحماية الجنائية لسرية المعلومات الالكترونية، مذكرة لنيل شهادة الماستر تخصص قانون جنائي للأعمال، جامعة العربي بن مهدي، أم البواقي، 2016.
31- **سمية مزغيش**، جرائم المساس بالأنظمة المعلوماتية، مذكرة مكملة من متطلبات نيل شهادة الماستر، قانون جنائي، جامعة محمد خضر، بسكرة، 2014.
32- **العمري ابتسام**، جريمة سرقة المعطيات المعلوماتية، مذكرة لنيل شهادة الماستر في قانون الجنائي للأعمال، جامعة العربي بن مهدي، أم البواقي، 2018.
33- **العيهاري فاطمة الزهراء، براشد منال**، جريمة سرقة المال المعلوماتي عبر الانترنت، مذكرة لنيل شهادة الماستر في قانون عام، المركز الجامعي بلحاج بوشعيب، عين تموشنت، 2017.
34- **فتيحة مهري**، جريمة الدخول والبقاء إلى أنظمة المعالجة الآلية، مذكرة لنيل شهادة الماستر في قانون جنائي أعمال، جامعة العربي بن مهدي، أم البواقي، 2016.
35- **لعاقل فريال**، الجريمة المعلوماتية في ظل التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون الجنائي، جامعة أكلي محند أولحاج، البويرة، 2015.

36- **مرابطن حياة**، الجريمة الالكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون الجنائي والعلوم الجنائية، جامعة عبد الحميد بن باديس، مستغانم، 2019.

37- **مهني محمد شريف**، استخدام القرصنة الالكترونية في السياسة الروسية (بين التجريم الدولي وحتمية التخابر)، مذكرة تخرج لاستكمال متطلبات لنيل شهادة الماستر في ميدان حقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، 2018.

38- **نايري عائشة**، الجريمة الالكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في قانون الإداري، جامعة احمد دراية، أدرار، 2017.

ثالثا: المقالات

39- **إبراهيم السنوسي نصر**، مقدمة للأنترنت، البرنامج التمهيدي للتدريب على استخدام الحاسوب والانترنت، جامعة سبها مكتب التدريب، 2015.

40- ابن **شهرة شول**، آليات مكافحة الجريمة المعلوماتية (مواقع التجارة الالكترونية نموذجا)، مجلة دراسات، العدد 13، 2016، دار المنظومة، الجزائر.

41- أحمد **حسن عبد العليم حسن الخطيب**، الجرائم المعلوماتية الواقعة عبر التواصل الاجتماعي قراءة في قانون مكافحة جرائم التقنية المعلومات المصري رقم 175 لسنة 2018، ونظام مكافحة جرائم المعلوماتية السعودي 1428هـ، مجلة دراسات الإفريقية وحوض النيل، العدد السادس أكتوبر تشرين 2019، مجلة 2، المركز الديمقراطي العربي، ألمانيا، برلين.

42- **إسراء جبريل رشاد مرعي**، الجرائم الالكتروني (الأهداف، الأسباب، طرق الجريمة ومعالجتها) مجلة الدراسات الإعلامية، المركز الديمقراطي العربي، العدد الأول يناير 2018.

43- أنسام **سمير طاهر**، جريمة السرقة الالكترونية، مجلة جامعية بابل العلوم الإنسانية، المجلد 27، العدد 5، 2019.

44- **براهيمي جمال**، مكافحة الجرائم الالكترونية في التشريع الجزائري، مجلة نقدية، كلية الحقوق والعلوم السياسية جامعة مولود معمري، تيزي وزو.

45- **روان بن عطية الله الصحفي**، الجرائم السيبرانية، المجلة الالكترونية الشاملة متعددة التخصصات، العدد الرابع والعشرون شهر 5، 2020، المملكة العربية السعودية جدة.

46- زايد **محمد**، الجريمة والقرصنة في مجال المعلوماتية والشبكات، المجلة العربية العلمية للفتيان، تونس، المجلد 10، العدد 19، دار المنظومة، 2016.

47- **زهير هشام المرشدي**، أنواع الفيروسات في الحاسب الآلي، تخصص هندسة اتصالات، جامعة سبا، اليمن، 2014.

48- سعدات **محمد فتوح محمد**، خصائص الجرائم المعلوماتية وصفات مرتكبها في ظل مجتمع المعلوماتية، المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية، كلية العلوم الحاسب والمعلومات، جامعة الإمام محمد بن سعود الإسلامية،الرياض، درا المنظومة 2016.

49- **سعيد بن سالم البادي، زايد بن حمد الجذيبي، يوسف الشيخ حمزة، محمد احمد العطاء**، الجريمة الالكترونية في المجتمع الخليجي وكيفية مواجهتها، مجمع البحوث والدراسات السلطات قابوس لعلوم الشرطة نزوى، سلطنة كمان، 2017.

50- سورية **ديش**، أنواع الجرائم الالكترونية وإجراءات مكافحتها، مجلة الدراسات الإعلامية، المركز الديمقراطي العربي، العدد الأول يناير 2018، جامعة جيلالي ليابس سيدي بلعباس، الجزائر.

51- **طرق الخن**، جرائم المعلوماتية، منشورات الجامعية الافتراضية السورية، الجمهورية العربية السورية، 2018، متوفر على الموقع الالكتروني: http://pedia.svuonline.org/

52- **عادل يوسف عبد النبي الشكر**ي، الجريمة المعلوماتية وأزمة الشرعية الجزائية، جامعة الكوفة، كلية القانون، العدد السابع، 2008.

53- **عبد الصديق شيخ**، الوقاية من الجرائم الالكترونية في ظل القانون رقم 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مجلة معالم للدراسات القانونية والسياسية، المجلد 4، العدد 1، 2020.

54- **عبد الله ماجد المطلب العكايلة**، سرقة البيانات والمعلومات الالكترونية دراسة مقارنة، كلية العلوم والدراسات الإنسانية، جامعة الأمير سطام بن عبد العزيز.

55- **عيشة خلدون**، الطبيعة الخاصة للجريمة الالكترونية وصورها، مجلة دراسات وأبحاث جامعة الجلفة، الجزائر، دار المنظومة، 2016.

56- **فاطمة الزهرة خبازي**، جرائم الدفع الالكتروني وسبل مكافحتها، أعمال الملتقى الوطني: آليات مكافحة الجرائم الالكترونية في التشريع الجزائري، الجزائر 29 مارس 2017، جامعة الجيلالي بونعامة، خميس مليانة.

57- **محمد طيب عمور**، السرقة الالكترونية: تكيفها الشرعي وطرق إثباتها، مجلة الإحياء، المجلد:19، العدد 22، كلية العلوم السياسية، جامعة حسيبة بن بوعلي، شلف.

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

59- **نميديلي رحيمة**، خصوصية الجريمة الالكترونية في القانون الجزائري والقوانين المقارنة، أعمال المؤتمر الدولي الرابع عشر: الجرائم الالكترونية، طرابلس 24-25 مارس 2017، جامعة محمد لمين دباغين، سطيف 2، الجزائر.

60- **هيئة التحرير (معد)**، مكافحة جرائم الحاسب الآلي الأمن والحياة، أكاديمية نايف العربية للعلوم الأمنية، مجلة 16: العدد 175، السعودية، ذي الحجة 1417هـ.

رابعا: النصوص القانونية

61- الأمر رقم 03-05 مؤرخ في 19 جمادي الأولى عام 1412 الموافق 19 يوليو سنة 2003، يتعلق بحقوق المؤلف والحقوق المجاورة.

62- الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966، الذي يتضمن قانون العقوبات، المعدل والمتمم.

63- أمر رقم 97-10 مؤرخ في 27 شوال عام 1417 الموافق 6 مارس سنة 1997، يتعلق بحقوق المؤلف والحقوق المجاورة.

64- قانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المتمم والمعدل للأمر 156/66 المتضمن قانون العقوبات.

65- قانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

66- مرسوم تشريعي رقم 93-17 مؤرخ في 23 جمادي الثانية عام 1414 الموافق 7 ديسمبر سنة 1993 يتعلق بحماية الاختراعات.

خامسا: المواقع الالكترونية

67- http://www.jsecurilylab.com/2020/10/blog-post-94.html
68- https://shella4ever.yoo7.com/t81-topic
69- https://www.alukah.net/culture/0/52639/
70- https://www.mlzamty.com/virus-damage/

الفهرس

الفهرس

الصفحة