وزارة التعليم العالي والبحث العلمي
Ministry of High Education and Scientific Research
جامعة محمد البشير الإبراهيمي – برج بوعريريج –
University of Mohamed el Bachir el Ibrahimi–Bba
كلية الحقوق والعلوم السياسية
Faculty of Law and Political Sciences

مذكرة مقدمة لاستكمال متطلبات نيل شهادة الماستر

تخصص: قانون إعلام آلي وإنترنت

الموسومة بـ

جريمة الدخول إلى النظام المعلوماتي في القانون الجزائري

– إعداد الطالبين:
– داود إدريس
– شيبان أنيس

تحت إشراف:
د. كمال فرشة

أعضاء لجنة المناقشة:

اسم ولقب العضو	رتبته	مؤسسته	صفته
خوضري محمد	محاضر – أ–	جامعة محمد البشير الإبراهيمي	رئيسا
كمال فرشة	محاضر – أ–	جامعة محمد البشير الإبراهيمي	مشرفا
بوجادي صليحة	محاضر – أ–	جامعة محمد البشير الإبراهيمي	مناقشا

السنة الجامعية: 2023/2022

بسم الله الرحمن الرحيم
١٤٣٨

الإهداء

الحمد لله والصلاة والسلام على محمد الهادي لأنوارك الجامع

لأسرارك الدال عليك الموصل اليك فالشكر كل الشكر لله الذي انعم

علي بنعم الحياة والسعادة اشكره على كل نعمة ورزق يسر لي

وعلى كل مصيبة كانت لها حكمة وعبرة.

الى الذي قال يوما لاتكن مثلي لأفخر بك فتعمدت ان اكون مثله

لأفخر بي، ابي الغالي رحمة الله عليه والى نبع الحنان الى الدعم

والحب الذي لا ينظب امي الغالية.

رزقك الله الستر ورزقك طول العمر وأمدك الصحة والعافية.

والى إخوتي وأخواتي وجميع أفراد الأسرة الكريمة

كلماتي لن تكف للتعبير عن عمق امتناني لكما بورك فيكما

وجزيتم من الرحمان خير الجزاء

الى كل من ساهم في هذا العمل المتواضع ولو بالكلمة الطيبة

اصدقائي، ورفقاء دربي.

إدريس

الإهداء

إلى التي تحمل أخف كلمة نطق بها اللسان، ووضعت تحت قدميها الجنات.

كانت الملاذ والمأوى سر السعادة والنجوى، نبع الحنان،

ومبعث الأمان... لكي أمـــــــــي.

إلى من خطى درب الصعاب من أجلنا، صاحب القلب الكبير، تاج رأسي

إلى رمز العطاء،

الذي علمني أن الحياة كفاح ونضال، فبعث في روحي الحياة،

وقوة الدفاع... لك أبـــــــــي.

أسأل الله سبحانه وتعالى أن يطيل في عمرهما على الطاعة، وأن يمنحهما الصحة والعافية،

وأن يجعل عاقبتهما جنة عرضها السموات والأرض.

إلى القلب الذي أحاطني بالجد والرعاية، ورافقني في دروب الحياة

أخي "أمين"،

إلى كل الأهل والأقارب.

إلى كل من التقيت بهم، وسرت معهم على درب العلم والتعلم، إلى الأصدقاء،

رمز الوفاء والعطاء، وكل طلبة الماستر في كلية الحقوق: 2022-2023.

أنيس

شكر وعرفان

نتقدم بجزيل الشكر والحمد لله الذي أمدنا بالقوة والصبر من أجل إنجاز هذا العمل المتواضع.

نسجل كذلك شكرنا للأستاذ الفاضل: الدكتور كمال فرشة الذي تكرم بقبول الإشراف على هذه المذكرة ولم يبخل علينا بنصائحه السديدة فأنار طريقنا بالإرشادات والتوجيهات القيمة.

كما لا يفوتنا في هذا المقام أن نتقدم بخالص الشكر والتقدير إلى أساتذتنا الأجلاء ونخص بالذكر أعضاء اللجنة الموقرة وكل من كان عونا لنا ونبراسا في طريق البحث والتعلم.

مقدمة

في ظل التطورات الهائلة في القرن العشرين في مجال الاتصالات وبفضل الوسائل التكنولوجية المعلوماتية الحديثة الممثلة في الحاسب الآلي والشبكة المعلوماتية الدولية (الانترنت) اعجوبة القرن التي امتدت حول أنحاء العالم وربطت بين شعوبه، حيث اطلق على القرن العشرين تعريف الثورة المعلوماتية le sicle de la revolution informatique، واحدثت هذه الثورة تأثيرا جذريا في جميع جوانب الحياة، مما ادى الى تغييرا جوهري في مدى تعاملنا مع المعلومات والتواصل والعمل والتعليم وغيرها، فقد اصبحت قوة لا يستهان بها في ايادي الدولة والافراد.

تتميز الثورة المعلوماتية بالتحول الكبير في استخدام التكنولوجيا في تبادل وتخزين ومعالجة المعلومات، وقد ادى هذا الى تطور انظمة حاسوبية وظهور الحواسيب الشخصية والاجهزة الالكترونية والشبكات العنكبوتية، وبالتالي بات لازما على كل مجتمع ان يتعايش ويتواصل مع المجتمعات الاخرى، حيث ان هذا التطور يعدو الى التأمل والتوقف إزاء هذه الظاهرة تكنولوجية، اكثر مما يدعو الى الدهشة لان تكنولوجيا المعلومات اصبحت الرئبة التي يتنفس بها ابناء هذا المجتمع.

تركت الثورة المعلوماتية اثارا ايجابية وشكلت قفزة نوعية حضارية في حياة الافراد والدول، حيث اصبحت رئة القطاعات المختلفة تعتمد على استخدام الانظمة المعلوماتية لتميزها لعنصر السرعة والدقة في تجميع المعلومات ونقلها ومعالجتها، وتبادلها بين الافراد، والشركات والمؤسسات داخل الدول الواحدة او عبر الدول الاخرى، إضافة الى انها اصبحت مستودعا كبيرا وضخم للبيانات والمعطيات الشخصية والاقتصادية والمالية وكذلك لأسرار الدول العسكرية والصناعية والاقتصادية، التي تعبر عن قدر كبير من السرية والاهمية.

ان كل هاته الايجابيات التي ظهرت مع الثورة المعلوماتية وما حملته من ايجابيات للأفراد والدول الا انه لا ينفي الانعكاسات السلبية التي احدثتها هذه التقنيات العالية، المتمثلة في استغلال الانظمة المعلوماتية واستعمالها على نحو غير مشروع، بصورة تمس

سرية معلومات الأفراد والجماعات وتضر بمصلحتهم الشخصية، لما تحمله البيانات في معلومات مهمة وسرية وبالتالي تضمن مصلحة المجتمع كله.

حيث ان التطور الهائل احدث في الفقه القانوني انماط مستحدثة للجرائم إصطلح على تسميتها **بالجرائم المعلوماتية** أو جرائم تقنية المعلومات.

فهذه الجريمة تختلف عن الجرائم التقليدية، حيث ان هذه الجرائم ترتبط بما مدى اعتماد المجتمع بمؤسساته المختلفة الخاصة والعامة على الانظمة المعلوماتية في انجاز اعمالهم، فكلما زاد الاعتماد عليها زادت الفرصة في ارتكاب الجرائم المعلوماتية.

من هذا فان الجرائم المستحدثة الماسة بالمعلوماتية لا يمكن ارتكابها الا عن طريق جريمة الدخول الغير مشروع الى النظام المعلوماتي، حيث يعتبر هذا القفل ضروري لارتكاب كل جريمة تدخل في اعداد هذه الجرائم ومن اخطر الجرائم التي تقع على نظام المعالجة الالية المعطيات. وهذا ما خلق تحديات كبيرة في مواجهة النظام القائم ما دعا المشرع في دول عديدة الى الحاجة في ادخال تشريعات جديدة، تحمي هاته المعلومات داخل النظام من فعل الدخول الغير مشروع الى المنظومة المعلوماتية نظرا لقصور قواعد التقليدية في قانون العقوبات عن حماية هذا النظام.

أقر المشرع الجزائري هذه الحماية في قانون العقوبات في الفصل الثالث القسم السابع مكرر منه، المتضمن المساس بنظم المعالجة الالية للمعطيات، والذي تضمن 8 مواد في المادة 394 مكرر الى المادة 394 مكرر 7 وكذلك من القانون 04/09 لسنة 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها[1] وكذلك من خلال قانون الاجراءات الجزائية الجزائري[2]، وذلك لمتابعة ومعاقبة مجرمي المعلومات ومرتكبي جريمة الدخول غير مشروع الى النظام المعلوماتي إذ خصهم بإجراءات خاصة وطبيعة الجريمة.

[1] الجريدة الرسمية للجمهورية الجزائرية الشعبية الديمقراطية، عدد 47، 25 شعبان 1430هـ، 16 أوت 2009.

[2] القانون 22/06، المؤرخ 20 ديسمبر 2006.

إشكالية موضوع البحث:

على ضوء ما سبق رصده من تصور للموضوع، وبغية التعمق أكثر في تفاصيله قمنا بطرح الإشكالية التالية:

كيف تصدى المشرع الجزائري لجريمة الدخول الى النظام المعلوماتي؟

ولدراسة هذه الإشكالية يتطلب منا الإجابة على التساؤلات التالية:

- ما مفهوم جريمة الدخول غير المشروع الى النظام المعلوماتي؟
- ما هي اركانها؟
- ما هو إطار قانوني والجزاءات المترتبة عليها؟

أهمية موضوع البحث:

تكمن أهمية موضوع الدراسة في انه من المواضيع الحديثة اليوم على المستوى الدولي والوطني، وبارتباط الجريمة المعلوماتية بحياة الافراد والمؤسسات، خاصتا جريمة الدخول الي النظام المعلوماتي، لصعوبة تطبيق النصوص التقليدية على هذه الجرائم، وهو ما دفع إلى التدخل التشريعي من قبل الدول لمواجهة جريمة الدخول بما فيها المشرع الجزائري، لذا فإن إدراك ماهية الجريمة المعلوماتية وجريمة الدخول الي النظام المعلوماتي، واستظهار خصائصها يتخذ أهمية كبيرة واستثنائية لسالمة التعامل مع هذه الجرائم.

أهداف الدراسة:

تسعي هذه الدراسة إلى المساهمة في الجهد الأكاديمي الذي يحاول التعرف علي خصوصية جريمة الدخول الي النظام المعلوماتي موضوعيا واجرائيا، ذلك أن حداثة هذه الجرائم وما تتسم به من خصائص احدثت لدي المشرع حيرة أمامها وكيفية التعامل معها، إذ ال شك أن تكييفها والإلمام بها يختلف عما هو الحال عليه في الجرائم التقليدية.

- **أسباب اختيار موضوع البحث:**

اسباب ذاتية:

ان من الاسباب الذاتية التي دفعتنا لاختيار هذا الموضوع هو رغبتنا في الاطلاع علي هاته الجريمة المعلوماتية، وإضافتا الي تسليط الضوء علي المواد والاحكام التشريعية التي جرمتها في القانون الجزائري.

الاسباب الموضوعية:

تعتبر جريمة الدخول الي النظام المعلوماتي من الجرائم المستحدثة، إن الوقوف على حقيقة التعامل مع هاته الجريمة من الناحيتين الموضوعية والإجرائية وخصوصيتها في كلا الناحيتين، هو السبب الرئيسي لاختيارنا للموضوع حيث أن الكثير من الدراسات التي عنيت بهذه الجرائم باتت تركز على الجانب الموضوعي فقط دون الإجرائي لذا حاولنا في دراستنا إثراء النقاش القانوني حول هذا الموضوع الهام.

- **المنهج المعتمد في البحث:**

اعتمدنا في دراستنا على المنهج التحليلي بالإضافة الى مناهج اخرى كالمنهج الوصفي والمنهج الاستقرائي، فالمنهج التحليلي يظهر من خلال تحليل بعض المفاهيم حول هذه الجريمة وكذلك من خلال خصوصيتها واخيرا المنهج الاستقرائي من جراء بيان نظام القانوني لهذه الجريمة.

وتماشيا مع هذه المناهج، اعتمدنا أسلوب البحث القانوني الأكاديمي الذي يعتمد المراجع المختلفة، كالكتب والنصوص القانونية والبحوث المقدمة إلى المؤتمرات والندوات، فضلا عن لجؤنا إلى شبكة الأنترنيت.

- **تقسيم البحث:**

تمت تقسيم الخطة تقسيما ثنائيا، وذلك من خلال فصلين:

الفصل الاول تناولنا فيه خصوصية الجريمة المعلوماتية من الناحية الموضوعية الذي بدوره قسمناه الى مبحثين ماهية الجريمة المعلوماتية في المبحث الاول، اما في المبحث الثاني فقد تناولنا فيه انواع الجرائم المعلوماتية.

الفصل الثاني تطرقنا فيه الى النظام القانوني لجريمة الدخول غير المشروع الذي قسمناه الى مبحثين، المبحث الاول تناولنا فيه اركان جريمة الدخول اما المبحث الثاني فتناولنا فيه العقوبات المقررة للجريمة.

الفصل الأول:

الإطار الموضوعي لجريمة الدخول إلى النظام المعلوماتي

ان الظاهرة الاجرامية الحديثة التي تتمثل في القفزة النوعية في المجال المعلوماتي وما صاحبه من ظهور الانترنت والتطور في وسائل الإتصال ونقل المعلومات اظهرت نوع جديد من الجرائم التي سميت بالجرائم المعلوماتية.

حيث اظهرت هذه الجرائم الوجه الثاني للثورة المعلوماتية لأنها من حقوق الاشخاص وسرية المعلومات المخزنة داخل المنظومة المعلوماتية حيث اصبح موضوع الجريمة المعلوماتية موضوع الساعة ومشكل كل الدول وكذلك الدولة الجزائرية لأنها من الجرائم المستخدمة في هذا العصر.

لدراسة هذه الجريمة لا بد من التطرق الى الجانب المفاهيمي او الموضوعي لها الذي قسمناه الى عناصر حيث تناولنا في المبحث الاول ماهية الجريمة المعلوماتية وفي المبحث الثاني انواع المعلوماتية الذي بدوره قسمناه الى مطلبين، المطلب الاول الجرائم الواقفة على النظام المعلوماتي وفي الطلب الثاني الجرائم التي تتم عن طريق النظام المعلوماتي.

المبحث الاول: مفهوم الجريمة المعلوماتية

تعددت الآراء بشأن تعريف الجريمة المعلوماتية وتعذر ايجاد مفهوم مشترك للجريمة المعلوماتية وهذا ما سنتطرق اليه في مبحثنا الاول. والتنقل فيما بعد الى تصنيفها.

المطلب الاول: تعريف الجريمة المعلوماتية

اختلاف النظم القانونية والثقافية بين الدول، نتج عنه تعريف للجريمة المعلوماتية، في المجال الضيق وتارة اخرى في المجال الموسع.

لذا نتطرق في هذا المطلب الى التعريف الضيق لهذه الجريمة والتعريف الموسع لها.

الفرع الاول: التعريف الضيق للجريمة المعلوماتية

لا يوجد مصطلح موحد للدلالة على ظاهرة الاجرامية الناشئة في البيئة الرقمية فيما يعد في بيئة الشبكات، بل تباينت هذه المصطلحات حيث رافق هذا التباين مسيرة نشأتها وتطور ظاهرة الاجرام المرتبط بتقنية المعلومات.

فظهرت عدة محاولات لتعريفها تعريفا ضيقا من بينتها:

- **Tiedement بانها:** "كل اشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب".[1]
- ويعرفها الفقيه MERWE الفعل الغير مشروع الذي يتورط في ارتكابه الحاسب الالي وهي الفعل الاجرامي الذي يستخدم في اقترافه الحاسب الالي كأداة رئيسية".[2]
- فيما عرفها الفقيه Rosblat "بانها كل نشاط غير مشروع موجه لنسخ او تغيير او حذف او الوصول الى المعلومات المخزنة داخل الحاسب الالي والتي تحول طريقه.

[1] خالد ممدوح ابراهيم :من الجريمة الالكترونية, الدار الجامعية مصر, 2008 ص42.

[2] Marwe Vander , computer crime and other grimes against information technologies in south Africa, « R.I.D.P ».1993.P.554

- كما عرفها مكتب تقييم التقنية بالولايات المتحدة الأمريكية انها الجرائم التي تلعب دورا رئيسيا.

ما جاء في التعريفات السابقة انها كانت قاصرة على الاحاطة بأوجه ظاهرة الاجرام المعلوماتي، فالبعض من الفقهاء هذا الاتجاه ركز على معيار موضوع الجريمة والبعض الاخر ركز على وسيلة ارتكابها والبعض الاخر ركز على معيار النتيجة.

الفرع الثاني: التعريف الموسع للجريمة المعلوماتية

حاول بعض الفقهاء تعريف الجريمة المعلوماتية على نحو واسع لتفادي اوجه القصور التي شابت تعريفات الاتجاه الاول "الاتجاه الضيق" في التصدي لظاهرة الاجرام المعلوماتي.

فعكس الإتجاه السابق انصار هذا الإتجاه يذهبون الى التوسع من مفهوم الجريمة المعلوماتية، باعتبار ان مجرد مشاركة حاسب آلي في الإجرامي يصبغ وصف الجريمة المعلوماتية.

حيث ذهب الفقيهان (Michel & escredo) على ان سوء استخدام الحاسب او جريمة الحاسب تشمل: استخدام حاسب كأداة لارتكاب الجريمة، هذا بالإضافة الى الحالات المتعلقة بالولوج الغير المصرح به لحاسب المجني عليه او بياناته، كما تشمل كذلك الاعتداءات المادية على جهاز الحاسب الالي ذاته او المعدات المتصلة به، كذلك استخدام غير مشروع لبطاقات الإئتمان، وعرفت في اطار المنظمات الأوروبية للتعاون والتنمية الاقتصادية بانها: "كل فعل او امتناع من شأنه ان يؤدي الى الاعتداء على الاموال المادية او المعنوية، يكون ناتجا عن طريقة مباشرة عن تدخل التقنية المعلوماتية الالكترونية. [1]

[1] حنان ريحان المبارك المضاحكي، الجرائم المعلوماتية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2014، ص 26-27

يمتاز هذا التعريف يحتوي على كل صور الإعتداء الإيجابية والسلبية، التي توقع الضرر على مكونات الحاسب المادي والمعنوية وشبكات الإتصال الخاصة به.

لا شك ان هذا الاتجاه يحتوي على توسع كبير لمفهوم الجريمة المعلوماتية، اذ يؤخذ عليه هذا التوسع الذي من شأنه ان يبسط من وصف الجريمة المعلوماتية على افعال قد لا نكون كذلك بمجرد مشاركة الحاسب الآلي في النشاط الإجرامي، ولا يمكن القبول بهذا التوجه فقد لا يبدو ان يكون الحاسب الالي محلا تقليديا في بعض الجرائم كسرقة الحاسب ذاته او الاقراص او الاسطوانات الممغنطة مثلا، فلا يمكن اعطاء وصف الجريمة المعلوماتية على سلوك الفاعل لمجرد ان الحاسب او احدى مكوناته المادية كانت محلا لفعل الاختلاس.[1]

الفرع الثالث: التعريف التشريعي للجريمة المعلوماتية

المشرع الجزائري عرف الجريمة المعلوماتية في نص المادة 2 الفقرة –أ– من القانون 09–04 المؤرخ في05 اوت2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها بالقول بأن "الجرائم المتصلة بالتكنولوجيات الاعلام والاتصال هي: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات او اي جريمة اخرى ترتكب او يسهل ارتكابها عن طريق منظومة معلوماتية او نظام الإتصالات الإلكترونية.[2]

تكون الجريمة المعلوماتية ايضا تلك الجرائم المرتكبة عن طريق اي نظام منفصل او مجموعة من الأنظمة المتصلة ببعضها البعض او المرتبطة، يقوم واحد منها او اكثر بمعالجة الية للمعطيات تنفيذا لبرنامج معين[3] او اي تراسل او ارسال او استقبال علامات

[1] نائلة محمد فريد قورة، جرائم الحاسب الآلي الإقتصادية، منشورات الحلبي الطبعة الأولى، القاهرة، 2005، ص 31.

[2] المادة 02 الفقرة –أ– من قانون 09–04.

[3] المادة 02 الفقرة –ب– من نفس القانون.

او اشارات او كتابات او صور او اصوات اي معلومات مختلفة بواسطة اي وسيلة الكترونية.[1]

الملاحظ ان المشرع الجزائري اعتمد على الجمع بين عدة معايير لتعريف الجريمة المعلوماتية. اولها معيار وسيلة الجريمة وهو النظام الاتصالات الالكتروني، وثانيها معيار موضوعي المتمثل في المساس بأنظمة المعالجة الالية للمعطيات، والمعيار الثالث هو معيار القانون الواجب التطبيق اي الركن الشرعي للجريمة المنصوص عليه في قانون العقوبات، اما المعيار الرابع الذي اعتمده المشرع الجزائري. وهذا ما يوسع نطاق الجرائم المعلوماتية في القانون الجزائري كونه اقر ان هذه الجريمة ترتكب في نظام معلوماتي او يسهل ارتكابها عليه.

المطلب الثاني: تصنيف الجرائم المعلوماتية

ارتباط الجريمة المعلوماتية بتقنية المعلومات والحاسب الآلي وما يتمتع به من تقنية عالية. ميزها عن غيرها من الجرائم التقليدية حيث اضفى لها ميزة خاصة، فقد اضافت هذه الحقيقة على هذا النوع من الجرائم عدد من السمات والحقائق، والتي انعكست بدورها على مرتكب هذه الجريمة، الذي اصبح يعرف بالمجرم المعلوماتي. لتميزه ايضا عن المجرم التقليدي، وقد كان لتطور شبكة المعلومات اثر في اعطاءها شكل جديد للجريمة المعلوماتية، ولعلى ما أضفته الأنترنت على الجريمة المعلوماتية هو الطبيعة الدولية العابرة للقارات والحدود.

سوف نحاول فيما يلي التطرق إلى بعض خصائص الجريمة المعلوماتية و سمات المجرم المعلوماتي وتصنيف المجرم المعلوماتي.

[1] المادة 02 الفقرة –و– من نفس القانون.

الفرع الأول: خصوصية الجريمة المعلوماتية

سنتطرق في هذا الفصل لدراسة خصوصية الجريمة المعلوماتية في العناصر التالية:

أولا: صعوبة اكتشاف الجريمة المعلوماتية

الجريمة المعلوماتية تتسم بصعوبة اكتشافها و اثباتها لأنها لا تترك أثرا مرأيا أو كتابيا لما يجري خلال تنفيذ الجريمة، كما يمكن للجاني حذف المعلومات والمعطيات التي يمكن أن يستخدم كدليل ضده[1]. مثلا عند ارسال الفيروسات، سرقة الأموال، البينات الخاصة، المكالمات واتلافها والتجسس وغيرها من الجرائم، بالتالي فهي صعبة الاكتشاف والاثبات لإدانة مرتكبها وهذا ما يشكل تحديا للمشرع.

ثانيا: صعوبة اثبات الجريمة المعلوماتية

ان اثبات الجريمة المعلوماتية يصعب تتبعها واكتشافها فهي لا تترك أثرا يقتفي، لأنها تتم في بيئة رقمية حيث يصعب على الجهات الأمنية والقضائية اثباتها نظرا لنقص المعارف التقنية وهو ما يتطلب تخصص في التقنية لتحصين الجهاز الأمني والقضائي ضد هذه الظاهرة، حيث تتم هذه الجريمة المعلوماتية دون رؤية دليل الإدانة، وحتى في وجود دليل يمكن للجاني طمس الدليل أو محوه في حضور أجهزة العدالة غير المتخصصة، وذلك غالبية الجرائم المعلوماتية تكتشف عن طريق المصادفة وليس عن طريق الابلاغ عنها، لأنها في الغالب لا تخلف أي آثار مادية كتلك التي تخلفها الجرائم التقليدية[2].

ثالثا: أسلوب ارتكاب الجريمة المعلوماتية

ذاتية الجرائم المعلوماتية تبرز بصورة أكثر وضوحا في أسلوب ارتكابها وطريقتها، فإذا كانت الجرائم التقليدية تتطلب من الجهد الذي قد يكون في صورة ممارسة العنف

[1] هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، الطبعة الأولى ، 1994 ص 27

[2] مصور فهيد سعيد الحارثي، معوقات إثبات الجرائم المتعلقة لتقنية المعلومات، المجلة القانونية، القاهرة، المجلد 15، العدد 04، فبراير 2023، ص 08.

والايذاء كما هو الحال في جريمة القتل أو الاختطاف، فإن الجرائم المعلوماتية هي جرائم هادئة بطبيعتها (soft crime) لا نحتاج إلى العنف بل كل ما نحتاج إليه هو القدرة على التعامل مع جهاز الحاسوب بمستوى تقني يوظف في ارتكاب الأفعال الغير مشروعة.

وتحتاج كذلك إلى وجود شبكة المعلومات الدولية (الأنترنت) مع وجود مجرم يوظف خبرته أو قدرته على التعامل مع شبكة للقيام بجرائم مختلفة كالتجسس أو اختراق خصوصيات الغير أو الغرير بالقاصرين، كل ذلك دون الحاجة لسفك الدماء[1].

رابعا: الصفة العالمية للجرائم المعلوماتية

تصف الجريمة المعلوماتية بكونها جريمة ذات بعد عالمي دولي، لكن لا ينبغي أن يفهم من ذلك أنها جريمة دولية، ذلك أن هذه الأخيرة محددة على سبيل الحصر والمعرفة وفق نظام روما الأساسي في جرائم الحرب، جرائم العدوان، ما يجعل بالضرورة التفرقة بين النوعين، فالجريمة المعلوماتية تصنف في مجال القانون الجنائي الدولي، بخلاف الجريمة الدولية التي تصنف في مجال القانون الدولي الجنائي[2].

فالجريمة المعلوماتية بهذا الشكل لا تعرف بالحدود بين الدول وهي بذلك شكل جديد من أشكال الجرائم العابرة للحدود الإقليمية بين دول العالم كافة، فلقد أثارت هذه الخاصية الدولية للجريمة المعلوماتية عدة اشكالات قانونية تتعلق أساسا بتحديد الدولة صاحبة الاختصاص القضائي في محاكمة مرتكب هذه الجريمة، بالإضافة إلى اشكالية مدى تفاعل القوانين القائمة في التعامل مع الجريمة المعلوماتية، وبصفة خاصة مسألة جمع الأدلة وقبولها اذ يتباين مواقف الدول فيها يتعلق بقبول الأدلة المستخلصة من أنظمة الحاسب الآلية، من أجل ذلك فقد تعالت الأصوات الداعية إلى التعاون الدولي المكثف

[1] نهلة عبد القادر المومني، الجرائم المعلوماتية، الطبعة الثانية، دار الثقافة، عمان، 2010، ص 57 ص 58.

[2] يعيش تمام شوقي، الجريمة المعلوماتية، دراسة تأصيلية مقارنة، مخبر أثر الإجتهاد القضائي حركة التشريع، جامعة محمد خيضر، بسكرة، ص 29.

من أجل التصدي لها بجزم وأن يشمل هذا التعاون تبادل المعلومات وتسليم الأدلة وضمان أن الأدلة يتم جمعها في دولة تقبل في محاكم أخرى[1].

خامسا: الجريمة المعلوماتية تتم عادة بالتعاون أكثر من شخص

تتميز الجريمة المعلوماتية انها تتم عادة بتعاون أكثر من شخص واحد على ارتكاب اضرار بالجهة المعني بها، وغالبا ما يشترك في إخراج الجريمة إلى حيز الوجود شخص متخصص في تقنية الحاسب الآلي والإنترنت يقوم من الجانب الفني من الشروع الإجرامي، وشخص آخر من المحيط أو من خارج المؤسسة المجني عليها لتغطية عملية التلاعب وتحويل المكاسب إليه. [2]

الفرع الثاني: سمات المجرم المعلوماتي

يتميز المجرم المعلوماتي عن غيره من المجرمين الأخرين بسمات خاصة به ما جعلت منه محل العديد من الأبحاث والدراسات، حيث اختلف الباحثين في تحديد هذه السمات والخصائص التي تميز المجرمين المعلوماتيين عن غيرهم من مرتكبي الجرائم الأخرى والتي يتم ذكر اهمها كما يلي:

أولا: الذكاء

يعتبر مرتكب الجريمة الإلكترونية في الغالب شخص يتميز بالذكاء والدهاء ذو مهارات تقنية عالية وعلى دراية بالأسلوب المستخدم في مجال أنظمة الحواسب وكيفية تشغيله وكيفية تخزين المعلومات والحصول عليها، كما له قدرة فائقة في المهارة التقنية اين يستغل مداركه ومهارته في اختراق الشبكات وكسر كلمات المرور والشفرات[3].

---

[1] سعيداني نعيم، آلية البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة بحث لنيل شهادة ماجيستير، جامعة الحاج لخضر، باتنة، ص 32 ص 33.

[2] نهلة عبد القادر المومني، مرجع سابق، ص 58.

[3] غريبي بشرى، خصوصية المجرم المعلوماتي ودوافعه، مجلة نموديا الأكاديمية، المجلد 02، العدد 02، 2021، ص 104.

فالمجرم المعلوماتي يمكن أن يكون له تصورا كاملا لجريمته قبل أن يرتكبها، بل يقوم بتجربها على أنظمة معلوماتية مماثلة لتلك المستهدفة وذلك ليتجنب عنصر المفاجئة خصوصا في الجرائم المعلوماتية المالية التي تحقق له الربح المالي، وتلحق الخسارة بالمجني عليه، فتجده لا يستعمل العنف أو الإتلاف المادي.

فالمجرم المعلوماتي يسعى دوما إلى معرفة كل ما هو جديد ومبتكر ولا يعرفه أحد سواه وذلك بهدف إختراق الحواجز الأمنية في البيئة المعلوماتية.[1]

ثانيا: اختيار الوسيلة بعناية

الوسيلة يراد بها الإمكانيات التي يتزود بها الفاعل لإتمام جريمته ،وفيما يتعلق بالمجرم المعلوماتي فإن الوسائل المتطلبة للتلاعب بأنظمة الحاسب الآلي هي في أغلب الحالات تتميز بالبساطة والسهولة في الحصول عليها ، فالمجرم المعلوماتي يتميز بقدرته على الحصول على ما يحتاج إليه أو ابتكار أساليب التي تقلل من الوسائل اللازمة لإتمام النشاط الإجرامي[2].

ثالثا: المجرم المعلوماتي يبرر ارتكاب جريمته

يوجد شعور لدى مرتكب فعل الإجرام المعلوماتي أن ما يقوم به لا يدخل في عداد الجرائم أو بمعنى آخر لا يمكن لهذا الفعل أن يتصف بعدم الأخلاقية وخاصة في الحالات التي يقف فيها السلوك عند حق قص نظام الحاسوب وتخطي الحماية المفروضة حوله، حيث بغرق مرتكبو هذه الجرائم بين الأضرار بالأشخاص الامر الذي يعدونه غاية

[1] ربيعي حسين، المجرم المعلوماتي – شخصيته وأصنافه، مجلة العلوم الإنسانية، جامعة خيضر، بسكرة، العدد 40، جوان 2015، ص 289.

[2] عامر محمد الحبيب عبد القادر، المجرم المعلوماتي، مذكرة لنيل شهادة ماستر تخصص قانون جنائي، جامعة عبد الحميد ابن بديس، 2019، ص 57.

في اللاأخلاقية وبين الإضرار بمؤسسة او جهة في استطاعتها اقتصاديا تحمل نتائج تلاعبهم[1].

فهؤلاء الأشخاص لا يدركون أن سلوكهم يتحقق العقاب ويبدو أن الاستخدام المتزايد للأنظمة المعلوماتية ضد إنشاء مناخا نفسيا موائما لتصور استبعاد فكرة الخير والشر وقد ساعد على ذلك عدم وجود احتكاك مباشر بالأشخاص، ومما لا شك فيه أن هذا التباعد في العلاقة الثنائية بين الفاعل والمجني عليه يحصل المرور إلى الفعل غير المشروع ويساعد على إيجاد نوع من الاضرار الشرعي الذاتي بمشروعية هذا الفعل.

رابعا: السلطة

يقصد بالسلطة جملة من الحقوق والمزايا التي يتمتع بها المجرم المعلوماتي والتي تسمح له وتمكنه في ارتكاب جريمته، فكثير من المجرمين في هذا المجال لديهم سلطة مباشرة أو غير مباشرة في مواجهة محل الجريمة كشفرة الدخول إلى النظام المعلوماتي، وشفرة الدخول إلى الملفات وخزائنها وتعديل مضمونها أو محوه وقد تختصر هذه السلطة في مجرد الحق الدخول إلى أماكن التي تحتوي على هذه أنظمة[2].

خامسا: التكيف الاجتماعي

هذه الخاصية تعتبر امتدادا لسمة التخطيط والتنظيم، حيث ينشأ التكيف الاجتماعي بين مجموعة من لها صفات مشتركة فمثلا جماعة صغار نوابغ المعلوماتية لا شك أنهم يتكيفون في أفكارهم فيما بينهم، وتنشأ بالتالي بينهم صلات وروابط تساعدهم على ارتكاب جرائمهم وتتعدى تلك الروابط والصلات النطاق المحلي بحيث تنشأ بينهم روابط دولية تتفق مع أفكارهم ومنهجهم [3] بالإضافة إلى ذلك أن مجرمي الإنترنت هم عادة أناس اجتماعيين قادرين على التكيف في بيئتهم الاجتماعية، حيث تمنح هذه

[1] نهلة عبد القادر المومني، مرجع سابق، ص78.

[2] نهلة عبد القادر المومني، مرجع سابق، ص 80.

[3] أيمن عبد الحفيظ ، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، دون دار نشر، سنة 2004، ص 18.

الخاصية القدرة على تحويل جريمتهم من دولة إلى أخرى تكون قوانينها أكثر مرونة، وهي خاصية تجعلها قادرة على الإفلات من إجراءات مكافحة غير فعالة بسبب الحدود الإقليمية، وبالتالي تبين هذه الخاصية تبين مدى خطورة قوة الجماعات الإجرامية المنظمة عبر الإنترنت.

سادسا: الدافع لارتكاب الجريمة المعلوماتية

تختلف الجريمة المرتكبة عبر الإنترنت عن الجريمة التقليدية من حيث دوافع ارتكابها، حيث أن مجرمي الإنترنت يسعون من خلال ارتكابهم للجريمة إلى أهداف معينة بالإضافة إلى تحقيق المكسب المالي مع تحقيق الأغراض المعنوية كالتعلم أو اللعب أو لمجرد الانتقام.

الرغبة في تحقيق مكاسب مادية تكون هائلة احيانا بزمن قياسي قد يكون من أكثر البواعث التي تؤدي إلى إقدام مجرمي المعلوماتية على اقتراف جرائمهم من اجل تحقيق المكاسب المالية هذه، يتم اللجوء إلى ارتكاب الجريمة المعلوماتية أما عن طريق المساومة على البرامج أو المعلومات المتحصل عليها بطريقة الاختلاس من جهاز الحاسوب عن طريق استعمال بطاقة سحب آلي منتهية الصلاحية أو مزورة او غير ذلك الكثير، ولقد أشارت مجلة (sécurité informatique) وهي مجلة متخصصة في الأمن المعلوماتي أن 43 % من حالات الغش المعلن عنها قد نصت من أجل اختلاس اموال و23% من أجل سرقة المعلومات و19% أفعال إتلاف و15 % سرقة وقت الآلة أي استعمال غير مشروع للحاسوب الآلي لأجل تحقيق منافع شخصية[1].

من أخطر الدوافع التي تدفع إلى ارتكاب الجريمة الانتقام الذي يصدر عن شخص يملك معلومات كبيرة وكثيرة عن المؤسسة التي يعمل بها، لفصله من العمل أو في الحوافز، حيث يقوم بزرع برنامج لتخريب المعلومات أو يقوم بحذفها أو تغييرها.

[1] نهلة عبد القادر المومني، مرجع سابق، ص 90.

وتعتبر الدوافع كذلك من أهم المحفزات على ارتكاب الجرائم المعلوماتية اذا تم تسخير شبكة الأنترنت في العديد من الصراعات، فشبكة الأنترنت تستعمل بشكل دائم لاختراق مواقع الحكومية أو تعطيلها أو الترويج لأعمالها الارهابية أو الأفكار المتطرفة أو محظورة[1].

وفي الأخير يمكننا القول أن المجرم المعلوماتي هو عبارة عن مزيج في الملامح الخاصة والدوافع العديدة، فالمجرم المعلوماتي لا يعني وبالضرورة أنه من فئة وحيدة وله دافع خاص معين، بل هو حسب شخصيته ودوافعه قد ينتمي إلى أكثر من فئة.

الفرع الثالث: تصنيف المجرم المعلوماتي

التطور في مجال استعمال الأنترنت أدى إلى ظهور عدة أصناف من المجرمين يصعب حرصهم تحت طوائف محددة، حيث صنفتهم الإتجاهات الفقهية الباحثة إلى فئات وهذا راجع إلى مقدار الخطورة الإجرامية الكامنة في التخلص المجرم المعلوماتي، وهذا ما سنتطرق إليه فيما يلي:

أولا: صغار مجرمي الأنترنت

كما يسمون صغار نوابغ المعلوماتية ويقصد بهم الشباب البالغ المقترن بالمعلوماتية وأنظمتها[2]، أنها تعتبر تلك المجموعات التي تميل إلى التحدي الفكري وهم غالبا ما يكونون في فترة المراهقة وعلى الرغم من صغر سنهم إلا أنهم قادرون على اقتحام كافة أنواع الأنظمة البنكية والشركات والمؤسسات المالية.

[1] عبد اللطيف معتوف، الإطار القانوني لمكافحة الجرائم المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماجيستر في العلوم القانونية، جامعة العقيد لخضر، باتنة، 2012، ص 13.

[2] محمد ساميالشوا ثورة المعلومات وإنعكاساتها على قانون العقوبات، دون طبعة، دار النهضة العربية، القاهرة، سنة 1994، ص 39.

ثانيا: طائفة القراصنة

وهناك صنفان:

أ- القراصنة الهواة(الهاكرز) Hackers:

كان يطلق على الأشخاص الذين يملكون قدرات عالية المستوى في البرمجة، والذين يتميزون بقدرات إبداعية معهد ماشوستس للتكنولوجيا، وكذلك البرمجيين في ستانفورد وجامعة brekely، حيث يعرف الهاكرز بأنه الشخص الذي يقوم بإنشاء أو تعديل البرمجيات والعتاد الحاسوبي، ويقصد بهم الشباب البالغ المفتون بالمعلوماتية والحاسبات الآلية، أغلب هذه الطائفة هم من الطلبة والشباب حاصلين على المعرفة في مجال تقنيات المعلوماتية والباعث الأساسي لهذه الطائفة هو الإستمتاع باللعب والمزاح بإستخدام هذه تقنيات لإثبات مهارتهم وقدراتهم بإكتشاف وإظهار مواطن الضعف في الأنظمة المعلوماتية، دون أي إلحاق ضرر بها هم لديهم الرغبة في المغامرة والتحري والرغبة في الإكتشاف. [1]

ب-القراصنة المحترفين Crackers:

ويعني ذلك المقصد تعرف هذه الطائفة بالمجرمين البالغين أو المخربين المهنيين والكراكز تتراوح أعمارهم بين 25-45 عاماً ومن أبرز سمات وخصائص أفراد هذه الطائفة أنهم ذوي مكانة في المجتمع وأنهم دائما ما يكونوا من المتخصصين في مجال التقنية الإلكترونية أي أنهم يتمتعون بمهارات ومعارف فنية في مجال الأنظمة الإلكترونية والمعلوماتية تمكنهم من الهيمنة الكاملة في بنية المعالجة الآلية للمعلومات. [2]

---

[1] عبد الفاتح اليومي الحجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، الاسكندرية، الطبعة الأولى، سنة 2006، ص 46.

[2] محمد دباس الحميد، ماركو إبراهيم ، حماية الأنظمة المعلوماتية، دار حامد للنشر والتوزيع، عمان، الطبعة الأولى، 2007، ص 73.

وعادة ما يعود المجرم المحترف بالجريمة المعلوماتية مرة أخرى، لأن اعتداءاتهم وميولهم الإجرامي خطير ينتج عنه إحداث التخريب، بالتالي فهم أكثر خطورة من الفئة الأولى.

ثالثا: المتطرفين فكريا

تتألف هذه الفئة من الجماعات الإرهابية أو المتطرفة التي تتكون من مجموعة من الأشخاص لديهم معتقدات وأفكار اجتماعية وسياسية أو دينية ويرغبون في فرض هذه المعتقدات باللجوء إلى النشاط الإجرامي ويتركز نشاطهم بصفة عامة في استخدام العنف ضد الأشخاص والممتلكات من أجل لفت الأنظار إلى ما يدعون إليه، وبدأ اهتمام هذه الجماعات وخاصة تلك التي تتمتع بدرجة عالية من التنظيم يتجه إلى نوع جديد من النشاط الإجرامي إلا وهو الجريمة المعلوماتية[1]، فإعتماد المؤسسات المختلفة داخل الدول على أنظمة الحاسبات الآلية في إنجاز أعمالهم والأهمية القصوى للمعلومات التي تحتويها في أغلب الأحوال قد جعل من هذه الانظمة هدفا جذابا لهذه الجماعات، ولا تزال هذه الأمثلة في هذا المجال قليلة وإن كان من المتوقع أن تزداد مستقبلا، ومن الأمثلة الشهيرة في هذا الخصوص قيام احدى الجماعات الإرهابية المعروفة في أوروبا بإسم The Red Brigades يدير 60 مركز للحسابات الآلية خلال الثمانينات لتلفت الأنظار إلى أفكارها ومعتقداتها[2].

رابعا: المبرمجون les codeurs

هم فئة من ذوي الخبرة في مجال المعلوماتية لا تقل عن (5) سنوات وبالضبط في مجال القرصنة المعلوماتية يتولون مهام البرمجة، بحيث يعملون على إنشاء وتعديل

[1] نهلة عبد القادر المومني، مرجع سابق، ص 85 ص 86.

[2] نائلة عادل محمد فريد وردة، المرج السابق، ص64 ص 65.

وتحديث البرامج المعلوماتية الحديثة التي تعتبر سلاح الجريمة المعلوماتية يقومون ببيعها عبر الشبكة لفائدة مجرمي أنترنت[1].

خامسا: المنتقمين

ظهرت هذه الفئة مع عصرنة الإدارة في أغلب دول العالم للأخذ بما يعرف بالإدارة الإلكترونية، بالرغم من إجابتها التي حملتها هذه العصرنة في طياتها لكنها استعملت سلبا من طرف بعض موظفي الإدارات الذين اصطلح عليهم بمصطلح الموظف الحاقد أو المنتقم.

حيث يشكل هذا الموظف الحاقد خطر كبير على الأنظمة المعلوماتية للإدارة والشركة أو المنشأ الذي يعمل بها، حيث يعمد إلى توظيف خبرته ومعرفته في سلوكات عدائية لإلحاق أكبر خسائر ممكنة بها، وتعدد حالات حسب الميادين والجهات، مثلا كاستغلال الثغرات ونقاط الضعف في النظام لتخريبه أو إتلاف أرشيف المستخدمين، وبالتالي هنا تكمن الخطورة الإجرامية الموظف الذي يستهدف بإجرامه الإنتقام والثأر من أصحاب وأرباب العمل[2].

المبحث الثاني: أنواع الجرائم المعلوماتية

مع التطور السريع لاستخدام شبكة الأنترنت في شتى المجالات، مما جعل الجرائم المرتكبة عليها من الجرائم المستحدثة، وهي تستهدف الكثير من القطاعات، مما جعل مهمة حصرها وتصنيفها تتميز بالصعوبة، وتجدر الإشارة أن تحليل صور الجريمة المرتكبة عبر الأنترنت وبيان أصنافها ليس بالأمر البسيط الذي يرجع إلى التباين

[1] ربيعي حسين، الجرم المعلوماتي شخصية وأصنافه، مجلة العلوم الإنسانية، جامعة محمد حنيفي، بسكرة، العدد 40، جوان 2015، ص299.

[2] أ، د، النحوي سليمان، طبيعة الخطورة الإجرامية للمجرب المعلوماتي، مجلة الإشراف الباحث في الدراسات القانونية والسياسية، جامعة محمد ثليجي الأغواط، المجلد 05، العدد 01، سنة 2020، ص 991,

والإختلاف لدى الفقه في تصنيفهم للجريمة المعلوماتية تصنيفا موحدا، لذا ارتأيتنا تقسيم وتصنيف الجريمة المعلوماتية على النحو التالي:

المطلب الأول: جرائم واقعة على النظام المعلوماتي

إضافة إلى الجرائم المعلوماتية التي تقع باستخدام النظام المعلوماتي، هناك نوع آخر من الجرائم المعلوماتية يمس بالنظام المعلوماتي ويستهدف فيه المعلوماتية لارتكاب الجرائم. وقد نجد ذلك في نوعين من الجرائم، وهي جرائم الواقعة على نظام المعالجة الآلية للمعطيات وكذلك الجرائم الواقعة على المعلومات داخل أنظمة المعالجة الآلية وذلك ما سنتطرق إليه في الفرعين الأتيين:

الفرع الأول: الجرائم الواقعة على نظام المعالجة الآلية للمعطيات

وسنتطرق في هذا الفرع على الجرائم الواقعة على نظام المعالجة الآلية للمعطيات وفق العناصر التالية:

أولا: جريمة الدخول أو البقاء غير المشروع في المنظومة المعلوماتية

1- جريمة الدخول

تعد جريمة الدخول غير المشروع إلى المنظومة المعلوماتية صورة في الوضعية الغير شرعية اتجاه هذه المنظومة، وقد نص المشرع الجزائري في هذه الجريمة في المادة 394 مكرر 1، والتي تنص: " يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة من 50.000 إلى 100.000 دج كل من يدخل أو يسعى عن طريق الغش في كل أو جزء من المنظومة للمعالجة الآلية للمعطيات أو يحاول ذلك"[1]. فالملاحظ أن القانون الجزائري لا يجرم فحسب الدخول إلى النظام المعلوماتي بل يكفي الدخول إلى جزء منه لقيام الجريمة، حيث تعد هذه الجريمة من الجرائم العمدية، حيث يتطلب لقيامها ومن ثم العقاب عليها توفر القصد الجنائي العام بعنصريه لدى مرتكبيها بصفتيه أن نتيجة إرادته

[1] المادة 394 من قانون العقوبات الجزائري المعدل والمتمم بموجب القانون 15/04 المؤرخ في 10-11 – 2004.

إلى فعل الدخول إلى النظام المعلوماتي مع عمله التام بأنه يدخل نظاما معلوماتيا غير مصرح به (الدخول)[1] إليه نستنتجه من نص المادة 394 مكرر والتي تنص " ... كل من يدخل أو يبقى عن طريق الغش ...".

2- جريمة البقاء غير المشروع

كما نصت المادة 394 مكرر 01 من القانون 15/04 على جريمة الدخول غير المشروع إلى المنظومة المعلوماتية احتوت فقرتها الثانية على جريمة البقاء في نفس المنظومة بصفة غير مشروعة، وبجريمة الدخول غير مشروع لا يشترط المشرع الجزائري أن يرتكب جريمة البقاء على كامل النظام بل يكفي البقاء في جزء منه ليكتمل ركن الجريمة.

ثانيا: جريمة التلاعب بمعطيات الحاسب الآلي

جريمة التلاعب هي الثانية التي ينص عليها قانون العقوبات الجزائري بعد جريمة الدخول أو البقاء غير المصرح بها، أما قانون العقوبات الفرنسي فينص عليها بعد جريمة إعاقة وإفساد أنظمة المعالجة نظرا للتشابه الكبير بينهما وبين جريمة التلاعب بالمعطيات، بحيث يصعب في الكثير من الأحيان التمييز بينهما وذلك لأن الأفعال التي تتضمنها جريمة التلاعب تؤدي هي الأخرى إلى إعاقة النظام وإفساده، وقد اكتفى المشرع الجزائري نتيجة إفساد النظام كظرف مشدد فقط لجريمة الدخول واستبعادها كجريمة قائمة بحد ذاتها والنشاط الإجرامي في هذه الجريمة يتمثل في أفعال الإدخال والتعديل، ويكفي توافر أحدهما لقيام الجريمة لا يشترط إجتماعها حتى يتوافر النشاط الإجرامي فيها، ومن ثم يقام الركن المادي للجريمة لكن القاسم المشترك في هذه الأفعال جميعها هو انطوائها على

[1] بردال سمر، الجريمة المعلوماتية في التشريع الجزائري، مجلة القانون، المركز الجامعي غليزان، العدد 2، جويلية 2010، ص 186.

التلاعب في المعطيات التي يتضمنها نظام معالجة البيانات بإدخال معطيات جديدة غير صحيحة أو محو أو تعديل. [1]

ثالثا: جريمة التعامل في معطيات غير مشروعة

نصت على تجريمها المادة 394 مكرر في فقرتها الأولى من قانون العقوبات كما يلي: "يعاقب بالحبس من شهرين (2) إلى ثلاثة (3) سنوات وبغرامة من 100,000 دج إلى 500,000 دج كل من يقوم عمدا وعن طريق الغش بما يأتي:

– 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.

– حيازة أو افتاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها هي إحدى الجرائم المنصوص عليها في هذا القسم"[2].

حيث أن الشرع الجزائري تكفل بالحماية لنظام المعالجة الآلية حيث قام بتجريم مجموعة من الأفعال التي تمس سرية المعلومات وسلامتها، حيث أتت هاته الأفعال في صورتين أولهما يتمثل في التعامل في معطيات صالحة لارتكاب جريمة والثانية هي التعامل في معطيات متحصلة من جريمة، حيث كل صورة منها هي مجموعة من الأفعال المكونة للركن المادي للجريمة التعامل في المعلومات غير المشروعة.

1- الصورة الأولى: جاءت في المادة 394 مكرر 2 في الفقرة (1) وهي الآتي:

أ- **التصميم:** هي أول عملية في سلسلة التعامل في المعطيات وهي تتمثل في اخراج المعطيات إلى الوجود أي القيام بخلق وايجاد معطيات صالحة لارتكاب الجريمة، وهذا

[1] إبتسام ميهوب، جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري، مذكرة لنيل شهادة ماجيستر، كلية الحقوق، جامعة العربي بن المهيدي أم البواقي، 2014، ص 15-16.

[2] المادة 394 مكرر 2، قانون العقوبة الجزائري، قانون 15/04، المؤرخ في 10 نوفمبر 2004.

العمل يقوم به المختصون في المجال كمصممي البرامج ومثال هذا: تصميم برنامج يحمل فيروسا وهذا ما يطلق عليه بالبرامج الخبيثة[1].

ب- البحث: يقصد بالبحث في نص المادة 394 مكرر2 بالبحث عن أداة والمعلومات لمعرفة تصميم وإعداد المعلومات لارتكاب الجريمة.

ج- التجميع: يقصد به تجميع أكبر عدد من المعطيات التي يمكن الإعتماد عليها لارتكاب الجريمة.

د- التوفير: من الأعمال التي جرمتها نص المادة 394 مكرر 2 أيضا فعل التوفير، ويقصد به توفير كم من المعطيات التي تمكن من ارتكاب جريمة الدخول أو بقاء أو جريمة تلاعب بالمعطيات.

هـ- النشر: هو اذاعة المعلومات ومحل الجريمة وتمكين الغير من الاطلاع عليها، اذ من شأنه نقل هذه الأخيرة إلى عدد كبير من الأشخاص[2].

و- الإتجار: هو تقديم المعطيات للغير بمقابل سواء كان نقديا أو عينيا أو عن طريق خدمة أو غيرها.

2- **الصورة الثانية:** وهي التعامل في المعطيات المتحصلة من الجريمة وجاءت في المادة 394 مكرر2 الفقرة 2 كما يلي:

أ-الحيازة: هي سيطرة الجاني على المعلومات للإنتفاع بها، أو التعديل فيها، أو نقلها، أو استعمالها بطريقة غير مشروعة.

ب- النشر: فعل النشر من أخطر الأفعال التي يمكن أن ترد على المعطيات المجرمة لكونه يقوم بنقلها لأكبر عدد من الأشخاص، ومجال النشر هو المكان المناسب الذي المحترفون.

---

[1] ابتسام ميهوب، مرجع سابق، ص 31-32.

[2] رشيدة بوبكر، جرائم الإعتداء على نظام المعالجة الآلية في التشريع الجزائري المقارن، الطبعة الأولى، منشورات حلبي الحقوقية، بيروت، لبنان، سنة 2012، ص 282-283.

ج- الاستعمال: هو الاستعمال الغير مشروع للمعلومات مهما كان الهدف منه في هذا الاستعمال ومهما كان نوعه أو الوسائل المستخدمة في ذلك وحتى لو تم هذا الاستعمال لمرة واحدة. حيث نصت عليه المادة صراحتا بـ: "... أو أي استعمال لأي غرض كان".

الفرع الثاني: الجرائم الواقعة على المعلومات داخل أنظمة المعالجة الآلية للمعطيات

أولا: سرقة المال المعلوماتي

ظهرت جريمة السرقة المعلوماتية المتمثلة بسرق المعلومات من برامج وبيانات مخزنة من دائرة الكمبيوتر أو نسخ برامج المعلومات بصورة غير شرعية، بعد تمكن مرتكب هذه الجريمة من التحصل على كلمة السر أو بواسطة التقاط موجات كهرومغناطسية الصادرة عن الحاسب الآلي أثناء تشغيله أو باستخدام نهايات طرفية تتصل بالحاسب الآلي.

وبالرجوع إلى تحليل جريمة السرقة التقليدية نجد أن المال فيها منقولا، فتنقل حيازته من المالك إلى السارق، ومعظم التشريعات لا تعترف بسرقة المعلومات بل الوصول غير المصرح لها واختراقها وتقليدها والإستلاء عليها ونسخها نسخا غير مشروعا يعد جريمة، هذا ما نراه بوجوب عدم قياس نصوص السرقة التقليدية على السرقة المعلوماتية مما يدعو إلى إقتراح أن يتدخل المشرع بنص صريح لمواجهة هذه الظاهرة الاجرامية المعاصرة[1].

ثانيا: اتلاف المعلومات وبرامج الحاسب الآلي

يقصد بالإتلاف المعلوماتي: "كل فعل الغاية من القيام به تدمير المعطيات أو التدمير كليا وذلك بجعلها غير صالحة للاستعمال أو تدميرا جزئيا ذلك من قيمة أدائها[2]" وعليه فإن الإتلاف لا يتحقق في التأثير على مادة الشيء عموما بل يتحقق في حالة

[1] محمد عبد المحسن بن طريف، جريمة السرقة المعلوماتية، مجلة الدراسات والبحوث القانونية، المجلد 7، العدد 2، 2022، جامعة عمان العربية، الأردن، ص 17

[2] عابد راجا الخلايا، المسؤولية التقصيرية الإلكترونية، المسؤولية الناشئة عن إستخدام أجهزة الحاسوب والأنترنت، دراسة مقارنة، طبعة 1، دار الثقافة، عمان، 2009، ص 109.

الإنقاص من قيمته، بإتلاف أو محو تعليمات البرامج أو البيانات ذاتها، وعادة لا يستهدف مرتكب هذه الجريمة فائدة مالية لنفسه بل بمجرد إعاقة نظام المعلومات عن الأداء بوظيفته وإحداث الضرر فيه.

حيث ترتكب جرائم إتلاف المعلومات عن طريق برامج الدودة والقنابل المعلوماتية والفيروس الذي يقصد "برنامج تم اعداده من قبل شخص أو أكثر على درجة متقدمة من العلم بالبرمجة باستخدام التقنيات المتطورة، بحيث يكون من خصائص هذا البرنامج الإنتقال إلى أجهزة الحاسب الآلي والتكاثر والإنتشار فيها".[1]

المطلب الثاني: الجرائم التي تتم عن طريق النظام المعلوماتي

تعد الجرائم المرتكبة على الأنترنت من الجرائم المستحدثة، حيث تستهدف الكثير من القطاعات ما جعل صعوبة في تحديدها وتصنيفها عكس الجريمة التقليدية التي يتم تصنيفها بكل سهولة.

فتشعب هذه الجرائم لم يسمح للفقهاء لتصنيفها تصنيفا مستقرا على معيار واحد، وعلى هذا الأساس سنعتمد في تقسيم هذا المطلب على مختلف معايير التصنيف وهي الجرائم الواقعة على أشخاص (فرع أول)، الجرائم الواقعة على أموال (الفرع الثاني) الجرائم الواقعة على أمن الدولة (الفرع الثالث).

الفرع الأول: الجرائم الواقعة على أشخاص

إن للحياة الشخصية خصوصية وحرمة لا يجوز لأي شخص أن يقتحمها، ومثال ذلك الإعتماد على المعلومات الالكترونية الخاصة بالمحامين والأطباء أو المحاسبين، أو

[1] أسامة محمد محي الدين عوض، جرائم الكمبيوتر، بحث مقدم للمؤتمر السادس للجمعية العربية للقانون الجنائي، ص 240.

غيرهم من المهنيين، وقد تتم هذه الجريمة من خلال الاطلاع على البيانات والمعلومات الخاصة بشخص ما أو تسجيل مكالمات أو فيديو أو مراقبته[1].

أولا: جرائم السب والقذف وتشويه السمعة

تعد جرائم السب والقذف وتشويه السمعة أكثر تداولا في نطاق شبكة الأنترنت، حيث تستعمل للمساس بشرف الغير أو كرامتهم أو اعتبارهم، حيث يستعمل الجاني حسب القواعد العامة لجرائم القذف والسب عبارات بذيئة تمس وتخدش شرف المجني عليه، ومهما كانت الوسيلة المعتمدة، مع علمه أن ما يقوم به يعد مساس بسمعة الغير، بل أن ارادته اتجهت إلى ذلك بالذات، وبالتطور أصبحت الأنترنت إحدى هذه الوسائل إن لم تقل أكثرها رواجا فعادة ترسل عبارات السب والقذف عبر البريد الصوتي أو ترسم أو نكتب على صفحة الوايب ما يؤدي كل من يدخل هذا الموقع إلى مشاهدتها أو الاستماع إليها، ويتحقق بذلك ركن العلنية التي تطلبه الكثير من التشريعات من السب العلني، وإذا لم يطلع عليها أحد فإنه يمكن تطبيق مواد السب أو القذف العلني[2].

ثانيا: صناعة ونشر الإباحة

إذا كان لشبكة الأنترت وجه إيجابي فإن لها وجه سلبي أيضا، ومن هذه الأوجه وجود مواقع على شبكة الأنترنت تحرض على ممارسة الجنس لكبار والصغار على حد سواء، تقوم هذه المواقع بنشر صور جنسية فاضحة للبالغين والأطفال[3].

---

[1] بوضياف إسمهان، الجريمة الالكترونية والاجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية السياسية، العدد 11، الجزائر، 2018، ص 357.

[2] صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة ماجيستير في القانون الدولي للأعمال، كلية الحقوق، جامعة مولود معمري، تيزي وزو، 2014، ص 53.

[3] محمد عابيد الكعبي، الجرائم الناشئة عن إستخدام الغير المشروغ لشبكة الانترنت، دار النهضة العربية، القاهرة، بدون سنة، ص 8.

وإذا كانت الدعوة لممارسة الجنس الموجه للبالغين يمكن أن تلاقي الرفض لتوافر تمام العقل لديهم، فإن الوضع بالنسبة للطفل الصغير يختلف لصغره وعدم اكتمال نضجه القعلي[1].

ثالثا: إنتحال الشخصية والتغرير والإستدراك

يقصد بإنتحال الشخصية ما يعيد إليه المجرم من إستخدام شخصية شخص آخر للإستفادة من سمعته مثلا أو ماله أو صلاحياته، ولذلك فهذا سبب وجيه يدعو للاهتمام بخصوصية وسرية المعلومات الشخصية للمستفدين على شبكة الأنترنت، وتتخذ جريمة إنتحال الشخصية عبر الأنترنت أحد الوجهين الآتيين: إنتحال شخصية الفرد وإنتحال شخصية المواقع.

ولقد سماها بعض المتخصصين في أمن المعلومات جريمة الألفية الجديدة وذلك نظرا لسرعة انتشار ارتكابها خاصة في الأوساط التجارية.

أما فيما يخص التغرير والاستدراج فغالبا يكون ضحايا هذا النوع من صغار السن من مستخدمي الشبكة، حيث يوهمهم المجرمون ضحاياهم برغبتهم في تكوين صداقة على الإنترنت والتي قد تتطور إلى التقاء مادي بين الطرفين[2].

رابعا: جريمة التهديد والمضايقة

يقصد بالتهديد الوعيد بالشر وهو زرع الخوف في النفس بالضغط على إرادة إنسان وتخويفه من أضرار ما سيلحقه أو سيلحق أشياء أو أشخاص له بها صلة[3].

---

[1] عبد الكريم خالد الشامي، جرائم الكمبيوتر والانترنت في التشريع الفلسطيني، ص 19، مثال متوفر على بوابة فلسطين القانونية http:// www.pal-ip.org.

[2] عمرو موسى الفقهي، الجرائم المعلوماتية، جرائم الحاسب الآلي والنترنت في مصر والدول العربية، المكتب الجامعي الحديث، الاسكندرية، 2006، ص 102.

[3] محمد الكعبي، مرجع سابق، ص 88.

ويعد تهديد الغير من خلال البريد الإلكتروني واحدا من أهم الاستخدامات غير المشروعة للإنترنت، حيث يقوم الفاعل بإرسال رسالة إلكترونية للمجني عليه تنطوي على عبارات تسبب خوفا أو ترويعا لمتلقيها.

الفرع الثاني: الجرائم الواقعة على الأموال

أولا: السرقة عبر أنترنت

تعرف السرقة بانها إختلاس الشيء المنقول مملوك للغير دون رضاه بنية إمتلاكه[1]، وتتم سرقة المال المعلوماتي إن أمكن الوصف عن طريق إختلاس البيانات والمعلومات، والإفادة منها إستخدام السارق للمعلومات الشخصية، مثل الإسم، العنوان، الأرقام الخاصة بالمجني عليهم والإستخدام غير الشرعي لشخصية المجني عليه ليبدأ بها عملية السرقة المتخفية عبر الأنترنت بحيث تؤدي بالغير إلى تقديم الأموال – إلكترونية أو مادية– إلى الجاني عن طريق التحويل البنكي.

ثانيا: جرائم السطو على أرقام بطاقات الإئتمان والتحويل الالكتروني غير المشروع للأموال

واكب استخدام البطاقات الائتمانية من خلال شبكة أنترنت واكبه ظهور الكثير من المتسللين للسطو عليها، باعتبارها نقودا الكترونية ، خاصة من جهة أن استيلاء على بطاقات الإئتمان أمر ليس بالصعوبة كما كان، فلصوص بطاقات الإئتمان مثلا يستطيعون الآن سرقة مئات الألوف من أرقام بطاقات في يوم واحد من خلال شبكة الأنترنت ومن ثم بيع هذه المعلومات للآخرين[2].

[1] نايف بن محمد الماروني، جريمة السرقة (دراسة نقدية إجتماعية)، جامعة نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، ص 57.

[2] حسين طاهر داود، جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية، الرياض، الطلعة الأولى،2000، ص 73.

تتم عملية تحويل الالكتروني غير المشروع للأموال من خلال الحصول على كلمة السر المدرجة في ملفات أنظمة الكمبيوتر الخاصة بالمجني عليه، مما يسمح للجاني بالتوغل في النظام المعلوماتي وعادة ما يكون هؤلاء من العاملين على إدخال البيانات في ذاكرة الجهاز أو من قبل المتواجدين على شبكة أثناء عملية تبادل البيانات[1] وتتم عملية التحويل الالكتروني غير المشروع للأموال عن طريق الاحتيال الذي يتم بوهم المجني عليه بوجود مشروع كاذب أو يحدث الأمل لديه بالحصول على الربح فيسلم المال للجاني بطريقة معلوماتية من خلال تصرف الجاني في المال وهو يعلم أن ليس له صفة التصرف فيه أو عن طريق الاحتيال باستخدام بطاقة دفع الكتروني.

ثالثا: القمار وغسيل الأموال عبر الأنترنت

تتداخل عملية غسل الأموال مع ممارسة القمار عبر شبكة الأنترنت مما زاد من انتشار أندية القمار والكازينوهات الافتراضية عبر الأنترنت محل للمراقبة والاشتباه ومن البديهي أن يأخذ المجرمون بأحدث ما توصلت إليه التقنيات لخدمة أنشطتهم الإجرامية ويشمل ذلك بالطبع طرق غسل الأموال التي استفادت من عصر التقنية فلجأت إلى الأنترنت لتوسعة وتسريع أعمالها في غسيل الأموال غير المشروعة[2].

وقد ساعدت شبكة الأنترنت القائمون بعمليات غسيل الأموال بين الدول وتفادي القوانين التي قد تضعها الدول من أجل إعاقة هذا النشاط وكذا تشفير عملياتهم مما يعطيها قدر كبير من السرية، وخاصة في تسهيل مرتكبي جرائم غسل الأموال نقلها إلى أي مكان في العالم[3].

---

[1] خاد ممدوح إبراهيم، امن الجريمة الالكترونية، دار الجامعية، اسكندرية، 2010، ص 76.

[2] محمد زيدان، محمد جمو، "متطلبات أمن المعلومات المصرفية في بيئة الأنترنت"، المؤتمر السادس لجمعيات المكتبات المعلومات السعودية، المعلومات الأمنية والتشريعات والتطبيقات، 6-7 أفريل 2010، الرياض، ص 09.

[3] خالد بن عبد الله بنو معييض العابدي، الحماية الجنائية للتعاملات الالكترونية، في نظام المملكة العربية السعودية، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، قسم العدالة الجنائية، الرياض، 2009، ص 179.

الفرع الثالث: الجرائم الواقعة على أمن الدولة

أخذت الجماعات المتطرفة الطبيعة الاتصالية للأنترنت من أجل بث أفكارها ومعتقداتها، بل تعدي الأمر إلى أفعال تمس أمن واستقرار الدولة، خاصة ما يسمى بالإرهاب والجريمة المنظمة، بل أخطر من ذلك سمحت لهم الأنترنت بالتجسس على الدول الأخرى وهذا ما سنتناوله فيما يلي:

أولا: الجريمة المنظمة

عرفت الجريمة المنظمة بأنها تعبير عن مجتمع إجرامي يعمل خارج إيطار الشعب والحكومة ويضم بين طياته آلاف المجرمين الذين يعملون وفقا لنظام بالغ الدقة والتعقيد يفوق النظم التي تتبعها أكثر المؤسسات تطورا وتقدما، كما يخضع أفرادها إلى أحكام قانونية سنوها لأنفسهم وتفرض أحكاما بالغة القسوة على من يخرج عن قاموس الجماعة ويلتزمون في أداء أنشطتهم الإجرامية بخطط دقيقة مدروسة يلتزمون بها ويجنون من ورائها الأموال الطائلة[1].

الجريمة المنظمة ليست وليدة التقدم وإن كانت استفادت منه، فالجريمة المنظمة وبسبب تقدم وسائل الاتصال والتكنولوجيا أصبحت غير محددة لا بقيود الزمان ولا بقيود المكان، بل أصبح انتشارها على نطاق واسع وكبير وأصبحت لا تحدها الحدود الجغرافية، كما استغلت عصابات الجريمة المنظمة الإمكانيات المتاحة في وسائل الإنترنت في تخطيط وتمرير وتوجيه المخططات الإجرامية، وتنفيذ وتوجيه العمليات الإجرامية بكل سهولة[2].

[1] نهلة عبد القادر المومني، مرجع سابق، ص 87.

[2] سامس علي عياد، الجريمة المعلوماتية والانترنت (الجرائم الالكترونية)، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2007، ص 83.

ثانيا: الإرهاب

أصبح يتم بث الإرهاب في الوقت المعاصر ظاهرة عالمية ترتبط بعوامل اجتماعية وثقافية وسياسية وتكنولوجية أفرزتها التطورات السريعة والمتلاحقة في العصر الحديث[1]، بحيث أصبح زرع ثقافة الإرهاب وبثها عبر الأنترنت عن طريق تأسيس مواقع افتراضية تمثل المنظمات الإرهابية، وأصبحت الجماعات الإرهابية تجند عناصر جديدة من خلال الأنترنت فتعلن عبر موقعها على الأنترنت حاجتها إلى عناصر انتحارية كما لو كانت تعلن عن وظائف شاغرة للشباب، مستخدمة في ذلك الجانب إلى الجهاد وحثهم إلى الاستشهاد في سبيل الله والفوز بالجنة[2].

المواقع الالكترونية أضحت عامل يتيح للجماعات الإرهابية القدرة الكبيرة في توجيه الرسائل الإعلامية والتحكم في المعلومات التي تريد توجيهها لفئات مختلفة من الجمهور ورسم صورة ذهنية عن الجماعات عن أعدائها أيضا.

ثالثا: جريمة التجسس

الاستخدام المتزايد للحاسبات الآلية في العديد من المجلات ينتج تجميع المعلومات بدرجة كبيرة في موضع واحد، ويؤدي هذا التخزين في الحاسبات المركزية إلى سهولة التجسس عليها، وعلى المعلومات المخزنة فيها بمختلف درجات سريتها، يقصد بالتجسس في هذا الموضع هو الاطلاع على المعلومات خاصة بالغير مؤمنة في جهاز آخر، وليس مسموحا لغير المخولين بالاطلاع عليها[3].

---

[1] عبد الله بنو عبد العزيز اليوسف، أساليب تطور البرامج والمناهج التدريبية لمواجهة الجرائم المستحدثة، جامعة نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، 2004، ص 25

[2] محمد سلطان، قضايا قانونية وحماية البيئة الالكترونية، دار ناشري للنشر والتوزيع الالكتروني، 2004، ص 13.

[3] محمد عبد الرحيم سلطان علماء، "جرائم الانترنت"، مؤتمر القانون الكمبيوتر والانترنت، المنعقد من 1-3 ماي 2000، بجامعة الامارات كلية الترقية و القانون، الجلد 3، الطبعة الثالثة، 2004، ص 880.

ومن جهة سهلت شبكة الأنترنت على مجرمي هذه الجريمة بشكل كبير حيث يقومون بالتجسس على الأشخاص أو الدول أو المنظمات أو الهيئات أو المؤسسات الدولية أو الوطنية، وتستهدف عملية التجسس في العصر الحالي المعلوماتي ثلاثة أهداف رئيسية: التجسس العسكري، والتجسس السياسي، والتجسس الاقتصادي[1].

حيث أن الشرع الجزائري اعتبر الجرائم المعلوماتية التي تستهدف الدفاع الوطني أو أي مؤسسات الرسمية بمثابة طرف تشديد وهذا ما أتى في المادة 394 مكرر3 بقولها:" تضاعف العقوبات المنصوص عليها في هذا القسم، اذا استهدفت الجريمة الدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام، دون الاخلال، تطبق عقوبات أشد".

[1] علي عدنان الفيل، الإجرام الالكتروني، الطبعة الأولى، منشورات زين الحقوقية، دمشق، 2011، ص 76.

الفصل الثاني

الإطار الإجرائي لجريمة الدخول إلى النظام المعلوماتي

ان الجريمة تقوم بتوافر اركانها الاساسية وهذا ما يطبق على الجرائم المعلوماتية ايضا فلا تقوم اي جريمة معلوماتية بدون اركانها ولا تخلو من العقوبات، وبهذا الصدد نتخصص في دراستنا جريمة الدخول الى النظام المعلوماتي من خلال دراستنا وما جاء به النصوص القانونية، من عقوبات لهذه الجريمة ودراسة سلوك الجاني والنتيجة الذين يمثلان الركن المادي للجريمة، الى الجاني الركن المعنوي لها ومدى توفر الحماية للنظام المعلوماتي، حيث صادقت العديد من الدول الغربية لمكافحتها وكذلك المشرع الجزائري، الذي اصدر بحقها عقوبات مختلفة لها.

ولتوضيح الاطار القانوني هذه الجريمة لابد من دراسة محتواها من خلال اركان هاته الجريمة والعقوبات المقررة لها، وهذا ما سنتطرق له من خلال:

المبحث الاول: اركان جريمة الدخول

المبحث الثاني: العقوبات المقررة للجريمة

المبحث الأول: أركان جريمة الدخول إلى النظام المعلوماتي

الشرع الجزائري بموجب الأمر 15/04 المؤرخ في 20 ربيع الثاني 1436هـ الموافق 10 فبراير 2015 المعدل والمتمم للأمر 66-156 المتضمن قانون العقوبات نصوصا خاصة بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو ما يصطلح عليها بالجريمة المعلوماتية أو الإلكترونية والتي تندرج ضمنها جريمة الدخول و البقاء الغير مشروع والتي تشكل بدورها كل فعل أو امتناع من شانه الاعتداء على الكيانات المعنوية بطريقة مباشرة أو غير مباشرة عن تدخل تقنية المعلومات، ولقد ورد نص على هذه الجرائم والعقوبات المقررة لها في المواد 394 مكرر إلى 394 مكرر 7.

نص الشرع الجزائري في المادة 394 مكرر من قانون العقوبات الجزائري على ما يلي: "يعاقب ... كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات..."، وانطلاقا من نص السابق سنحاول تفصيل أركان هذه الجريمة من خلال المطالب التالية.

المطلب الأول: الركن المادي لجريمة الدخول

باستقراء نص المادة 394 مكرر من قانون العقوبات الجزائري، ينتج أن الركن المادي لهذه الجريمة هو نشاط جرمي يتمثل في الدخول المنطقي أو الاتصال بطريق الغش مع نظام معالجة آلية،[1] بغرض اختراق كله أو جزء منه ومن تم يعد هذا النظام هو المستهدف وهو المحل بالنسبة لهذه الجرائم.

بالرغم أن الدخول إلى النظام المعلوماتي بعد مرحلة سابقة وضرورية لإرتكاب الجرائم المعلوماتية الأخرى، مثل سرقة المعلومات وتزويرها أو التجسس المعلوماتي أو جريمة الإحتيال المعلوماتي أو الإعتداء على حرمة الحياة الخاصة للأفراد وغيرها من

[1] الجريدة الرسمية الجمهورية الجزائرية الديمقراطية، العدد 6 للأمر 04/15 المؤرخ في 10 افريل 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتنسيق الالكتروني.

الجرائم، إلا أن مرتكب هذا الفعل يقصده بهدف أنه دون أن يهدف إلى ارتكاب جريمة أخرى من ورائه[1].

لكن قبل ذلك، هل تعد الحماية الفنية عنصرا في الركن المادي لهذه الجريمة؟ أو بعبارة أخرى هل للأنظمة المعلوماتية التي لا تحميها نظم أمنية، الأحقية بالحماية الجزائية ضد الدخول غير مصرح به.

وهذا ما شكل خلافا بين الفقهاء في الإتجاه المقيد والموسع للحماية الجزائية والإتجاه الذي ذهب إليه الشرع الجزائري هو الإتجاه الموسع حيث أصحابه يرون أن الحماية الجزائية يجب أن تمتد لتغطي كل أنظمة المعالجة الآلية للمعطيات سواء كانت تتمتع بحماية فنية أم لا، حيث أن الشرع الجزائري لم يذكر عنصر الحماية الفنية يعني أن الشرع أراد استبعاده والواقع العلمي يكشف أن غالبية نظم المعالجة الآلية يتمتع بالحماية الفنية على درجة عالية من الكفاءات ، وذلك في ظل تنامي الإعتماد على نظام المعالجة الآلية وهو الرأي الذي أخذه الشرع الفرنسي في عدل أحكام له، من ذلك حكم محكمة استئناف باريس الشهود في 5 أفريل 1994 حيث جاء فيه النص: " من غير الضروري لقيام جريمة الدخول الغير المصرح به أن يكون فعل الدخول قد تم بمخالفة التدابير الأمنية وأنه يكفي أن يكون هذا الدخول قد تم ضد إرادة المسؤول عن النظام".[2]

وبناء على ذلك نتطرق إلى عرض الركن المادي لهذه الجريمة من خلال الفرعين التاليين

الفرع الأول: السلوك

النشاط الجرمي أو السلوك الإجرامي لهذه الجريمة من أهم عناصر الركن المادي، فلا يقوم الركن المادي إذا اختلف هذا السلوك فلا جريمة، إذ القاعدة تقول «لا جريمة

[1] نهلة عبد القادر المومني، مرج السابق، ص 156.

[2] ابو بكر رشيدة، جرائم الاعتداء على نظم المعالجة الالية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية، الطبعة الأولى، سنة 2012، ص 165.

بغير سلوك» والسلوك في جريمة الدخول إلى النظام المعلوماتي سلوك ايجابي يتحقق بفعل الدخول.

وعليه تقتضي دراستنا لسلوك الإجرامي لهذه الجريمة تحديد مفهوم فعل الدخول والدخول الغير مصرح به تحرص له التصريح بالدخول مرورا بتبيان ، صور الدخول إلى النظام المعلوماتي، ووسائل الدخول غير مصرح به.

أولا: فعل الدخول

عرف البعض فعل الدخول في إطار المعلوماتية بأنه: «كل الأفعال التي تسمح بالولوج إلى النظام المعلوماتي والإحاطة أو السيطرة على المعطيات والمعلومات التي يتكون منها».[1]

من خلال هذا التعريف يمكننا القول بأن مجرد الدخول إلى نظام المعالجة الآلية للمعطيات لا يشكل فعلا غير مشروع، وإنما يستمد هذا الدخول عدم مشروعيته من كونه قد تم بغش ويكون كذلك في حالة ما إذا كان ضد إرادة المسؤول عن النظام أي بدون تصريح منه.[2]

ثانيا: الدخول غير المصرح به

تعددت التعريفات بشأن الدخول غير المصرح، حيث عرفه البعض بأنه الولوج غير المصرح به أو بشكل غير مشروع إلى نظام معالجة آلية للبيانات بإستخدام الحاسوب وعرفه البعض الآخر على أنه: "الولوج إلى المعلومات والمعطيات المخزنة داخل نظام الحاسب الآلي بدون رضا المسؤول عن هذا النظام". رغم تعدد التعريفات التي قيلت بشأن الدخول غير المصرح به تدور حول مفهوم واحد هو: الدخول إلى النظام ضد إرادة المسؤول عليه ومن يملك تنظيمه.

---

[1] نهلة عبد القادر المومني، المرج السابق، ص 158.

[2] أبو بكر رشيدة، المرج السابق، ص 176.

فصل الدخول الذي يتشكل الركن المادي لهذه الجريمة لا بقصد بها الدخول المادي الى المكان الذي توجد به الحاسب ونظامه،[1] الأن هذا يمكن تطبيقه بشأن الدخول الى النظام المعالجة الألية بالطريقة ذاتها، بإعتبار هذا النظام ظاهري في مادية وإنما يقصد بالدخول التواجد المعنوي أو المنطقي في نظام المعالجة الألية.

وتقع هذه الجريمة على أي تخص محاكمات صفته، وهذا ما عبر عنه المادة 394 المكرر بقولها: "كل من يدخل ..." وبالتالي لا يشترط فاعلها صفة معينة، فالجريمة تقع على أي شخص محاكمات صفته سواء كان يعمل في مجال الأنظمة أم لا علاقة له بالحاسب الألي وشبكاته وبالتالي بتطبيق عليها الجرائم الشعبية.[2]

ثالثا: من يصرح بالدخول

يسمى صاحب النظام لصاحب السلطة حيث له الأحقية المطلقة في استعمال النظام المعلوماتي واستغلاله والتصرف فيه، حيث لا وجود لنظام دون أن يكون هناك مسؤول عليه، ولا شك أن تحديد الشخص المسؤول عن النظام يسمح بحصر نطاق الأشخاص الذين ينطبق عليهم وصف الدخول غير المصرح به إلى النظام، على اعتبار أن المسؤول عن نظام المعالجة الآلية هو الذي يملك حق الدخول إليه، إلى جانب المرخص له بالدخول، أما ما عدا ذلك فهو غير مرخص له بالدخول.

ثالثا: حالات عدم التصريح بالدخول

يتحقق الدخول غير المصرح به إلى نظام المعالجة الآلية للمعطيات بأحد الأمرين:

أولهما: ألا يكون هناك تصريح بالدخول بتاتا لدى من يقوم بالدخول.

ثانيهما: أن يوجد تصريح بالدخول، ولكن المصرح له بالدخول يقوم بتجاوز الحدود التي رسمت له في هذا التصريح.

---

[1] نهلة عبد القادر المومني، مرجع سابق، ص 158.

[2] رشيدة أبوبكر، مرجع سابق، ص 182.

1- حالة عدم وجود تصريح إطلاقا:

وهي الحالة التي لا يكون فيها للشخص الذي يدخل النظام أي علاقة بهذه الأخيرة، حيث هذه الحالة لا تثير إشكال بحكم نص المادة 394 مكرر من قانون العقوبات الجزائري التي جاءت صيغتها بأنها كامل حالات الدخول غير المصرح به بقولها: «يعاقب ... كل من يدخل» ومنه مجرد عملية الدخول بدون تصريح تتحقق الجريمة.

2- حالة تجاوز التصريح بالدخول:

تثير حالة وجود التصريح إشكال، في هذه الحالة يكون مصرحا بالولوج إلى النظام المعلوماتي في حدود معينة لكن الفاعل يقوم بتجاوز هذه الحدود، والفاعل في أغلب الأحوال يكون من العاملين لدى الجهة التي تم الولوج إلى نظامها الآلي، ويقوم بتجاوز السلطة المخولة له بالدخول إلى هذا النظام في غير الحالات المرخص له فيها بذلك، ويصعب في كثير من الحالات تحديدها إذا كان العامل قد تجاوز اختصاصه بالفعل وما إذا كان قد تجاوزه بقصد أو بغير قصد، لهذا يكون من الواجب تحديد اختصاصات كل عامل بدقة والمجالات التي يمكن لكل واحد الدخول فيها.[1]

حيث أن نص المادة 394 مكرر من قانون العقوبات الجزائري جاء صريح في تجريم الدخول غير المصرح إلى نظام المعالجة الآلية حيث نصت على أن مجرد الدخول عن طريق الغش يشكل جريمة بحد ذاته وليس فيما يحصل بعد هذا الدخول من التزام بالحدود المرسومة في التصريح أو التجاوز.

[1] محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، الإسكندرية، دار الجامعة الجديدة، 2007، ص 149.

رابعا: وسائل الدخول على النظام

تتعدد الوسائل التي يمكن اللجوء إليها للدخول غير المصرح به إلى نظام المعالجة الآلية حيث يتم الدخول بإحدى الوسائل التالية:

1- تشغيل الكمبيوتر مقفل:

هذه الطريقة تتمثل في قيام المتهم بتشغيل جهاز الكمبيوتر وفتحه بعد أن كان مغلقا فإذا بدأ العمل فإن المتهم يعتبر قد دخل إلى النظام دون وجه حق طالما تم ذلك دون موافقة صاحب الحق.

ويرى أن العبرة ليست هي تشغيل الجهاز ولكن بالتمكن من الدخول إلى الملفات إذا قد يتمكن المتهم من الدخول إلى الملفات الموجودة داخل النظام على الرغم من أن الجهاز المغلق كما أنه قد يتمكن من تشغيل الجهاز وذلك بإيصال الكهرباء إليه، دون أن يتمكن من الدخول إلى الملفات[1]، في هذه الحالة يعتبر المتهم قد حاول الدخول إلى الجهاز الذي يحمل النظام ماتعتبره التشريعات متساويا في وقوع الجريمة.فإذا اطلع على المعلومات وهي كانت مفتوحة على الشاشة دون تحريك لوحة المفاتيح لايقع عليه فعل الدخول الغير مشروع.

2- استعمال الكمبيوتر مفتوح:

قد يكون جهاز الكمبيوتر قيد الاستعمال لصاحب السلطة فإذ تغافل عنه أو انشغل وقام شخص آخر باستعماله وذلك بفتح ملفات موجودة فيه فإنه يكون قد دخل في النظام ويقع منه النشاط المعاقب عليه، ويختلف هذا الغرض كما لوكان الكمبيوتر قيد الاستعمال واكتفى المتهم بالنظر إلى الملف الذي كان مفتوحا أمام المستخدم.[2]

ويمكن أن تقوم جريمة الدخول إلى النظام المعلوماتي أيضا بعدة وسائل أخرى نذكر منها:

---

[1] شيماء عبد الغاني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، دار جامعة الجديدة، مصر، 2007، ص 107.

[2] مرجع نفسه، ص 108.

- الدخول إلى كمبيوتر عن طريق استعمال كارت تشغيل ينتمي إلى شخص آخر.
- الدخول إلى كمبيوتر عن طريق خط تلفزيوني.
- الدخول إلى نظام متصل بنفس الكمبيوتر بدائرة واحدة.
- التجسس على النظام بعد اقتحامه.

الفرع الثاني: النتيجة

الشرع الأصل أنه يتطلب لقيام جريمة ما وجود نتيجة الإجرامية التي تأتي من السلوك الإجرامي، لكن هناك جرائم يكتفي فيها بالسلوك الإجرامي لكي يعاقب عليه، وهذه النتيجة في الغالب من الأحيان ما تظهر بصورة أثر مادي ضار، لكن في أحيان أخرى لا تظهر كذلك بل تمثل الاعتداء على حق أو مصلحة يحميها القانون فحسب.

تحمي الجرائم في النوع الأول بالجرائم المادية أو الجرائم ذات النتيجة بينما يحمي النوع التالي بالجرائم الشكلية أو جرائم السلوك.

بالرجوع إلى نص المادة 394 مكرر في فقرتها الأولى في قانون العقوبات الجزائري نجد أنها جرمت الدخول غير مصرح به إلى النظام المعلوماتي، نجد أن الشرع قد عاقب على فعل الدخول دون استخراجها أن يترتب على ذلك تحقيق نتيجة معينة لاكتمال الركن المادي لهذه الجريمة[1].

يستنتج أنه هاته الجريمة تنتمي إلى الجرائم الشكلية، التي لا تتطلب أي جريمة معينة، حيث لجئ الشرع الجزائري إلى تحديد العفوية على الجرائم المترتبة على فعل أو جريمة الدخول غير المشروع نتائج ضارة بالمعلومات أو النظام بصورة مختلفة وذلك وفقا للفقرة الثانية ص المادة 394 مكرر بقوله:" تضاعف العفوية اذا ترتب على ذلك حذف أو تغير للمعطيات المنظومة".

[1] المادة 394، مكرر، ق ع ج.

المطلب الثاني: الركن المعنوي

لوقوع الجريمة قانونيا لا يكفي قيام الركن المادي فقط، بل أن الركن المادي هو ثمرة للإتجاه الإرادي للجاني، فلا بد من علاقة بين الركن المادي والجاني يعبر عنها بالركن المعنوي للجريمة.

تعتبر الجريمة الدخول الغير مشروع من الجرائم العمدية حيث استعمل المشرع في نص المادة 394 مكرر من قانون العقوبات الجزائري بقولها: "كل من يدخل ... عن طريق الغش" التي تتطلب القصد الجنائي.

يتوافر القصد الجنائي العام بعنصر به العلم والإرادة وهذا ما نتطرق إليه خلال الفرع الأول والثاني

الفرع الأول: العلم

هو انصراف علم الجاني إلى واقعه ذات أهمية قانونية تتمثل بعلمه بكافة العناصر التي تشكل الجريمة خاصة ما تعلق منها بأن ليس له الحق في الدخول إلى كل أو جزء من النظام المعالجة الآلية للمعطيات.[1]

وأول ما يجب أن ينصرف إليه علمه هو موضوع الحق المتعدي عليه ،فعلى الجاني فلابد أن يعلم الجاني أن فعله بنصب على نظام المعالجة الآلية للبيانات وليس على شيء آخر، وكذلك أنه يقوم بالدخول إلى هذا النظام من غير تصريح أي بصفة غير مشروعة فإذا كان يعتقد أن له تصريحا بالدخول.

وفضلا على ذلك لابد أن يعلم الجاني بخطورة الفعل الذي يقوم به على المصلحة التي يحميها القانون، كأن يعلم أنه ينتهك سرية هذا النظام وأن فعله قد يؤدي إلى تخريب هذا النظام، أو الاضرار بالبيانات الموجودة فيه، وهناك بعض العناصر لا يتطلب القانون

[1] حديدان سفيان، الدخول أو البقاء في النظام المعالجة الآلية للمعطيات، مجلة الباحث للدراسات القانونية والسياسية جامعة المسيلة، المجلد 05، العدد 04، ديسمبر، 2017، ص 676.

توقفها لتقوم الجريمة، فالقانون لا يحدد في حمايته نظاما بعينه فإذا قصد الجاني الدخول إلى نظام معين فوجد نفسه في نظام آخر فإن الجريمة تتحقق[1] والقصد الجنائي يتحقق.

الفرع الثاني: الإرادة

أن تتجه إرادة الجاني إلى فعل الدخول وإرتكاب الفعل وهو الدخول إلى النظام المعالجة الآلية بدون تصريح وطالما أن جريمة الدخول غير المصرح به إلى النظام المعالجة الآلية للمعطيات هي جريمة شكلية في التشريع الجزائري لا تتطلب بقيامها تحقيق نتيجة معينة فإن الإرادة فيها تقتصر على إثبات سلوك إجرامي واستغراقه بكل مقوماته ولا تمتد إلى أي نتيجة لأن هذه الأخيرة لا يعد بها القانون في قيام الجريمة[2].

المبحث الثاني: العقوبات المقررة لجريمة الدخول

نص الشرع الجزائري على جملة من العقوبات الخاصة بالجرائم المعلوماتية أو جرائم المساس بأنظمة المعالجة الآلية للمعطيات، منها عقوبات أصلية وأخرى تكملية الواردة في قانون العقوبات الجزائري، ص المادة 394 مكرر إلى غاية المادة 394 مكرر 7 نجد أن المشرع سن عقوبات على الشخص الطبيعي وعقوبات تطبق على الشخص المعنوي وما سنوضح من خلال دراستنا في المطلب الأول للعقوبات المقررة للشخص الطبيعي والمطلب الثاني بالعقوبات المطبقة على الشخص المعنوي.

المطلب الأول: العقوبات المطبقة على الشخص الطبيعي

أورد المشرع الجزائري جملة من العقوبات أو الجزاءات على الشخص الطبيعي منها العقوبات الأصلية والأخري التكميلية وهي كالآتي:

---

[1] عبير علي حسين الورقلي، مقال بعنوان جرائم تجسس الالكتروني للمعلومات الشخصية في اطار اتفاقية بودا بست بشأن الجريمة الالكترونية، مجلة أبحاث كلية الأدب جامعة سرت، ليبيا، مجلد 15، العدد 1، مارس 2021، ص 143.

[2] الطيبي البركه، الحماية الجنائية لنظام المعالجة الالية للمعطيات، دراسة مقارنة، مذكرة لنيل شهادة دكتوراه، جامعة أحمد دراية، أدرار، قسم الحقوق، سنة 2021، ص 169.

الفرع الأول: العقوبات الأصلية المطبقة على كل جريمة من جرائم المعطيات

من خلال استقراء هذه النصوص المتعلقة بالجرائم الماسة بالأنظمة المعلوماتية يبين لنا وجود تدرج داخل النظام العقابي. هذا التدرج في العقوبات يحدد الخطورة الاجرامية التي قدرها الشرع لهذه التصرفات اذ نجد سلم الخطورة يتضمن ثلاثة درجات جريمة الدخول أو البقاء بالغش في الدرجة الأولى، وبعدها الدرجة الثانية جريمة الدخول والبقاء المشددة، أما الدرجة الثالثة فتحتلها الجريمة الخاصة بالمساس العمدي بالمعطيات.[1]

أولا: جريمة الدخول والبقاء

نص الشرع الجزائري من خلال نص المادة 394 مكرر ص ق.ع.ج على عقوبة هذه الجريمة في صورتها البسيطة والمشددة.

أ- الدخول والبقاء بالغش(الجريمة البسيطة):

يعاقب الشرع الجزائري في نص المادة سابقة الذكر بثلاثة(3)أشهر إلى ستة حبس وبغرامة من 50,000دج إلى 100،000دج غرامة(المادة 394 مكرر).

ب- الدخول والبقاء بالغش(الجريمة المشددة):

تضاعف العقوبة اذا ترتب عن هذه الأفعال حذف أو تغير لمعطيات العقوبة من 06 أشهر إلى سنتين (2) وغرامة من 50،000دج إلى 150,000دج اذا ترتب عن الدخول والبقاء غير الشروع تخريب لنظام استفعال المنظومة المعلوماتية (المادة 394 مكرر 02,03).

[1] أمال قارة، الحماية الجزائية للمعلومات في التشريع الجزائري، دار مومة، للطباعة والنشر والتوزيع، الجزائر، الطبعة الأولى، 2007، ص 127.

ثانيا: جريمة التلاعب بالمعطيات

نصت المادة 394 مكرر 1 ق.ع.ج عليها وأتت عقوبتها بالحبس 6 أشهر إلى 3 سنوات وغرامة من 500,000دج إلى 2,000,000دج، الملاحظ أن عقوبة التلاعب بالمعطيات تفوق الدخول والبقاء غير المصرح بهما سواء كانت في صورتهما البسيطة أو المشددة، لأن في صورتهما البسيطة لا تؤدي إلى أضرار معينة تلحق بالمعطيات أو بنظام معالجتها وحتى في صورتها المشددة، وإن أدت إلى نفس النتائج التي تؤدي إليها جريمة التلاعب بالمعطيات، وهي إزالة المعطيات أو تعديلها، فإن العقوبة المقررة لجريمة التلاعب تبقى أكبر لأنها جريمة عمدية يتوافر لدى مرتكبها القصد الجنائي بينما لا يتوافر هذا القصد لدى مرتكب جريمة الدخول أو البقاء المشددة.[1]

ثالثا: جريمة التعامل بالمعطيات غير المشروعة

تعاقب المادة 394 مكرر 2 من ق.ع.ج على جريمة التعامل في معطيات غير مشروعة بعقوبة الحبس من شهرين إلى 3 سنوات وبالغرامة المالية من ,1,000,000دج إلى 5,000,000دج.

بهذا يكون ترتيب هذه الجريمة من حيث عقوبة الحبس هو الثاني بين جريمتين الدخول والبقاء غير مصرح بهما سواء في صورتهما البسيطة أو المشددة وبين جريمة التلاعب بالمعطيات (غير أن حدها الأدنى يقل عن كلتا الجريمتين).

ذلك أن حدها الأقصى يزيد عن الحد الأقصى لجريمة الدخول أو البقاء في صورتهما(سنة أو سنتين) وستتساوى مع الحد الأقصى لجريمة التلاعب بالمعطيات (3) سنوات.

[1] د/ ناتلة محمد فريد قورة، مرجع سابق، ص 228.

غير أن حدها الأدنى يقل عن الجريمتين معا، لأنه في جريمة الدخول أو البقاء البسيطة 3 أشهر وفي هذه الجريمة في صورتها المشددة وفي جريمة التلاعب هو 6 أشهر.[1]

الفرع الثاني: العقوبات التكملية

نصت المادة 394 مكرر 06 من قانون العقوبات الجزائري، على العقوبات التكملية التي يمكن الحكم بها إلى جانب العقوبات الأصلية وجاء فيها مع الاحتفاظ بحقوق الغير حسن النية، يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق الموقع التي تكون محلا للجريمة من الجرائم المعاقب عليها في هذا القسم، علاوة على إغلاق المحل أو مكان الاستعمال اذا كانت الجريمة قد ارتكبت بعلم مالكها ويستخلص من نص هذه المادة العقوبات التكميلية التالية:

أولا: المصادرة

عرفتها المادة 15 في فقرتها الاولى من قانون العقوبات الجزائري على أنها الأيلولة النهائية إلى الدولة لمال أو مجموعة أموال معينة أو ما يعادل قيمتها عند الاقتضاء.

مع الاحتفاظ بحقوق الغير حسن النية، تجدر الاشارة إلى أن الشرع نص فقط على مصادرة الأجهزة والبرامج والوسائل المستخدمة فقط، وأغفل مصادرة الوسائل الموجهة لارتكاب الجريمة من المعطيات المخزنة أو المعالجة أو المراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها جرائم المساس بأنظمة المعالجة الآلية للمعطيات المنصوص عليها في الفقرة الأولى من المادة 394 مكرر 2 قانون العقوبات الجزائري، حيث أن عبارة "المستخدمة" الواردة في نص المادة 394 مكرر 6 الخاصة بالعقوبات التكميلية تفيد صيغة الماضي وهذا ما نصت عليه المادة 394 مكرر 6 من القانون عقوبات الجزائري التي تنص على العقوبات التكميلية، وفي فقرتها الثالثة علي المصادرة

[1] محمد خليفة، مرجع سابق ص 219.

الشيء الذكي كان موجها للقيام، وبذلك تكون المصادرة بالنسبة لهذه الجرائم عقوبة وجوبية.

ثانيا: إغلاق المواقع

يقصد به إغلاق المواقع التي تكون محلا للجريمة من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.[1]

ثالثا: إغلاق المحل أو مكان الاستغلال

شرط أن تكون الجريمة قد ارتكبت بعلم مالك المكان الذي سمح من خلاله بالدخول غير مصرح به لمختلف الأنظمة وسمح بالتلاعب بالمعطيات، اذا كان على سبيل المثال الجاني مستأجر للمحل والمالك المؤجر له يعلم بالخطورة التي يقوم بها الجاني، كغلق نادي الأنترنت الذي ترتكب فيه هذه الجرائم مع علم مالك أو مسير النادي بالأفعال الخطيرة التي يقوم بها زبونه.

بالنسبة لمدة الغلق لم يحددها الشرع الجزائري في نص المادة 394 مكرر 6 من ق.ع.ج، مما يطرح اشكال في المدة القصوى لغلق المحل أو مكان الاستغلال، وفي تنفيذ هذه العقوبة فمن جهة يعتبر الإغلاق المحل أو مكان الاستغلال كعقوبة تكميلية للشخص الطبيعي المسؤول جزائيا، ومن جهة أخرى لا يمكننا الرجوع إلى القواعد العامة للمسؤولية الجزائية للشخص المعنوي لتحديد المدى "المدة "، لأنه في هذه الحالة تقع المسؤولية الجزائية على عاتق الشخص الطبيعي، حيث يتم توقيع جزاء خاص بالشخص المعنوي غلق المحل على الشخص الطبيعي، بحيث يمكن أن تكون المدة مؤقتة أم مؤبدة الغلق.

– إن العقوبة التكميلية الورادة في المادة 394مكرر 06،ق،ع،ح،غير كافية في مواجهة العديد من الحالات التي يرتكبها الشخص الطبيعي، مثلا تنص المادة على العفوية

[1] أحسن بوسقيعة، الوجيز في القانون الجزائري الخاص، الجزء الأول، دار هومة، الجزائر، الطبعة 9، 2008، ص 448.

التكميلية الخاصة بالموظف العمومي المصرح به بالدخول إلى النظام الآلي للمعطيات لكنه يبتعد ذلك إلى ارتكاب جرائم أخرى متعلقة بالمنظومة المعالجة آليا.

كذلك بالنسبة للوظيفة المهنية، كالأطباء والمحامين مثلا، وكذا الوظيفة الإجتماعية إذا ارتكبت الجريمة عند تأدية الوظيفة أو بمناسبتها وماذا ما جاءت به أحكام المادة 323-05 من قانون العقوبات الفرنسي التي نصت على تكميلات أخرى كالآتي:

- المنع لمدة أقصاها 5سنوات من الحقوق السياسية والمدنية.
- المنع لمدة أقصاها 5 سنوات من ممارسة الوظيفية العمومية أو النشاط المهني أو الاجتماعي إذا ارتكبت الجريمة أثناء تأدية الوظيفة أو بمناسبتها.
- مصادرة الشيء الذي استخدم أو الموجه لارتكاب الجريمة أو التي محل الجريمة الغلق لمدة أقصاها 5سنوات للمؤسسات، أو للأحد او عدة مؤسسات المقاولة التي استعملت في ارتكابها الأفعال الإجرامية.
- الحرمان لمدة أقصاها 5سنوات من الصفقات العمومية.
- المنع لمدة أقصاها خمس سنوات في إصدار الشيكات، بما فيها التي تسمح بسحب الاموال من طرف الساحب لدى المسحوب له أو المرخص أو المرخص لهم بذلك، تقليل او نشر القرار الصادر.[1]

الفرع الثالث: العقوبات المشددة

نصت المادة 394 مكرر 2و3 على الظروف المشددة على عقوبة جريمة الدخول والبقاء الغير مصرح به داخل النظام المعلوماتي ويتحقق هذا الظرف عندما ينتج عن الدخول والبقاء إما حذف أو تغيير المعطيات التي يحتويها النظام وإما تخريب نظام اشتغال المنظومة.

– في الحالة الأولى تضاعف العقوبة المقررة في الفقرة الأولى في المادة 394مكرر.

– في الحالة الثانية تكون العقوبة الحبس من (6) ستة أشهر إلى (2) سنتين وبغرامة من 50.000غلى 150.000 دج، هذا الظرف المشدد هو ظرف مادي يكفي أن تقوم بينه

[1] أحسن بوسقيعة، المرج السابق، ص 449.

وبين الجريمة الأساسية وهي جريمة الدخول غير مشروع إلى النظام المعلوماتي علاقة سببية للقول بتوافره.

نصت المادة 394 مكرر على ان تضاعف العقوبات المقررة للجرائم الماسة بالأنظمة المعلوماتية وذلك اذا استهدفت الجريمة الدفاع الوطني أو الهياءات أو المؤسسات الخاضعة للقانون العام.[1]

المطلب الثاني: العقوبات المطبقة على الشخص المعنوي في الجرائم المعلوماتية

ورد مبدأ مساءلة الشخص المعنوي في المادة 12 من اتفاقية الدول للإجرام المعلوماتي بحيث يسأل الشخص المعنوي عن هذه الجرائم سواء كان بصفته الفاعل الأصلي أو الشريك أو متدخلا كما يسأل عن الجريمة التامة والشروع فيها، شرط أن تكون الجريمة قد ارتكبت لصالح الشخص المعنوي بواسطة أحد أعضاءه أو ممثليه.

الفرع الأول: عقوبات المقررة للشخص المعنوي

تضمنت المادة 8 مكرر من قانون العقوبات الجزائري بعد تعديله سنة 2004، أنواع العقوبات المطبقة على الشخص المعنوي في مواد الجنايات والجنح، وأول ضده العقوبات في الغرامة التي تساوي من مرة إلى خمس مرات الحد الأقصى المقررة على الشخص الطبيعي، وكذلك بواحدة أو أكثر من العقوبات الآتية كما نصت عليها المادة 18 مكرر:

- حل الشخص المعنوي.
- غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز خمس (5) سنوات.
- الإقصاء من الصفقات العمومية لمدة لا تتجاوز خمس (5) سنوات.
- المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر نهائيا أو لمدة لا تتجاوز خمس سنوات.

[1] المادة 394 مكرر 3، قانون العقوبات الجزائري.

– مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها .

– نشر أو تعليق الإدانة.

– الوضع تحت حراسة القضائية لمدة لا تتجاوز خمس (5) سنوات، وتنصب الحراسة على ممارسة النشاط الذي أدى إلى ارتكاب الجريمة بمناسبتها.

أما بالنسبة لعقوبات الغرامة المطبقة على الشخص المعنوي عن ارتكابه أحد الجرائم الماسة بالأنظمة المعلوماتية فهي تعادل طبقا للمادة 394مكرر 4 قانون العقوبات (5) خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.

الفرع الثاني: عقوبة الإنفاق والشروع الجنائي

نصت المادة 11من الإتفاقية الدولية للإجرام المعلوماتي على تحريم التحضير للجرائم الماسة بالأنظمة المعلوماتية، وقد تبنى الشرع الجزائري مبدأ معاقبة الإتفاقية الجنائي بنص المادة 394 مكرر 05 من ق ،ع، ج إذا جاء فيها أن" كل من شارك في مجموعة اوفي اتفاق تالف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية يعاقب بالعقوبات المقررة للجريمة ذاتها".

إن الحكمة التي ارتأها المشرع الجزائري من تحريم الإشتراك في مجموعة او اتفاق بغرض الإعداد لجريمة من الجرائم الماسة بالأنظمة المعلوماتية ، يتمثل في كون أن مثل هذه الجرائم تم عادة في إطار مجموعة ، كما أن المشرع أراد توسيع نطاق العقوبة فأخضع الأعمال التحضيرية للعقوبة المقررة للجريمة التي تم التحضير لها إذا نصت في إطار اتفاق جنائي، بمعنى آخر أن الأعمال التحضيرية المرتكبة من طرف شخص منفرد غير مشمولة بالنص".[1]

[1] أمال قارة، مرجع سابق، ص 132.

ويعاقب الشرع الجزائري على الاشتراك في الاتفاق الجنائي بعقوبة الجريمة التي تم التحضير لها فبعقوبة الجريمة التي تم التحضير لها فإذا انعقدت الجرائم التي تم التحضير لها تكون العقوبة من عقوبة الجريمة الأشخاص وشروط المعاقبة على الإتفاق الجنائي يمكن استخلاصها من نص المادة 394 مكرر 5 أما الشروع قد نصت عليه المادة 394 مكرر 7 بقولها:" يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها".

يبدو من خلال هذه النصوص رغبة المشرع في توسيع نطاق العقوبة لتشتمل أكبر قدر من الأفعال الماسة بالأنظمة المعلوماتية ، اذا جعل الشروع في إحدى الجرائم الماسة بالأنظمة المعلوماتية معاقب عليه بنفس عقوبة الجريمة التامة.

ومن خلال استقراء نص المادة 394مكرر(5) فإن الجنحة الواردة مشمولة بهذا النص، أي أن الشرع الجزائري بهذا المنطق يكون قد تبنى فكرة الشروع في اتفاق الجنائي.[1]

[1] أمال قارة، مرجع سابق، ص 133.

الخاتمة

استخدام النظام المعلوماتي ينطوي على مخاطر لا يستهان بها فقط ابرزت هذه المخاطر الوجه الثاني للثورة المعلوماتية، التي اظهرت انواع جديدة وحديثة من النشاط الاجرامي ،ولعل اخطر هذه الجرائم جريمة الدخول غير المصرح به الى النظام المعلوماتي باعتبارها الشرارة الاولى او بوابة لارتكاب باقي الجرائم المعلوماتية.

جريمة الدخول من الجرائم المعلوماتية الغير مصرح بها التي تقع على انظمة المعالجة الالية للمعطيات، اي قيام الجاني بالولوج والاطلاع او التجسس على المعطيات داخل النظام المعلوماتي، حيث يقوم بالاعتماد على المعطيات المخزنة دون اي تصريح او ترخيص بالدخول الى النظام المعلوماتي، كما يمكنها ان تقوم هذه الجريمة بوجود تصريح بالدخول لان المجرم يقوم بتعدي حدود التصريح الذي قدم له.

هذا ما يستدعي المشرع الجزائري الى تجريم هذا الفعل وهذا ما تبينه نصوص المواد المستعان بها المتمثلة في الركن الشرعي لهاته الجريمة, وجريمة الدخول كغيرها من الجرائم لابد من قيام الركن المفترض وعنصر العلم لدى الجاني.

انطلاقا من ذلك يتضح ان جريمة الدخول صورة من صور الجرائم، حيث تعد هذه الجريمة عابرة للحدود حيث حصلت على ارتكاب العديد من الجرائم على تفاقم المخاطر في البيئة الرقمية التي تمس سلامة الافراد والدول ولنتمكن مكافحة هذه الجرائم المعلوماتية.

وقد توصلنا إلى الإقتراحات التالية:

الإقراحات:

1. استغلال الاجهزة المعنية لمواجهة ومكافحة هاته الجرائم من شرطة او اجهزة فضاء وتطويرهم واعادة برمجتهم تماشيا للتطورات الحاصلة في مجال مكافحة الجرائم.
2. زيادة الوعي لدى المواطنين وبوجود مثل هذه الجرائم والحرص على حماية معلوماتهم.
3. القضاء الجزائري في وضع قوانين جديدة تتماشى مع هذه التطورات الاجرامية.

4. ضرورة التعاون الدولي لمكافخة هذه الجرائم في البيئة المعلوماتية من خلال الدخول في معاهدات واتفاقيات دولية، كما تنص هذه الاتفاقيات على تبادل الخيرات والمعلومات والوسائل المتعلقة بهذه الجرائم.

قائمة المصادر والمراجع

- **المراجع باللغة العربية:**

أولا: المصادر

1. الأوامر والقوانين:

- القانون 22/06، المؤرخ 20 ديسمبر 2006، يعدل ويتمم الأمر رقم 66-155 المؤرخ في 8 يونيو سنة 1966 والمتضمن قانون الاجراءات الجزائية.
- قانون 09-04 المؤرخ في 05 أوت 2009، الجريدة الرسمية، العدد 47، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة لتكنولوجيا الإعلام والإتصال ومكافحتها الصادرة 16 أوت.
- المادة 394 من قانون العقوبات الجزائري المعدل والمتمم بموجب القانون 15/04 المؤرخ في 10-11 – 2004.

2- الجرائد الرسمية:

- الجريدة الرسمية للجمهورية الجزائرية الشعبية الديمقراطية، عدد 47، 25 شعبان 1430هـ، 16 أوت 2009.
- الجريدة الرسمية الجمهورية الجزائرية الديمقراطية، العدد 6 للأمر 04/15 المؤرخ في 10 افريل 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتنسيق الالكتروني.

ثانيا: المراجع

1- الكتب:

- ابو بكر رشيدة، جرائم الاعتداء على نظم المعالجة الالية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية، الطبعة الأولى، سنة 2012.
- أحسن بوسقيعة، الوجيز في القانون الجزائري الخاص، الجزء الأول، دار هومة، الجزائر، الطبعة 9، 2008.
- أمال قارة، الحماية الجزائية للمعلومات في التشريع الجزائري، دار مومة، للطباعة والنشر والتوزيع، الجزائر، الطبعة الأولى، 2007.

- أيمن عبد الحفيظ ، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، دون دار نشر، سنة 2004.
- بوضياف إسمهان، الجريمة الالكترونية والاجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية السياسية، العدد 11، الجزائر، 2018.
- حسين طاهر داود، جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية، الرياض، الطلعة الأولى،2000.
- حنان ريحان المبارك المضاحكي، الجرائم المعلوماتية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2014.
- خاد ممدوح إبراهيم، امن الجريمة الالكترونية، دار الجامعية، اسكندرية، 2010.
- خالد بن عبد الله بنو معييض العابدي، الحماية الجنائية للتعاملات الالكترونية، في نظام المملكة العربية السعودية، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، قسم العدالة الجنائية، الرياض، 2009.
- خالد ممدوح ابراهيم، من الجريمة الالكترونية, الدار الجامعية مصر, 2008.
- رشيدة بوبكر، جرائم الإعتداء على نظام المعالجة الآلية في التشريع الجزائري المقارن، الطبعة الأولى، منشورات حلبي الحقوقية، بيروت، لبنان، سنة 2012، ص 282-283.
- سامس علي عياد، الجريمة المعلوماتية والانترنت (الجرائم الالكترونية)، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2007.
- شيماء عبد الغاني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، دار جامعة الجديدة، مصر، 2007.
- عابد راجا الخلايا، المسؤولية التقصيرية الإلكترونية، المسؤولية الناشئة عن إستخدام أجهزة الحاسوب والأنترنت، دراسة مقارنة، طبعة 1، دار الثقافة، عمان، 2009.
- عبد الفاتح اليومي الحجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، الاسكندرية، الطبعة الأولى، سنة 2006.

- عبد الكريم خالد الشامي، جرائم الكمبيوتر والانترنت في التشريع الفلسطيني، ص 19، مثال متوفر على بوابة فلسطين القانونيةhttp:// www.pal-ip.org
- عبد الله بنو عبد العزيز اليوسف، أساليب تطور البرامج والمناهج التدريبية لمواجهة الجرائم المستحدثة، جامعة نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، 2004.
- علي عدنان الفيل، الإجرام الالكتروني، الطبعة الأولى، منشورات زين الحقوقية، دمشق، 2011.
- عمرو موسى الفقهي، الجرائم المعلوماتية، جرائم الحاسب الآلي والنترنت في مصر والدول العربية، المكتب الجامعي الحديث، الاسكندرية، 2006.
- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، الإسكندرية، دار الجامعة الجديدة، 2007.
- محمد دباس الحميد، ماركو إبراهيم، حماية الأنظمة المعلوماتية، دار حامد للنشر والتوزيع، عمان، الطبعة الأولى، 2007.
- محمد زيدان، محمد جمو، "متطلبات أمن المعلومات المصرفية في بيئة الأنترنت"، المؤتمر السادس لجمعيات المكتبات المعلومات السعودية، المعلومات الأمنية والتشريعات والتطبيقات، 6-7 أفريل 2010، الرياض.
- محمد سامي الشوا ثورة المعلومات وإنعكاساتها على قانون العقوبات، دون طبعة، دار النهضة العربية، القاهرة، سنة 1994.
- محمد سلطان، قضايا قانونية وحماية البيئة الالكترونية، دار ناشري للنشر والتوزيع الالكتروني، 2004.
- محمد عابيد الكعبي، الجرائم الناشئة عن إستخدام الغير المشروغ لشبكة الانترنت، دار النهضة العربية، القاهرة، بدون سنة.

- محمد عبد الرحبم سلطان علماء، "جرائم الانترنت"، مؤتمر القانون الكمبيوتر والانترنت، المنعقد من 1-3 ماي 2000، بجامعة الامارات كلية الترقية والقانون، الجلد 3، الطبعة الثالثة، 2004.
- نايف بن محمد الماروني، جريمة السرقة (دراسة نقدية إجتماعية)، جامعة نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى.
- نائلة محمد فريد قورة، جرائم الحاسب الآلي الإقتصادية، منشورات الحلبي الطبعة الأولى، القاهرة، 2005.
- نهلة عبد القادر المومني، الجرائم المعلوماتية، الطبعة الثانية، 2010، دار الثقافة، عمان، ص 57-58.
- هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، الطبعة الأولى ،1994.
- يعيش تمام شوقي، الجريمة المعلوماتية، دراسة تأصيلية مقارنة، مخبر أثر الإجتهاد القضائي حركة التشريع، جامعة محمد خيضر، بسكرة.

2- المذكرات:

- الرسائل الجامعية:

- عامر محمد الحبيب عبد القادر، المجرم المعلوماتي، مذكرة لنيل شهادة ماستر تخصص قانون جنائي، جامعة عبد الحميد ابن بديس، 2019.

- مذكرات ماجيستير:

- إبتسام ميهوب، جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري، مذكرة لنيل شهادة ماجيستر، كلية الحقوق، جامعة العربي بن المهيدي أم البواقي، 2014.
- سعيداني نعيم، آلية البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة بحث لنيل شهادة ماجيستير، جامعة الحاج لخضر، باتنة.

- صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة ماجيستير في القانون الدولي للأعمال، كلية الحقوق، جامعة مولود معمري، تيزي وزو، 2014.
- عبد اللطيف معتوف، الإطار القانوني لمكافحة الجرائم المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماجيستر في العلوم القانونية، جامعة العقيد لخضر، باتنة، 2012.

- أطروحات دكتورة:

- الطيبي البركه، الحماية الجنائية لنظام المعالجة الالية للمعطيات، دراسة مقارنة، مذكرة لنيل شهادة دكتوراه، جامعة أحمد دراية، أدرار، قسم الحقوق، سنة 2021.

3- المجلات:

- أ، د، النحوي سليمان، طبيعة الخطورة الإجرامية للمجرب المعلوماتي، مجلة الإشراف الباحث في الدراسات القانونية والسياسية، جامعة محمد ثليجي الأغواط، المجلد 05، العدد 01، سنة 2020,
- بردال سمر، الجريمة المعلوماتية في التشريع الجزائري، مجلة القانون، المركز الجامعي غليزان، العدد 2، جويلية 2010.
- حديدان سفيان، مقال بعنوان الدخول أو البقاء في النظام المعالجة الآلية للمعطيات، مجلة الباحث للدراسات القانونية والسياسية جامعة المسيلة، المجلد 05، العدد 04، ديسمبر، 2017.
- ربيعي حسين، الجرم المعلوماتي شخصية وأصنافه، مجلة العلوم الإنسانية، جامعة محمد حنيفي، بسكرة، العدد 40، جوان 2015.
- ربيعي حسين، المجرم المعلوماتي – شخصيته وأصنافه، مجلة العلوم الإنسانية، جامعة خيضر، بسكرة، العدد 40، جوان 2015.
- عبير علي حسين الورقلي، مقال بعنوان جرائم تجسس الالكتروني للمعلومات الشخصية في اطار اتفاقية بودا بست بشأن الجريمة الالكترونية، مجلة أبحاث كلية الأدب جامعة سرت، ليبيا، مجلد 15، العدد 1، مارس 2021.

- غريبي بشرى، خصوصية المجرم المعلوماتي ودوافعه، مجلة نموديا الأكاديمية، المجلد 02، العدد 02، 2021.
- محمد عبد المحسن بن طريف، جريمة السرقة المعلوماتية، مجلة الدراسات والبحوث القانونية، المجلد 7، العدد 2، 2022، جامعة عمان العربية، الأردن.
- مصور فهيد سعيد الحارثي، معوقات إثبات الجرائم المتعلقة لتقنية المعلومات، المجلة القانونية، القاهرة، المجلد 15، العدد 04، فبراير 2023.

- **المراجع باللغة الأجنبية:**

- Marwe Vander , computer crime and other grimes against information technologies in south Africa, « R.I.D.P ».1993.

فهرس المحتويات

فهرس المحتويات:.....

الإهداء:

شكر وعرفان:

مقدمة: 05

الفصل الأول: الإطار الموضوعي لجريمة الدخول إلى النظام المعلوماتي 07

المبحث الاول: مفهوم الجريمة المعلوماتية 08

المطلب الاول: تعريف الجريمة المعلوماتية 08

الفرع الاول: التعريف الضيق للجريمة المعلوماتية 08

الفرع الثاني: التعريف الموسع للجريمة المعلوماتية 09

الفرع الثالث: التعريف التشريعي للجريمة المعلوماتية 10

المطلب الثاني: تصنيف الجرائم المعلوماتية 11

الفرع الأول: خصوصية الجريمة المعلوماتية 12

الفرع الثاني: سمات المجرم المعلوماتي 14

الفرع الثالث: تصنيف المجرم المعلوماتي 18

المبحث الثاني: أنواع الجرائم المعلوماتية 21

المطلب الأول: جرائم واقعة على النظام المعلوماتي 22

الفرع الأول: الجرائم الواقعة على نظام المعالجة الآلية للمعطيات 22

الفرع الثاني: الجرائم الواقعة على المعلومات داخل أنظمة المعالجة الآلية للمعطيات 26

المطلب الثاني: الجرائم التي تتم عن طريق النظام المعلوماتي 27

الفرع الأول: الجرائم الواقعة على أشخاص 27

الفرع الثاني: الجرائم الواقعة على الأموال 30

الفرع الثالث: الجرائم الواقعة على أمن الدولة 32

الفصل الثاني: الإطار الإجرائي لجريمة الدخول إلى النظام المعلوماتي 36

المبحث الأول: أركان جريمة الدخول إلى النظام المعلوماتي 37

المطلب الأول: الركن المادي لجريمة الدخول 37
الفرع الأول: السلوك 38
الفرع الثاني: النتيجة 43
الفرع الأول: العلم 44
المطلب الثاني: الركن المعنوي 44
الفرع الثاني: الإرادة 45
المبحث الثاني: العقوبات المقررة لجريمة الدخول 45
المطلب الأول: العقوبات المطبقة على الشخص الطبيعي 45
الفرع الأول: العقوبات الأصلية المطبقة على كل جريمة من جرائم المعطيات 46
الفرع الثاني: العقوبات التكملية 48
الفرع الثالث: العقوبات المشددة 49
المطلب الثاني: العقوبات المطبقة على الشخص المعنوي في الجرائم المعلوماتية 51
الفرع الأول: عقوبات المقررة للشخص المعنوي 51
الفرع الثاني: عقوبة الإنفاق والشروع الجنائي 52
خاتمة: 55
قائمة المصادر والمراجع: 58

الملخص:

الدخول الغير مشروع لنظام المعالجة الالية للمعطيات، جريمة نص عليها المشرع الجزائري ولحقها بدراسات ضمن تعديل قانون العقوبات لسنة 2004، ظهر مصطلح الجرائم المساس بالمعالجة الالية للمعطيات في لغة القانون نتيجة تطور العالم الافتراضي، هذه الجريمة تخضع الي نظام قانوني خاص وأي خرق له وبأي صفة كانت قد ينتج عنه ضرر للغير سواء كان الدخول في نظام المعالجة الآلية للمعطيات عن طريق الصدفة، ويتعدد الضرر ما بين المساس بالحياة الخاصة للأفراد إلى زعزعة الأمن القومي، حيث أن هذه الجريمة هي بوابة الجرائم المعلوماتية وتختلف العقوبة بالنظر إلى مرتكب الجريمة سواء كان شخصا طبيعيا أو معنويا.

كلمات المفتاحية:

1/الجريمة المعلوماتية 2/ المعالجة الآلية للمعطيات 3/ جريمة الدخول الغير المشروع

Résumé:

L'accès illégal au système de traitement automatisé des données, délit prévu par le législateur algérien et suivi d'études dans le cadre de l'amendement du Code pénal de 2004, le terme délits contre l'informatique est apparu dans le langage de la loi à la suite de la développement du monde virtuel, ce délit est soumis à un régime juridique particulier et toute violation de celui-ci et à quelque titre vie privée des individus à porter atteinte à la sécurité nationale, car ce délit est la porte d'entrée des délits d'information et la sanction diffère selon l'auteur du délit, qu'il soit une personne physique ou morale.

Mots clés:

1/ cybercriminalité 2/ Traitement automatisé des données 3/ la crime d'entrée illégale

ملحق بالقرار رقم ....1082.... المؤرخ في 27 ديسمبر 2020 .....

الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

1

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي

الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

أنا الممضي أسفله،

السيد(ة): داود ادريس الصفة: طالب، أستاذ، باحث طالب

الحامل(ة) لبطاقة التعريف الوطنية رقم 199811604405 والصادرة بتاريخ 05-12-2022

المسجل(ة) بكلية / معهد: الحقوق والعلوم السياسية قسم: إعلام آلي وانترنت

والمكلف(ة) بإنجاز أعمال بحث (مذكرة التخرج، مذكرة ماستر، مذكرة ماجستير، أطروحة دكتوراه).

عنوانها: مذكرة ماستر تحت عنوان "جريمة الدخول إلى النظام المعلوماتي في القانون الجزائري"

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

التاريخ: 14/06/2023

توقيع السيد: المعني

بطاقة التعريف رقم: 403855443

بتاريخ: 05/12/2022

توقيع المعني (ة)

مصادق عليه

برج بوعريريج، في: 14 جوان 2023

رئيس المجلس الشعبي البلدي

عن رئيس المجلس الشعبي البلدي

مفوض الحالة المدنية

بودشيشة نوال

* ملحق بالقرار رقم ...1082... المؤرخ في ...27 ديسمبر 2020...
الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

1

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي
الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

أنا الممضي أسفله،

السيد(ة): ...بن شيباني أسيا... الصفة: طالب، أستاذ، باحث ...طالب...

الحامل(ة) لبطاقة التعريف الوطنية رقم ...104690018... والصادرة بتاريخ ...2023-02-13...

المسجل(ة) بكلية / معهد ...العلوم السياسية... قسم ...السنة الثالثة ماستر تخصص علاقات دولية وتنمية...

والمكلف(ة) بإنجاز أعمال بحث (مذكرة التخرج، مذكرة ماستر، مذكرة ماجستير، أطروحة دكتوراه).

عنوانها: ...حق العودة للاجئين في ظل النظام العالمي الجديد...

...

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

التاريخ: 14 جوان 2023

توقيع المعني (ة)

توقيع المعني
بطاقة التعريف رقم 104690018
بتاريخ: 2023/02/13
مصادقة عليها

حرر بوهران في 14 جوان 2023

عن رئيس المجلس الشعبي البلدي
ملحق إداري للأمانة الإقليمية
زهار خليفة