جامعة عمارثليجي - الأغواط
كلية الحقوق والعلوم السياسية
قسم: الحقوق

عنوان المذكرة:

القانون كوسيلة للوقاية من جرائم المعلومات ومكافحتها

مذكرة مكملة لنيل شهادة الماستر حقوق تخصص: قانون أعمال

من إعداد الطالبة :
- بقوقة بشرى

تحت إشراف
الدكتور: رابحي لخضر

لجنة المناقشة:

الدكتور بوقرين عبد الحليم..... رئيسا
الدكتور رابحي لخضر ..... مشرفا ومقررا
الدكتور بوزيدي أحمد التجاني..... عضوا ممتحنا

السنة الجامعية:2020/2019


بسم الله الرحمن الرحيم

شكر وعرفان

نشكر الله عز و جل

ونحمده حمداً كثيراً على عطاءه لإنجاز هذا العمل المتواضع.

نتقدم بكل الاحترام والتقدير على كل من ساعدنا من بعيد أو قريب في إنجاز هذه المذكرة ونخص بالذكر:

الدكتور الفاضل "**رابحي لخضر**" على مجهوداته الجبارة والذي لم يبخل علينا في تصويب كل صغيرة وكبيرة في هذا العمل وإشرافه عليه والذي لن تكفي حروف هذه المذكرة لإيفائه حقه بصبره الكبير ولتوجيهاته العلمية التي لا تقدر بثمن والتي ساهمت بشكل كبير في إتمام وإستكمال هذه المذكرة .

وكل أساتذة قسم الحقوق على ما قدموه لنا خلال مشوارنا الدراسي

وعلى رأسهم اللجنة الموقرة التي قبلت مناقشة هذه المذكرة المتواضعة

وإلى كل من مدنا بيد العون من قريب ومن بعيد

وشكراً

إهـــداء

ا

بداية إن الفضل والمنة لله وحده وليس للعبد الضعيف أن هدانا الى طريق النجاح وجعلنا نعيش في هذا العصر بثقة بالله عزوجل.

بعملي المتواضع هذا اسأل الله عزوجل الحفظ والستر لكل من احبه.

إلى التي أهدتني نور الحياة وسقتني من دفقات حبها ورعايتها والتي قدمت لي ايات الحب والحنان، إلى أعذب كلمة رددها لساني والتي وضعت الجنة تحت قدميها أمي الحبيبة أطال الله في عمرها .

إلى الذي إستلهمت منه معاني الثبات وزرع في قلبي حب العلم والقوة العزيمة، إلى الذي وهبني كل رعايته وإهتمامه أبي العزيز أدامه الله لي .

إلى من ترعرعت معهم ونمى غصني بينهم اخوتي: **بلال** و**بلقيس** وجميع أفراد العائلة الكبيرة وإلى رفيقة دربي **حليمة** التي لم تترك بيدي في يوم من الأيام.

الى كل ما صادقتهم الروح في مشواري الأصدقاء والزملاء على رأسهم **أمينة وصبرينة**

وإلى كل من ذكرهم لساني ولم يسعهم قلمي.

الى كل من جرى بيننا سلام الله عزوجل حفظهما الله لي حيث ما كنتم.

ولكل من ساندنا من قريب وبعيد نقول له شكراً.

قائمة المختصرات:

الكلمة	إختصارها
بدون طبعة	ب ط
الصفحة	ص
من صفحة الى الصفحة	ص ص
قانون العقوبات الجزائري	ق ع ج
الجريدة الرسمية	ج ر
المادة	م
الى اخره	الخ
بدون عدد	ب ع

مقدمة

كانت الحياة صعبة وتقليدية وبسيطة في شتى المجالات سواء السفر أو الاتصال أو التواصل مع الغير والعديد من ذلك، فكان الإنسان بسيطا لكن كونه كائن متطور بطبيعته فدائما يبحث عن افضل السبل لمتطلباته وهذا ما يجعله يفكر ويطور من نفسه فتم اختراع الآلات وتطوريها كالهاتف والتلفاز، ثم ظهرت الانترنت التي جعلت العالم قرية صغيرة، فهذه التكنولوجيا سهلت حياتنا اليومية في شتى الميادين سواء في التنقل من مكان الى آخر والتي جعلت الشخص يسافر في بضع ساعات فقط، كما ساعدت هذه التكنولوجيا في الاتصال والتواصل بين الناس رغم المسافات البعيدة وليس ذلك فقط بل حتى في انتقال الاحداث والمعلومات التي تصل الينا في حينها بالصوت والصورة في أي مكان نتواجد به ورغم تقدم التكنولوجيا الا انها سلاح ذو حدين فأصبحت تستعمل بشكل سلبي حيث ظهرت جرائم ما كانت أبدا تخطر على بالنا، فقد ترتكب هذه الجرائم عن بعد التي يكون فيها الجاني في دولة وترتكب الجريمة في دولة اخرى وهذه ما تعرف بالجرائم المعلوماتية .

فكانت اول جريمة معلوماتية ارتكبت بواسطة الحاسوب والتي تمثلت في نشر تقارير تسئ الى استخدمها ثم اصبحت تقترف عن طريق زرع فيروسات إلكترونية التي تؤدي الى تخريب الملفات والبرامج وهذا ما دفع الاشرار لاستغلالها واستعمالها بشكل سيء واصبحوا شئ فشيئا يخترقون بها قاعدة بيانات أو بطاقات ائتمان ويتلاعبون بملفات خاصة وحسابات بنكية والعديد من الجرائم المختلفة كجرائم تبييض الأموال والإرهاب والجريمة المنظمة بكل صورها.

تكمن أهمية الموضوع في إبراز العناصر التي تقوم عليها الجرائم المعلوماتية والوقوف على الأحكام التي جاء بها قانون العقوبات الجزائري بالإضافة إلى قانون رقم 09-04 المؤرخ في 05 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها بالإضافة إلى أنه موضوع يستحق الدراسة وليس ذلك فقط بل تكاثرت هذه الجرائم وأصبحت تهدد سلامة الفرد والمجتمع.

ومن بين الأهداف المتوخاة من الدراسة التعرف على الجرائم المعلوماتية واليات مكافحتها دوليا ووطنيا وكيفية معالجة المشرع هذه الجرائم من خلال القوانين التي شرعها وتسليط الضوء على العقوبة .

وتعود أسباب اختيار الموضوع الى أسباب شخصية وأسباب موضوعية فالأولى تكمن في الميول الشخصي والرغبة في دراسة هذا الموضوع، أما الأسباب الثانية تتمثل في محاولة إثراء هذا الموضوع وبيان آليات الوقاية والمكافحة لجرائم المعلوماتية.

ومن بين الصعوبات التي التقينا بها فتكمن في قلة المراجع خاصة في الجانب الإجرائي وذلك بسبب فيروس كوفيد 19 الذي أدى إلى غلق جميع المرافق خاصة المكتبات العامة والخاصة.

أما بالنسبة للدراسات السابقة التي تناولت نفس الموضوع منها

ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة لنيل شهادة الدكتوراه، تخصص قانون العقوبات وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة1 2015-2016.

فيصل بدري، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة لنيل شهادة الدكتوراه، تخصص قانون عام، كلية الحقوق، جامعة يوسف بن خدة،2017-2018.

وبناءا على ما تقدم التساؤل الذي يثار في هذا الموضوع هو:

إلى أي مدى وفقت التشريعات الوطنية والاتفاقيات الدولية في مكافحة الجريمة المعلوماتية؟

اعتمدت في دراستي على عدة مناهج بغية الإلمام بجوانب الموضوع محل الدراسة كالاتي:

1/ المنهج الوصفي: تظهر معالمه في دراستنا في العديد من المواضع لبيان التعاريف المستعملة ضمن الدراسة.

2/ المنهج المقارن: وذلك بمقارنة القوانين الجزائرية التي نصت على الجرائم المعلوماتية وبنصوص قانونية أخرى لدول تناولت نفس الجريمة.

وقد قسمنا دراستنا إلى مقدمة وفصلين وخاتمة

الفصل الأول: بعنوان الأحكام العامة للجريمة المعلوماتية حاولنا من خلاله التطرق الى مفهوم الجريمة المعلوماتية في المبحث الأول والى سبل الوقاية من الجرائم المعلوماتية في المبحث الثاني.

الفصل الثاني: بعنوان آليات مكافحة الجريمة المعلوماتية القانون الجزائري والاتفاقيات الدولية حاولنا من خلاله التطرق الى إلى الجوانب الموضوعية في نصوص الجريمة المعلوماتية في المبحث الأول وإلى الأساليب الإجرائية لنصوص الجريمة المعلوماتية في الاتفاقيات الدولية والقانون الجزائري في المبحث الثاني.

الفصل الأول:

الأحكام العامة للجريمة المعلوماتية

الفصل الأول : الأحكام العامة للجريمة المعلوماتية

توجد العديد من التسميات لجرائم المعلوماتية فهناك من يسميها جريمة تقنية المعلومات الحديثة أو الجرائم الإلكترونية أو جرائم الأنترنت، فهذه تعتبر من أخطر الجرائم في وقتنا فبدأت تظهر وتنمو تدريجيا بنمو وتطور عصابات الجريمة المنظمة التي تتخذ من غسيل الأموال وتجارة المخدرات والأسلحة غير مشروعة وأعمال السرقة والابتزاز والفساد وجرائم الإلكترونية والإرهاب حرفة لها.

وسوف نبحث فيما يلي عن الاطار المفاهيمي لجرائم المعلوماتية والذي يتضمن مفهوم هذه الجريمة (مبحث الأول) وطرق الوقاية منها (مبحث الثاني) .

المبحث الأول: مفهوم الجريمة المعلوماتية

تعددت التعريفات التي تناولت الجريمة المعلوماتية، ويرجع ذلك إلى الخلاف الذي أثير بشأن تعريف هذه الجريمة، فالجرائم المعلوماتية هي صنف جديد من الجرائم، ذلك أنه مع ثورة المعلومات والاتصالات ظهر نوع جديد من المجرمين انتقلوا بالجريمة من صورتها التقليدية إلى أخرى إلكترونية قد يصعب التعامل معها، الجريمة المعلوماتية من خلال(المطلب الأول) إلى الخصائص (المطلب الثاني).

المطلب الأول : تعريف وخصائص الجريمة المعلوماتية

لقد تعددت التعاريف حول الجريمة المعلوماتية باعتبارها ظاهرة جديدة فلا يوجد تعريف متفق عليه ، سوف نحاول تبيان مختلف التعاريف لهذه الجريمة (الفرع الأول) وخصائصها (الفرع الثاني).

الفرع الأول : تعريف الجريمة المعلوماتي

اهتم الفقهاء و القانونين و المختصين في مجال المعلوماتية لوضع تعريف شامل للجريمة المعلوماتية فحاول كل منهم حسب اختصاصه وضع تعريف ملائم فمنهم من عرفها بأنها الجرائم المرتبطة بالحاسوب والتي تشكل انتهاكا للقانون الجنائي

ومنهم من قال بأنها تلك الجريمة التي يستخدم فيها الحاسوب ولوضع تعريف متكامل لهذا النوع من السلوك الاجرامي فيجب معرفة مدلولها باللغة الفرنسي (cybercriminalitè)

فأصل الكلمة(cyber) يوناني و يقصد بها التحكم والتسيير والمراد بها في مجال المعلوماتية المعالجة الالية للمعطيات، وقد شاع استعمال هذا المصطلح واتصل بكافة[1] صور الإجرام

كالغش المعلوماتي، الإرهاب المعلوماتي، أما من الناحية القانونية لا يوجد مصطلح قانوني موحد للدلالة على الجرائم الناشئة عن سوء استغلال النظم المعلوماتية، أو إساءة استخدامها فهناك من يطلق عليها وصف جريمة الغش المعلوماتي، وهناك من يطلق عليها وصف جريمة الاختلاس المعلوماتي وآخر يصفها بجرائم الاحتيال المعلوماتي غير أن مصطلح الأكثر شيوعا هو مصطلح الجريمة المعلوماتية.

أولا : التعريف الفقهي

إنقسم الفقهاء لإعطاء التعريف فهناك من اتجه اتجاه ضيق وأخر اعتمد الاتجاه الموسع

1) **الاتجاه الضيق:** تزعم هذا الاتجاه الفقيه (merwe) حيث عرف الجريمة المعلوماتية على أنها "هي ذلك الفعل الغير المشروع الذي يتورط في ارتكابه الحاسب"،كما عرفها (rosblat) بأنها "نشاط غير مشروع موجه لنسخ أو تغير أو حذف أو الوصول الى المعلومات المخزنة داخل الحاسوب أو التي تحول عن طريقه"[2]

أما (solerez) فعرفها بأنها " أي نمط من أنماط الجرائم المعروفة في قانون العقوبات طالما كان مرتبطا بتقنية المعلومات ."

-هذه التعاريف نجدها تستند الى موضوع الجريمة و نمط السلوك محل الجريمة دون أن تأخذ بعين الاعتبار المجرم وهو ما أدى الى ظهور الاتجاه الموسع الذي نجده يستند الى الفاعل يدل موضوع الجريمة .

[1] حسين ربيعي، اليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة لنيل شهادة الدكتوراه في الحقوق، تخصص قانون عقوبات وعلوم جنائية، كلية الحقوق و العلوم السياسية، جامعة باتنة 1، 2015-2016 ص 23.

[2] نجاة بن مكي، السياسة الجنائية لمكافحة جرائم المعلومات، ط1، الجزائر، 2017، ص 11.

2) الاتجاه الموسع: حاول هذا الاتجاه اعطاء تعريف موسع للجريمة المعلوماتية لتفادي النقص الموجود في التعاريف السابقة فعرفت بأنها: "كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع للتقنية المعلوماتية بهدف الاعتداء على الأموال المادية أو المعنوية[1] " كما عرفت بأنها "كل سلوك سلبي كان أم إيجابي يتم بموجبه الاعتداء على البرامج أو المعلومات للاستفادة منها بأية صورة كانت".

وهنا يرى الفقيهان (Michel و credo) أن سوء استخدام الحاسوب يشمل استخدام الحاسوب كأداة لارتكاب الجريمة، إضافة الى الحالات المتعلقة بالولوج غير المصرح بها لحاسوب المجني عليه، أو بياناته.

كما تمتد هذه الجريمة لتشمل الاعتداءات المادية الماسة بالحاسوب ذاته أو المعدات المتصلة به و كذلك الاستخدام غير المشروع لبطاقات الائتمان و تزييف المكونات المادية و المعنوية للحاسوب بل و سرقة جهاز الحاسوب في حد ذاته أو مكون من مكوناته .

ثانيا: التعريف الاصطلاحي

عرفت منظمة التعاون الاقتصادي و التنمية سنة 1983 O.E.C.D الجريمة المعلوماتية بأنها " كل فعل وعمل غير مشروع أو مخالف للأنظمة و غير مرخص يستهدف أنظمة المعالجات الآلية للمعلومات أو تبادلها أو نقلها "وتشمل الجريمة المعلوماتية بهذا المفهوم "كل الجرائم التي يمكن أن تقع أو تمس بشبكات الاتصال بصفة عامة وشبكة الأنترنت بصفة خاصة".

وقد ورد تعريف الجريمة المعلوماتية بحسب ما قدمه مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين الذي عقد بفيينا سنة 2000 بأنها :"كل جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام الحاسوب و تشمل من الناحية

[1] حسين ربيعي، المرجع السابق، ص26.

المبدئية جميع الجرائم التي يمكن أو ترتكب في بيئة إلكترونية وعرفها الخبير الأمريكي (PARKER) كل فعل إجرامي متعمد أي كانت صلته بالمعلوماتية ينشأ خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل".

فما يمكن استنتاجه من جملة هذه التعاريف أن الجريمة المعلوماتية هي تلك الجريمة المرتبطة أساسا بمظاهر التقدم التكنولوجي.[1]

ثالثا: التعريف القانوني

اختلفت التشريعات في تعريف الجريمة المعلوماتية

- **1) تعريفات الجريمة المعلوماتية لدى بعض التشريعات العربية**

سنتناول تعريفات كل من المشرع المصري و السعودي

- **أ) تعريف المشرع المصري للجريمة المعلوماتية**

تعتبر الجريمة المعلوماتية من الجرائم المستحدثة التي بدأت في الانتشار بشكل واسع في الآونة الأخيرة نظرا لكونها جريمة حديثة، وبالرجوع للمشرع المصري نجده لم يقم بتعريف الجريمة بل ترك مسألة تعريف الجريمة المعلوماتية للفقه وبالتالي اختلف الفقهاء في تعريفها فهناك من عرفها من الزاوية الفنية على أساس أنها عمل أو امتناع يأتيه أضرار بمكونات الحاسب وشبكات الاتصال الخاصة به التي يحميها قانون العقوبات ويفرض لها عقابا، كما يعرفها البعض الأخر من الفقه على أنها نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول الى المعلومات المخزنة داخل الحاسب .

كما أنه يوجد من عرفها اعتمادا على وسيلة ارتكاب الجريمة على أساس أنها فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية لحدوث هذا النوع المستحدث من الإجرام.

[1] حسين ربيعي، المرجع السابق، ص24.

ب) تعريف المشرع السعودي للجريمة المعلوماتية

عرف المشرع السعودي الجريمة المعلوماتية من خلال نظام مكافحة جرائم المعلوماتية بأنها" أي فعل يرتكب متضمنا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام."[1]

وبالتالي فالجريمة المعلوماتية بحسب هذه المادة هي عبارة عن سلوك إجرامي يستخدم فيه الحاسب الآلي أو شبكة المعلوماتية كوسيلة لحدوث هذا النوع المستجد من الجرائم، كما نجد أن نظام مكافحة الجرائم المعلوماتية في المملكة السعودية عرف الجريمة المعلوماتية على غرار بعض التشريعات الأخرى التي تركت مسألة تعريفها للفقه كالمشرع المصري و المشرع الجزائري .

2) تعريف الجريمة المعلوماتية في بعض التشريعات الأخرى .

سنتناول تعريفات كل من المشرع الفرنسي والأمريكي

أ) تعريف المشرع الفرنسي للجريمة المعلوماتية

لم يعرف المشرع الفرنسي الجريمة المعلوماتية فقد نص على تجريم بعض الأفعال المساهمة في حدوثها ضمن نصوص قانونية. وقام الفقهاء بإعطاء عدة تعاريف و من بين الفقهاء الفرنسين نجد الفقيه (Masse)

[1] أمينة بوشعرة أمينة وسهام موساوي ، الإطار القانوني للجريمة الإلكترونية (دراسة مقارنة)، مذكرة لنيل شهادة الماستر تخصص القانون الخاص والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة ميرة – بجاية – 2017-2018، ص ص 7،8 .

فعرف الجريمة المعلوماتية أنها "الاعتداءات القانونية التي يمكن أن تتركب بواسطة المعلوماتية بغرض تحقيق الربح" .

كما يعرفها الفقيهان الفرنسيان (stane) و (vivant)بأنها "مجموعة من الأفعال المرتبطة بالمعلوماتية والتي يمكن أن تكون جديرة بالعقاب."[1]

تطرق المشرع الفرنسي في الفصل الثالث من قانون العقوبات الفرنسي الى جريمة المعلومات وأعطى له عنوان المساس بأنظمة المعالجة الالية للمعطيات فجرم بعض الأفعال المساهمة في حدوث الجريمة المعلوماتية كتجريمه لفعل البقاء والدخول بطريق الغش الى نظام المعالجة الآلية للمعطيات وسلط على ذلك عقوبة الحبس لمدة سنتين وغرامة قدرها 60000 أورو، وبالتالي فالمشرع الفرنسي لم يعرف الجريمة المعلوماتية بل إكتفى بتجريم بعض الأفعال المساهمة في حدوث هذه الجريمة[2].

ب) تعريف المشرع الأمريكي للجريمة المعلوماتية

-أشار الخبير الأمريكي (parker) الى الجريمة المعلوماتية بأنها " كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية ينشا عنه خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل "

حسب نظره الجريمة المعلوماتية تنطوي على ست خطوات أساسية يتم تنفيذها آليا بواسطة برنامج أو عدة برامج و تكمن هذه الخطوات فيما يلي :

* البحث عن نظام الحاسب الآلي الذي يحتوي على المعلومات أو البرامج المطلوبة
* الوصول الى نقاط الضعف في النظام الذي يحتوي على هذه المعلومات أو البرامج .
* الاستفادة من هذه النقاط للدخول الى نظام ثم التحكم فيه .

[1] أمينة بوشعرة وسهام موساوي، المرجع السابق، ص 9.

[2] L'article 323-1 du code pénal ,dispose « Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende. » loi n°92-685 du 22 juillet 1992 le code pènal français (Dernière modification: 11/05/2020)

* تنفيذ السلوك الإجرامي الذي تم التخطيط له و تحديده مسبقا .

*تحويل هذا السلوك الى ربح غير مشروع يحصل عليه الجاني أو الى خسارة تلحق بالمجني عليه.

*إخفاء جميع الأدلة تجنبا لكشف الفاعل و سلوكه الإجرامي.

كما يعرفها الفقيه (david thompson) بأنها " أية جريمة يكون متطلبا لاقترافها أن يتوفر لدى فاعلها معرفة تقنية الحاسب ".

من خلال إستعراض التعريفات الفقهية يتضح لنا أن هناك إختلاف في تعريف الجريمة المعلوماتية إلا أنها كلها تؤدي إلى نفس المدلول للجريمة التي نحن بصدد دراستها[1].

3) تعريف المشرع الجزائري للجريمة المعلوماتية

عرف المشرع الجزائري الجريمة المعلوماتية في نص المادة 2 الفقرة –أ– من القانون رقم 09– 04 بأن (الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال هي جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية) [2].

نجد أن المشرع الجزائري للدلالة على الجريمة المعلوماتية اصطلح على تسميتها بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال، فقد اعتبر أن النظام المعلوماتي في حد ذاته وما يحتويه من مكونات غير مادية محلا للجريمة و يمثل نظام المعالجة الألية للمعطيات الشرط الاول الذي لابد من تحققه .

[1] أمينة بوشعرة وسهام موساوي، المرجع السابق، ص ص 11،12.

[2] المادة الثانية من قانون رقم 09– 04 المؤرخ في 5 اوت 2009 المتضمن القواعد الخاصة للوقاية من جرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، ج ر عدد 47 سنة 2009 .

حتى يمكن توافر أركان الجريمة، وبالرجوع لقانون العقوبات الجزائري نجده لم يعرف جرائم المعلوماتية بل اكتفى بتسليط العقوبة على بعض الأفعال تحت عنوان الجرائم الماسة بنظام المعالجة الآلية للمعطيات [1]

حيث نصت المادة 394 مكرر على ما يلي: (يعاقب بالحبس من ثلاثة أشهر الى سنة وبغرامة من 50.000 دج الى 200.000 دج)

كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الالية للمعطيات أو يحاول ذلك، واذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين وبغرامة من 50.000 دج إلى 300.000 دج)[2].

نجد أن المشرع الجزائري اعتمد على عدة معايير للدلالة على الجريمة المعلوماتية، فاعتمد على معيار وسيلة الجريمة من جهة وهو نظام الاتصالات الإلكتروني ومن جهة أخرى معيار موضوع الجريمة إلا وهو المساس بأنظمة المعالجات الآلية للمعطيات، أما المعيار الثالث وهو قانون الواجب التطبيق أو الركن الشرعي للجريمة المنصوص عليها في قانون العقوبات.

أما المعيار الرابع يتمثل في تحديد نطاق الجريمة المعلوماتية باعتبارها ترتكب في نظام معلوماتي أو نظام الاتصالات الإلكترونية.[3]

[1] أمينة بوشعرة وسهام موساوي، المرجع السابق، ص 12،13.

[2] المادة 394 مكرر من الامر 66-156 المؤرخ في صفر عام 1386 الموافق ل 8 يونيو 1966 الذي يتضمن قانون العقوبات المعدل والمتمم.

[3] أمينة بوشعرة وسهام موساوي، نفس المرجع، ص 13.

الفرع الثاني : أنواع الجرائم المعلوماتية

ساعد استخدام الحاسوب والأنترنت مجرمي المعلوماتية في ارتكاب عدة جرائم وذلك باستخدام وسائل وتقنيات حديثة ومتطورة لبلوغ أهدافهم، وبسبب هذه التقنيات تعددت أنواع الجرائم المعلوماتية أهمها:

أولا : الاعتداء على الوظائف الطبيعية للحاسب

تمثل البرامج و المعلومات المحور الأساسي الذي تدور حوله المعلوماتية نظرا لقيمتها والتالي تكون هدفا أساسيا بالنسبة إلى الجناة الذين يحاولون الاستيلاء عليها بشتى الطرق وذلك من خلال التعدي على المعلومات أو البرامج أو الإخلال بأمنها أو العبث بمحتوياتها.

ثانيا :الاعتداءات الواقعة على الأشخاص

تشكل المعلوماتية في جانبها السلبي خطرا على سرية المعلومات الخاصة بالأشخاص كما تسهل عمليات الاحتيال والسرقة للأموال وعليه فالاعتداءات الواقعة على الأشخاص تكمن في الاعتداء على حرمة الحياة الخاصة للأفراد مثال قيام الجاني بالمعالجة الإلكترونية للبيانات الشخصية قاصدا استغلالها في غير الذي تم جمعها من أجله إضافة على ذلك.

هناك السب والقذف التي تبرز سلبيات الشخص المستهدف أو نشر أسراره التي قد يتم الحصول عليها بطريقة غير مشروعة بعد الدخول على جهازه أو بإشاعة الأخبار عنه وحوادث التشهير والقدف على شبكة الأنترنت كثيرة[1].

[1] نجاة بن مكي، المرجع السابق، ص ص 45، 57.

توجد حماية دستورية و قانونية للحياة الخاصة بالأفراد في مختلف تشريعات الدول لأهميتها على كيان الفرد و المجتمع ، فقد كفل الدستور الجزائري الحماية الدستورية للعديد من الحقوق من بينها المادتين 1/40 و 46.[1]

ثالثا : الاعتداءات الواقعة على الاموال

يقصد بالاعتداءات الواقعة على الأموال تلك الجرائم التي تستهدف عناصر الذمة المالية، ويكون الطمع وراء ارتكابها والاستيلاء والحصول على تلك الأموال، فتوجد العديد من تطبيقات هذه الجرائم في نطاق الجرائم المعلوماتية، ومن بينها إساءة استخدام البطاقة من قبل الغير فعملية نقل وتبادل البيانات على الإنترنت منها البيانات المتعلقة ببطاقة الائتمان[2] كالرقم السري يجعلها عرضة للالتقاط من قبل الغير سيء النية وبالتالي إستخدامها بطرق غير مشروعة في سحب النقود الإلكترونية أو الوفاء بها[3].

أما الاعتداءات الواقعة على أمن الدولة فهي تلك الجرائم التي تنال بالاعتداء أو تهدد حقوق ذات طابع عام[4]، ولها عدة صور من بينها الجريمة المنظمة التي تستقطب عناصرها من بين الخبراء في المعلوماتية ورجال السياسة والعاملين في الاجهزة الحكومية والمؤسسات المالية.

فهي تستخدم كافة عناصر التكنولوجيا الحديثة لتحقيق أهدافها، ولقد وجدت هذه المنظمات في شبكة الأنترنت وسيلة لا تضاهى للقيام بعمليات غسيل الأموال على نطاق واسع وكذلك

[1] القانون رقم 16-01 المتضمن التعديل الدستوري المؤرخ في 6مارس 2016 ج ر عدد 14

[2] نادية ضريفي وزوليخة بن طاية، الجريمة المعلوماتية في إطار ماهيتها وأنواعها، مؤلف جماعي حول مواجهة الجريمة المعلوماتية، جامعة محمد بوضياف بالمسيلة، ب ع، المنشورات العلمية لكلية الحقوق والعلوم السياسية، أكتوبر 2019، ص 23.

[3] نجاة بن مكي، المرجع السابق، ص 60.

[4] نادية ضريفي وزوليخة بن طاية، نفس المرجع، ص 32.

لتدعيم تجارة الأعضاء البشرية عبر إنشاء مواقع خاصة بهذه الأعمال، وهذه التقنيات الحديثة تتناسب مع طبيعة النشاطات الإجرامية لجماعات الجريمة المنظمة التي تعد من الجرائم العابرة للحدود، وخلال السنوات القليلة الماضية بدأت بعض المجموعات التي تتعاطى الجريمة المنظمة كحرفة لها وبناء قاعدة عمل في الدول الضعيفة التي أصبحت ملاذا آمنا تستطيع من خلاله ممارسة عملياتها العابرة للأوطان حيث لا توجد أي حدود ويشكل ذلك مزية تجعل النشاط الإجرامي عملا سهلا للغاية مقارنة بالواقع التقليدي للجريمة أيضا هناك جرائم ذوي الياقات البيضاء المرتكبة من طرف الطبقات الراقية في المجتمع ذوي المناصب الادارية الكبيرة و تشمل أنواعا مختلفة من الجرائم كالرشوة والتلاعب[1] بالشيكات

والاختلاس والسرقة وتزوير المعاملات التجارية للشركات العالمية ووصفها على منتجات محلية أو عالمية غير مشهورة وشراء المعلبات قبل انتهاء صلاحيتها واستبدال تاريخ صلاحيتها.

المطلب الثاني: خصائص و أركان الجريمة المعلوماتية

تتميز الجريمة المعلوماتية بمجموعة من الخصائص تميزها عن الجرائم التقليدية التي سنتعرف عليها من خلال هذا المطلب بالإضافة الى الأركان التي تقوم عليها هذه الجريمة .

الفرع الأول: مميزات الجريمة المعلوماتية

للجريمة المعلوماتية مميزات منها انها عابرة للحدود وانه يصعب اكتشافها والعديد من المميزات الاخرى وأيضا توجد للمجرم المعلوماتي سمات خاصة به تميزه عن غيره من المجرمين سنتعرف عليهما من خلال هذا الفرع.

[1] نجاة بن مكي، المرجع السابق، ص ص 62،63.

أولا: سمات الجريمة المعلوماتية

من بين أهم سمات الجريمة المعلوماتية ما يلي:

1) الجريمة المعلوماتية جريمة عابرة للحدود

تتسم الجريمة المعلوماتية غالبا بالطابع الدولي، فهي لا تعترف بالحدود بين الدول أو القارات ولذلك فهي جريمة عابرة للقارات، حيث تعتبر شكلا جديدا من أشكال الجرائم العابرة للحدود الاقليمية بين دول العالم كافة، إذ يمكن من خلال النظام المعلوماتي ارتكاب العديد من الجرائم مثل جرائم التعدي على قواعد البيانات والاحتيال المعلوماتي والقرصنة وغسيل الاموال[1].

فالجريمة المعلوماتية هي من نوع الجرائم التي يتم ارتكاب عن بعد، حيث لا يتواجد الفاعل في مسرح الجريمة بل يرتكب جريمته عن بعد أي عدم التواجد المادي للمجرم المعلوماتي في مكان الجريمة بالإضافة الى تباعد المسافات بين الفعل الذي يتم من خلال جهاز كمبيوتر الفاعل وبين النتيجة اي المعطيات محل الاعتداء وبالتالي لا تقف الجريمة المعلوماتية عند الحدود الاقليمية لدولة معينة بل تمتد الى الحدود الاقليمية لدولة اخرى مما يزيد من صعوبة اكتشافها.

ونجد هذه الخاصية أيضا في جرائم اخرى كتجارة المخدرات وغسيل الاموال لكن ما يميز الجريمة المعلوماتية عنهم حيث أنها ترتكب دون مغادرة المقعد المقابل للحاسب الالي بعكس جرائم المخدرات[2].

التي تتطلب حركة بين الدول، فالتباعد بين مكان الجاني والمجني عليه في هذه الجرائم ادى الى تشتت الجهود في مواجهة هذا النوع من الإجرام، فمثلا قد يكون الجاني موجود في

[1] خالد ممدوح، الجرائم المعلوماتية، ط1، دار الفكر الجامعي، مصر،2009، ص 77.

[2] غانم مرضي الشمري، الجرائم المعلوماتية، ط1، الدار العلمية الدولية، الاردن، 2016، ص 37.

اوروبا والمتضرر في أمريكا وهذا ما يجعل التصدي لهذا النوع من الاجرام أمرا عسيرا وذلك لاختلاف الاجراءات الجنائية أو النزاع حول القانون الواجب التطبيق.

2) صعوبة اكتشاف و إثبات الجريمة المعلوماتية

تتميز جرائم المعلوماتية بصعوبة اكتشافها وإثباتها وذلك يسبب أنها لا تترك أثرا خارجيا يمكن الإعتماد عليه في الإثبات فلا يوجد جثث لقتلى ولا اثار للدماء وإذا اكتشفت الجريمة فلا يكون ذلك إلا بمحض الصدفة، فجرائم المعلوماتية لها طبيعة خاصة ما يكسبها هذه الميزة، ويعد التطور التكنولوجي المتلاحق سببا رئيسيا لذلك حيث أن شبكة الانترنت (تلك الشبكة الدولية) انتشرت بواسطتها مكاتب معروفة ومتخصصة ترتزق من قيامها بأعمال السطو وبيع المعلومات وبالإمكان الاستعانة بها أو استئجار القراصنة المحترفين للقيام بالأعمال غير المشروعة المتصلة بالحاسب مقابل مبالغ مالية يتفق عليها.

وهؤلاء القراصنة الذين يقومون بالجرائم باستخدام الحاسب الالي لا يهاجمون من أجهزة الحاسب الخاصة بهم مما يزيد لأمر تعقيدا، إنما يدخلون الى شبكات بعيدة عنهم و يهاجمون من خلالها[1].

فعدم تعاون المجني عليه أدى إلى عدم وجود إحصاءات دقيقة تحدد الحجم الحقيقي لهذه الظاهرة وذلك بعدم التبليغ عنها أصلا خوفا الاضرار بالمركز المالي للجهة المعتدى عليها وحفاظا على شعور المساهمين بالائتمان والثقة حتى لا تقلد هذه الجرائم مرة أخرى[2].

[1] غانم مرضي الشمري، المرجع السابق، ص ص 39، 40.

[2] نجاة بن مكي، المرجع السابق، ص 21.

3)الحاسب الالي هو اداة ارتكاب الجريمة المعلوماتية

حيث تعتبر هذه الخاصية أهم الخصائص التي تتميز بها الجريمة المعلوماتية، كما أن ارتباط شبكة الأنترنت بالحاسب الالي أمر لا مفر منه، باعتباره النافذة التي تطل بها تلك الشبكة على العالم الخارجي.

4)صعوبة تحديد المسؤول جنائيا عن الفعل الاجرامي

ويظهر ذلك بوضوح في حالة وقوع جريمة على شبكة الأنترنت، كأن يدخل المستخدم الى شبكة فيجد موقعا به أفعال إباحية فهل يسال عن هذه الجريمة عامل الاتصال أم مورد المعلومات أم غير ذلك من العاملين في مجال الأنترنت؟

5)من حيث القوة المتطلبة لارتكابها

عدم وجود عنف في هذه الجرائم فلا وجود لجثث وأثار دماء أو اقتحام من أي نوع، كما أنها لا تستلزم جهدا شاقا حيث يكفي لمس لوحة مفاتيح وأساليب الحماية الأكثر خداعا.

6)تقع الجرائم المعلوماتية عادة في بيئة المعالجات الالية للبيانات [1]

فالبرامج بما تتضمنه من معلومات هي محل الاعتداء.

7)تعتبر جرائم فادحة الاضرار

إن الاعتماد المتزايد على الحاسب الالي في ادارة مختلف الاعمال في شتى المجالات ضاعف من الاضرار والخسائر التي تخلفها الاعتداءات على معطيات هذا الحاسب لا سيما إذا كانت تمثل قيمة مالية خاصة مع ازدياد اعتماد البنوك والمؤسسات المالية ومختلف الشركات على الحاسب الالي في تسييرها .

[1] نجاة بن مكي، المرجع السابق، ص22.

وفي هذا الخصوص تشير الدراسات الى أن الاضرار الناجمة عن جرائم المعطيات تفوق بكثير تلك الناجمة عن الجرائم التقليدية[1].

ثانيا : سمات المجرم المعلومات

لم يكن لارتباط الجريمة المعلوماتية بالحاسب الالي اثره على تمييز الجريمة المعلوماتية على غيرها من الجرائم التقليدية فحسب، وإنما كان له اثره ايضا على تمييز المجرم المعلوماتي عن غيره من المجرمين، وقد يختلف الباحثون في تحديد هذه السمات ويعد الأستاذ" باركر[2]"

واحد من اهم الباحثين الذين اهتموا بالجريمة المعلوماتية بصفة عامة وبالمجرم المعلوماتي بصفة خاصة إلا أنه لا يخرج في النهاية عن كونه مرتكبا لفعل اجرامي يتطلب توقيع العقاب عليه.

فالمجرم المعلوماتي ينتمي في الكثير من الحالات الى وسط اجتماعي متميز كما انه على درجة من العلم والمعرفة، وان لم يكن من الضروري ان ينتمي الى مهنة يرتكب من خلالها الفعل الاجرامي[3].

و يتميز المجرم المعلوماتي بمجموعة من الخصائص التي تميزه بصفة عامة عن غيره من المجرمين ويرمز إليها الأستاذ باركر بكلمة(S.K.R.A.M) والتي تعني:

[1] نجاة بن مكي، المرجع السابق، ص ص23،20.

[2] فريال لعاقل، الجريمة المعلوماتية في ظل التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون العام، تخصص القانون الجنائي و العلوم الجنائية، كلية الحقوق و العلوم السياسية، جامعة اكلي محند اولحاج –البويرة– 2014–2015، ص19.

[3] فريال لعاقل ،نفس المرجع، ص 20.

1) المهارة SKILL والمعرفة KNOWLEDGE

فالمهارة المتطلبة لتنفيذ النشاط الاجرامي ابرز خصائص المجرم المعلوماتي والتي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات، أو بمجرد التفاعل مع الاخرين. أما المعرفة يقصد بها التعرف على كافة الظروف المحيطة بالجريمة المراد تنفيذها وإمكانية نجاحها واحتمال فشلها حيث يستطيع المجرم المعلوماتي تكوين تصورا كاملا لجريمته ويرجع ذلك الى أن المسرح الذي تمارس فيه الجريمة المعلوماتية هو نظام الحاسب الآلي، فالفاعل يستطيع أن يطبق جريمته على انظمه مماثلة لتلك التي يستهدفها وذلك قبل تنفيذ جريمته[1].

3)الوسيلة RESOURCES والباعث MOTIVES

يقصد بالوسيلة الإمكانيات التي يتزود بها الفاعل لإتمام جريمته وفيما يتعلق بالمجرم المعلوماتي فان الوسائل المتطلبة للتلاعب بأنظمة الحاسبات الآلية هي في أغلب الحالات تتميز نسبيا بالبساطة وبسهولة الحصول عليها[2].

ولا يختلف الدافع لارتكاب الجريمة المعلوماتية في كثير من الاحيان عن الدافع لارتكاب غيرها من الجرائم الاخرى فالرغبة في تحقيق الربح المادي بطريقة غير مشروع يظل الباعث الاول وراء ارتكاب الجريمة المعلوماتية، ثم يأتي بعد ذلك مجرد الرغبة في قهر نظام الحاسب وتخطي حواجز الحماية المضروبة حوله وأخيرا الانتقام من رب العامل أو احد الزملاء[3].

[1] طارق ابراهيم الدسوقي عطية، الامن المعلوماتي، ب ط، دار الجامعة الجديدة، مصر،2009، ص ص 176،177.

[2] فريال لعاقل، المرجع السابق، ص 21.

[3] طارق إبراهيم الدسوقي عطية، نفس المرجع، ص 178.

4) السلطة AUTHORITY

ويراد بها جملة الحقوق والمزايا التي يتمتع بها المجرم المعلوماتي والتي تسمح له وتمكنه من ارتكاب جريمته، كثير من المجرمين في هذا المجال لديهم سلطة مباشرة أو غير مباشرة في

مواجهة محل الجريمة كشفرة الدخول الى النظام المعلوماتي وشفرة الدخول للملفات قراءتها وتعديل مضمونها أو محوه، وقد تنحصر هذه السلطة في مجرد حق الدخول الى اماكن التي تحتوي على هذه الأنظمة[1].

فهناك مجرمي المعلوماتية يطلق عليهم المتطفلون (الهاكرز)، وهم يقومون عادة بتحدي إجراءات أمن النظم والشبكات وباعثهم لارتكاب الجريمة يكون عادة التحدي وإثبات الذات والقدرة أما المخترقون (الكراكرز) فهم على النقيض من ذلك فهم يميلون للتخريب والتدمير فقد يكون الباعث من نشاطهم تدمير عمل المنشأة التي كانوا أو لا يزالوا يعملون بها بغرض الانتقام على سبيل المثال.

وهناك مجرمون محترفون حيث تتحقق لدى هذه الفئة الخبرة والعلم بماهية التقنية المعلوماتية وأوجه قصورها وعادة ما يكون باعثهم من ارتكاب الجرائم هو الباعث المادي أو لتحقيق مكاسب معنوية كالحصول على معلومات بغرض تحقيق أهداف سياسية.

الفرع الثاني: أركان الجريمة المعلوماتية

لقيام أي جريمة في القانون فانه يجب أن تتحقق أركانها العامة، والأركان العامة للجريمة هي الاركان التي تسري على الجرائم بشكل عام باختلاف نوع وطبيعة هذه الجرائم فبمجرد تحققها على النحو الذي تطلبه المشرع فانه يستلزم ايقاع العقوبة المتصلة بهذا الموضوع

[1] حسين ربيعي، المجرم المعلوماتي (شخصيته و أصنافه) مجلة العلوم الإنسانية، جامعة محمد خيضر بسكرة، عدد40، جوان 2015، ص 290.

أولا: مبدا شرعية الجريمة والعقوبة

إن مبدا شرعية الجريمة والعقوبة يعني ان القاضي الجنائي لا يملك خلق جريمة جديدة أو تقرير عقوبة جديدة لجريمة قائمة وإنما لتحقق ذلك يجب صدور تشريع بذلك ولا يمكن ملاحقة الشخص عن فعل ارتكبه قبل صدور نص التجريم أو عن فعل ارتكبه بعد الغاء نص التجريم.

ثانيا: الركن المادي للجريمة

الركن المادي من اي جريمة يتحقق بتوافر سلوك يؤتيه الفاعل ويكون معاقبا عليه في القانون أو الامتناع عن إتيان فعل، و تتحقق نتيجة ضارة من جراء هذا السلوك أي تتوافر علاقة سببية بين هذا السلوك و ما نتج عنه من ضرر، فلا يكفي الاعتقاد الجرمي وانصراف نية الجاني لارتكاب السلوك الإجرامي وإنما يجب أن يترجم الاعتقاد إلى سلوك مادي له طبيعة مادية ملموسة .

فالسلوك الإجرامي في الجريمة المعلوماتية عادة ما يبدا بضغطة زر أو لمسة يد على شاشة الهاتف أو الحاسب الآلي على اختلاف أنواعه، فعلى سبيل المثال عندما يقوم المجرم المعلوماتي بالدخول للشبكة والتعارف على الأشخاص بعد انتحال شخصية أو صفة تتناسب مع ما يدعيه ككونه مستثمرا أو تاجرا للحصول على مبالغ نقدية دون وجه حق من الأشخاص الذين تعاملوا معه من خلال الشبكة المعلوماتية، فالفعل هنا يتحدد بالإرسال وحدوث الضرر من جراء ما تم إرساله.

ثالثا : الركن المعنوي

لا يكفي للقول بان المسؤولية الجنائية قائمة من الناحية القانونية ان يصدر من الجاني سلوك[1] اجرامي ذو مظهر مادي وإنما يلزم أيضا توافر الركن المعنوي، فيجب أن تكون هناك

[1] حنان ريحان مبارك المضحكي، الجرائم المعلوماتية، ط1، منشورات الحلبي الحقوقية، لبنان، 2014، ص 42.

علاقة نفسية بين السلوك الإجرامي وإرادة الجاني المتجهة إلى جعل النتيجة الغير مشروعة كأثر لفعله الإجرامي وهو الخطأ العمدي ويجب أن يدرك الجاني أنه يقوم بعمل غير مشروع وأن تكون لديه حرية الاختيار المطلقة للقيام بهذا السلوك الإجرامي

أما الخطأ الغير عمدي فهو ناتج عن الإهمال وعدم الاحتياط كونها لا تتطلب في الجاني توافر الإرادة للقيام بالسلوك الإجرامي، ويتحقق القصد الجرمي في الجرائم العمدية بتحقق عنصري العلم والإرادة، فالعلم يتحقق بالعلم بكافة العناصر المكونة للجريمة أما عنصر الإرادة تتمثل في القوة النفسية التي تحرك كل أعضاء الجسم أو بعضه لتحقيق هدف غير مشروع ومعاقبته عليه قانونا[1].

[1] حنان ريحان مبارك المضحكي، المرجع السابق، ص ص ،57، 93.

المبحث الثاني : أساليب الوقاية من الجرائم المعلوماتية

عندما ازداد انتشار الجرائم المعلوماتية كان على التشريعات وضع قوانين للحد منها فظهرت قوانين ومراسيم للوقاية منها وطنيا (الفرع الأول من المطلب الأول) أما من بين الدول العربية نجد الإمارات العربية المتحدة التي واجهت هذا النوع من الجرائم (الفرع الثاني من المطلب الأول) أما دوليا (المطلب الثاني) نجد المنظمة الدولية للشرطة الجنائية(الفرع الأول) والاتحاد الدولي للاتصالات (الفرع الثاني).

المطلب الأول: سبل الوقاية على المستوى الوطني والدول العربية (الجزائر/الإمارات العربية المتحدة)

سنتطرق الى التدابير الوقائية على مستوى الجزائر من خلال قوانين العامة والخاصة بالإضافة الى الإمارات العربية المتحدة من خلال قانون مكافحة الجرائم المعلوماتية المتعلق بها.

الفرع الأول: سبل الوقاية على المستوى الوطني

عرفت الجزائر خطر الجريمة المعلوماتية، فسنت تشريعات متعلقة بمحاربة الجريمة المعلوماتية ومواكبة التشريعات الغربية[1]، من بينها نذكر ما يلي:

القانون رقم 2000-03 المؤرخ في 5أوت2000 المتعلق بالقواعد العامة للبريد والمواصلات السلكية واللاسلكية .

[1] عبدالرحمان نشادي، الجرائم المعلوماتية في وسائل الاتصال الحديثة، أطروحة لنيل شهادة الدكتوراه، في علوم الإعلام والاتصال، كلية الإعلام والاتصال، جامعة الجزائر3، 2016-2017، ص 189.

قد وضع هذا القانون القواعد التي تنظم مختلف شبكات المواصلات السلكية واللاسلكية مهما كانت الوسيلة المستعملة سواء أسلاك بصريات أو لاسلكي كهربائي أو أجهزة أخرى كهربائية مغناطيسية (م 18-21)[1].

القانون رقم 09-04 المؤرخ في 14 شعبان 1430 الموافق 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها (سيتم التفصيل فيه في الفصل الثاني)

القانون رقم 05-10 المؤرخ في 20 جوان 2005 المعدل والمتمم للأمر رقم 75-58 المتضمن القانون المدني فيما يخص الاعتراف بالكتابة الإلكترونية كوسيلة إثبات حيث

نصت المادة 323 مكرر 1 "يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها"[2].

القانون رقم 04-14 المؤرخ 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية (الجريدة الرسمية عدد 71 بتاريخ 10 نوفمبر 2004) تنشا لدى وزارة العدل مصلحة لنظام الي وطني لصحيفة السوابق القضائية مرتبطة بالجهات القضائية.

القانون رقم 18-05 المؤرخ في 24 شعبان عام 1439 الموافق 10 مايو2018 يتعلق بالتجارة الالكترونية .

[1] مختار الاخضري، الاطار القانوني لمواجهة جرائم المعلوماتية وجرائم الفضاء الإفتراضي، المجلة القضائية، المديرية العامة للشؤون القضائية والقانونية، العدد 66، 2010، ص66.

[2] عبدالرحمان نشادي، المرجع السابق، ص 189.

القانون رقم 15-04 المؤرخ في 1 فيفري 2015 المتضمن تحديد القواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين.

القانون رقم 18-07 المؤرخ في 25 رمضان 1439 الموافق 10 يونيو 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

القانون رقم 06-22 الصادر في 20 ديسمبر 2006 المعدل و المتمم لقانون الإجراءات الجزائية . (سنفصل فيه في الفصل الثاني)

الأمر 03-05 المؤرخ في 19 يوليو2003 المعدل والمتمم للأمر 97-10 المتعلق بحقوق المؤلف والحقوق المجاورة والأمر رقم 03-07 المؤرخ في 19 جويلية 2003 متعلق ببراءة الاختراع (الجريدة الرسمية العدد 44 بتاريخ 23 يونيو 2003)، (سيتم التفصيل فيهما في الفصل الثاني).

الأمر رقم 03-07 المؤرخ في 19 جويلية 2003 متعلق ببراءة الاختراع (الجريدة الرسمية العدد 44 بتاريخ 23 يونيو 2003)[1].

المرسوم التنفيذي رقم 98-256 المؤرخ في 25 أوت 1998 المعدل والمتمم للجزء التنظيمي من الأمر 75-98 المؤرخ في 1975/12/30 المتضمن قانون البريد والمواصلات الذي عرف خدمات الإنترنت وشروط ممارسة مقدمي الخدمة ومستضيفي المواقع لنشاطهم و العديد من الأحكام الأخرى[2].

الفرع الثاني : سبل الوقاية على المستوى الدول العربية(الإمارات العربية المتحدة)

نص القانون الإتحادي رقم 2 لسنة 2006 نص على تجريم أفعال التالية.

[1] عبدالرحمان نشادي، المرجع السابق، ص 192.

[2] مختار الأخضري، المرجع السابق، ص 66.

أولا: الجرائم التي نص عليها نظام مكافحة جرائم تقنية المعلومات الحديثة في الإمارات العربية المتحدة

1- جريمة إختراق المواقع و الأنظمة الإلكترونية

عاقب هذا القانون على جريمة اختراق المواقع وأنظمة المعلومات، وفرد لتلك الجريمة أنواعا من العقوبة تتدرج وفقا لحالات أربع:

حالة القيام بالفعل دون ترتب نتيجة، حالة القيام بالفعل مع ترتب نتيجة متعلقة بإلغاء أو حذف أو تدمير معلومات، حالة القيام بالفعل مع ترتب نتيجة متعلقة بانتهاك معلومات شخصية، حالة القيام بالفعل أثناء أو بسبب العمل أو تسهيل للغير مهمة القيام بهذا الفعل.

2- جريمة تزوير مستندات معترف بها في نظام معلوماتي.

يعاقب هذا القانون كل من زور مستندا من مستندات الحكومة الإتحادية أو المحلية أو الهيئات أو المؤسسات العامة الإتحادية والمحلية المعترف به قانونا في نظام معلوماتي.

3- جريمة تعطيل الوصول إلى الوسائل أو البرامج أو المعلومات أو الشبكات المتعلقة بتقنية المعلومات[1].

يعاقب هنا كل من أعاق أو عطل الوصول إلى الخدمة أو الدخول إلى الأجهزة أو البرامج أو مصادر البيانات أو المعلومات بأية وسيلة كانت عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات.

4-جريمة العبث بالشبكة المعلوماتية أو إحدى وسائل التقنية والتي يترتب عليها ضرر موصوف يعاقب كل من أدخل عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية

[1] علي جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، ط1، منشورات زين الحقوقية، بيروت، 2013، ص 161.

المعلومات، ما من شأنه إيقافها عن العمل أو تعطيلها أو تدمير أو مسح أو حذف أو اتلاف أو تعديل البرامج أو البيانات أو المعلومات[1].

5-جريمة العبث بالفحوص الطبية باستخدام الإنترنت أو إحدى وسائل تقنية المعلومات يقصد بها كل من أتلف الفحوص الطبية أو التشخيص الطبي أو العلاج الطبي أو الرعايا الطبية أو سهل للغير فعل ذلك أو مكنه منه باستعمال شبكة المعلوماتية أو إحدى وسائل تقنية المعلومات.

6- جريمة التنصت باستخدام الإنترنت أو إحدى وسائل تقنية المعلومات أي كل من تنصت أو التقط أو اعترض عمدا من دون وجه حق.

7-جريمة التهديد باستخدام الإنترنت أو إحدى وسائل تقنية المعلومات أي التهديد أو الابتزاز لشخص آخر وإلزامه على القيام بالفعل أو الامتناع عنه.

8- جريمة السرقة والاحتيال والإستيلاء على البطاقات الإلكترونية باستخدام الانترنت أو إحدى وسائل تقنية المعلومات.

9- جريمة المساس بالآداب العامة و التحريض على الدعارة باستخدام الإنترنت أو إحدى وسائل تقنية المعلومات.

10- جريمة العبث بالمواقع الإلكترونية على الإنترنت فيعاقب كل من دخل، بدون وجه حق، موقعاً في الشبكة المعلوماتية لتغيير تصاميم هذا الموقع أو إلغائه أو إتلافه أو تعديله.

11-جرائم المس بالأديان باستخدام الانترنت أو إحدى وسائل تقنية المعلومات.

12- جريمة إنتهاك حرمة الحياة الخاصة عن طريق الإنترنت أو إحدى وسائل تقنية المعلومات، فيعاقب هذا القانون كل من اعتدى على أي من المبادئ أو القيم الأسرية أو

[1] عبد الله عبدالكريم عبدالله، جرائم المعلومات والانترنت ،ط1، منشورات الحلبي الحقوقية ، لبنان، 2007، ص 68.

نشر أخبارا أو صورا تتصل بحرمة الحياة الخاصة أو العائلية ولو كانت صحيحة عبر الشبكة المعلوماتية إحدى وسائل تقنية المعلومات.

13- جريمة الإتجار بالبشر عبر الإنترنت يعاقب كل من أنشأ موقعاً أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، بقصد الإتجار في الأشخاص أو تسهيل التعامل فيه.

14- جريمة الإتجار بالمخدرات عبر الإنترنت فيعاقب كل من أنشا موقعا أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، بقصد ترويج المخدرات أو المؤثرات العقلية وما في حكمها أو تسهيل التعامل فيهما و ذلك في غير الأحوال المصرح بها قانون.

15- جريمة غسل الأموال عبر الإنترنت، فيعاقب كل من قام بتحويل الأموال غير المشروعة أو نقلها أو تمويه المصدر غير المشروع لها أو إخفائه أو قام باستخدام أو اكتساب وحيازة الأموال مع العلم بأنها مستمدة من مصدر غير مشروع أو بتحويل الموارد أو الممتلكات مع العلم بمصدرها غير المشروع، وذلك عن طريق استخدام الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات بقصد إضفاء الصفة المشروعة على تلك الأموال أو أنشأ أو نشر معلومات أو موقعا لارتكاب أي من هذه الأفعال. [1]

16- جريمة إنشاء مواقع إلكترونية مخالفة للنظام العام والآداب أو استخدام وسائل تقنية المعلومات لهذه الغاية، فكل من أنشأ موقعاً أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات لأية مجموعة تدعو لتسهيل وترويج برامج وأفكار من شأنها الإخلال بالنظام العام والآداب العامة.

[1] القانون الاتحادي رقم2 لسنة 2006 في شان مكافحة جرائم تقنية المعلومات، منشور في العدد رقم 442 من الجريدة الرسمية لدولة الإمارات العربية المتحدة.

17- الجرائم الإرهابية عبر أو باستخدام وسائل تقنية المعلومات كل من أنشأ موقعاً أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات لجماعة إرهابية تحت مسميات تمويهية لتسهيل الاتصالات بقياداتها أو أعضائها، أو ترويج أفكارها أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة أو المتفجرة، أو أية أدوات تستخدم في الأعمال الإرهابية.[1]

18- جريمة الحصول على معلومات حكومية سرية باستخدام الانترنت فيعاقب كل من دخل وبغير وجه حق موقعاً أو نظاماً مباشرة أو عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات بقصد الحصول على بيانات أو معلومات حكومية سرية إما بطبيعتها أو بمقتضى تعليمات صادرة بذلك

19- جرائم التحريض أو التدخل في الجرائم السابق ذكرها في هذا القانون يعاقب كل من حرض أو ساعد أو اتفق مع الغير على ارتكاب جريمة من الجرائم المنصوص عليها في هذا القانون ووقعت الجريمة بناء على هذا التحريض أو المساعدة أو الاتفاق يعاقب بذات العقوبة المقررة لها[2].

المطلب الثاني: سبل الوقاية على مستوى المنظمات الدولية

تشكل الجريمة المعلوماتية خطرا على معظم سكان العالم فهي تهدد المجتمعات الصناعية والمتقدمة كما أنها تعيق التنمية الاقتصادية والاجتماعية في الدول النامية، كل هذا أدى الى ضرورة التعاون الدولي لمواجهة هذه الجرائم من بينهم المنظمة الدولية للشرطة الجنائية (الانتربول) والاتحاد الدولي للاتصالات[3].

[1] عبدالله عبدالكريم عبدالله، المرجع السابق، ص 76.

[2] علي جعفر، المرجع السابق، ص 164.

[3] عبدالكريم الردايدة، الجرائم المستحدثة، ط1، دار الحامد، الأردن،2013، ص 230.

الفرع الأول : الاتحاد الدولي للاتصالات(UIT)

هو وكالة متخصصة تابعة للأمم المتحدة يلعب دورا رئيسيا في توحيد وتطوير الاتصالات وقضايا الأمن السيبراني.

يزعم مؤتمر القمة العالمي للمجتمع المعلومات الذي عقد في جزأين في جنيف سويسرا سنة 2003 وفي تونس سنة 2005 يقاسم المقررون والخبراء حكومات من مختلف انحاء العالم الافكار والخبرات حول افضل طريقه للتعامل مع المشاكل الجديد التي تتعلق بتطور المجتمع العالمي للمعلومات، بما في ذلك تطوير المعايير والقوانين المتوافقة.

فنتائج القمة الواردة في إعلان مبادئ جنيف هي خطة عمل مؤتمر تونس بشان مجتمع المعلومات وتؤكد على أهمية خطة عمل جنيف بخصوص تدابير مكافحة الجريمة المعلوماتية.

الجزء الثاني من القمة في تونس عام 2005 كان أيضا فرصة لدراسة مشكلة جرائم المعلومات.

ويؤكد برنامج عمل تونس بشان مجتمع المعلومات الحاجة للتعاون الدولي في مجال مكافحة الجرائم المعلوماتية يذكر بالنهج (المقاربات) التشريعية والقرارات القائم بما في ذلك القرارات

التي اتخذت الجمعية العامة للأمم المتحدة واتفاقية مجلس اوروبا بشان جرائم المعلوماتية في المقتطف الاتي:[1]

"و نؤكد كم هو مهم متابعة مرتكبي جرائم المعلوماتية، بما في ذلك المرتكبة في البلاد، لكن العواقب يشعر بها في بلد آخر، نحن نصر أيضا على الحاجة الى ادوات واليات فعالة على المستوى الوطني والدولي لتعزيز التعاون الدولي لاسيما بين الشرطة والعدالة في مجال

[1] عبدالرحمان الرشادي، المرجع السابق، ص 175.

معلومات في الجرائم المعلوماتية ونحن نحث الدول على وضع التشريعات اللازمة للتحقيق في جرائم المعلوماتية ومقاضاة مرتكبي هذه الجرائم بالتعاون مع اصحاب المصلحة الاخرين مع مراعاة الاطر القائمة مثل قرارات الجمعية العامة للأمم المتحدة حول مكافحة استغلال لتكنولوجيا المعلومات الاتصالات لأغراض إجرامية والمبادرات الإقليمية بما في ذلك اتفاقيه مجلس أوروبا بشان الجرائم المعلوماتية".[1]

الفرع الثاني: المنظمة الدولية للشرطة الجنائية (الإنتربول)

يشكل الإنتربول ببلدانه الأعضاء، أكبر منظمة عالمية للشرطة الجنائية فيمكن أجهزة الشرطة في العالم من العمل معا لجعل العالم أكثر أمانا وتساعد البنية التحتية المتطورة للدعم الفني والميداني التي تملكها المنظمة على مواجهة التحديات المتنامية في مجال مكافحة الجريمة المنظمة العابرة للحدود[2].

فتتكون الجمعية العامة من الدول الأعضاء في المنظمة الدولية للشرطة الجنائية، وهي أعلى سلطة تشريعية فهي التي وضعت الدستور الخاص بالمنظمة، ولا تملك أي جهة أخرى تعديله سوى هذه الجمعية العامة حيث يتم تشكيل وفد كل دولة بقرار من سلطات الدولة العضو، ويضم غالبا رئيس المكتب المركزي للشرطة الجنائية في تلك الدولة العضو إضافة إلى بعض قيادات الشرطة في نفس الدولة والمعنية بأمر متابعة الجريمة وضبط فاعلها وليس هناك عدد محدد الأعضاء لكل وفد[3].

في سنة1923 تم تأسيس منظمة الإنتربول وهو المنظمة الشرطية الدولية الأكبر في العالم ببلدانه الدول الأعضاء البالغ عددها 194 دولة.

[1] عبدالرحمان نشادي، المرجع السابق، ص 176.

[2] وافية ديوبي، المرجع السابق، ص 24.

[3] عبدالكريم الردايدة، المرجع السابق، ص 238.

وللأمانة العامة في ليون (فرنسا) ستة مكاتب إقليمية فرعية، مكتب ارتباط واحد، ومكتبا ممثل الإنتربول الخاص لدى الأمم المتحدة ولدى الاتحاد الأوروبي في بروكسل، ومكتب مركزي وطني في كل بلد عضو[1].

وتهدف المنظمة إلى تيسير التعاون الشرطي بين الدول، ومساعدة السلطات والأجهزة والمنظمات المعنية في الوقاية من الجريمة ومكافحتها على القيام بدورها على أكمل وجه، بالإضافة إلى تنسيق التعاون الدولي من خلال العلاقات الدبلوماسية بين الدول الأعضاء في حدود القوانين القائمة في كل دولة، حيث تعد هذه المنظمة من المنظمات الدولية التي تثبت وجودها وقدرتها العمل في مكافحة الجريمة على المستوى الدولي، من حيث ملاحقة مرتكبي الجرائم ذات الصفة الدولية وتقديمهم للمحاكمة وإيقاع العقاب عليهم، الأمر الذي يتطلب كل التعاون الدولي والمساعدة المتبادلة بهدف تحقيق السرعة والفاعلية في إجراءات ملاحقة وعقاب مرتكبي هذه الجرائم.

تتسم طبيعة عمل الإنتربول الدولي بالصفة الاجتماعية البحتة، حيث قيدت المادة الثالثة من دستور المنظمة على أنه (ممنوع على المنظمة أن تقوم بأي تدخل أو نشاط له طابع سياسي أو عسكري أو ديني أو عنصري) وإنما تنحصر أهداف المنظمة وفقا لما بينته المادة الثانية ن الدستور في تأكيد القوانين القائمة وبروح الإعلان العالمي لحقوق الإنسان وإقامة وتنمية النظم التي من شانها أن تسهم على نحو فعال ف منع ومكافحة الجرائم وتتبع مرتكبيها ومن هذه الجرائم جرائم الإرهاب والإتجار غير المشروع بالمخدرات والإتجار في الرقيق والاغتيال والسرقة ... وما إلى ذلك[2].

[1] وافية ديوبي، المرجع السابق، ص 25.

[2] عبدالكريم الردايدة، المرجع السابق، ص 240.

ومن بين إستراتيجيات هذه المنظمة تنسيق الموارد الميدانية في التحقيقات الجارية في مجال تكنولوجيا المعلومات بالتعاون مع بلدان الأعضاء، ففي مارس 2008 طلبت كولومبيا من

الإنتربول إجراء فحوص أدلة جنائية مستقلة على أجهزة ومعدات كمبيوترية ضبطت خلال عملية مكافحة المخدرات والإرهاب نفذت ضد معسكر للقوات المسلحة الثورية الكولومبية الفارك، وذلك لتحديد ما إذا كان قد جرى التلاعب بمضمون أي من المعدات بعد ضبطها.

وتم إجراء دراسة فنية مستقلة من طرف فريق خبراء الأدلة الجنائية التابع للإنتربول و أصدر تقريرا خلص إلى غياب أي دليل يشير إلى تعديل ملفات المستخدمين أو تحريفها أو الإضافة عليها أو حذفها.

انضمت الجزائر إلى المنظمة الدولية للشرطة الجنائية (إنتربول) في شهر أوت 1963 بناءا على طلب تقدمت به السطات الجزائرية والذي حظي بمصادقة أغلبية الدول المجتمعة والتي كان عددها آنذاك 51 دولة وذلك بمناسبة إنعقاد الجمعية العامة للمنظمة بهلسنكي/فنلندا في دورتها العادية.[1]

[1] وافية ديوبي، المرجع السابق، ص 25.

الفصل الثاني

آليات مكافحة الجريمة المعلوماتية في القانون الجزائري والاتفاقيات الدولية

الفصل الثاني:اليات مكافحة الجريمة المعلوماتية في القانون الجزائري والإتفاقيات الدولية

تطورت الجرائم من تقليدية إلى معلوماتية وأصبحت تهدد الأفراد والدول وحتى يتداركوا هذه الجرائم كان لزاما عليهم بمواجهتها ومكافحتها لأنها أثرت سلبا عليهم و أصبحت الدول غير قادرة على حماية أفرادها وتحقيق لهم الأمن والإستقرار لذلك وضعت نصوص قانونية تجرم هذه الأفعال ووضعت عقوبات لها.

وهذا ما سنتعرف عليه من خلال هذا الفصل حيث تطرقنا في المبحث الأول إلى الجوانب الموضوعية في نصوص الجريمة المعلوماتية أما المبحث الثاني خصصناه للأساليب الإجرائية لنصوص الجريمة المعلوماتية في الاتفاقيات الدولية والقانون الجزائري.

المبحث الأول: الجوانب الموضوعية في نصوص الجريمة المعلوماتية

عالج المشرع الجزائري الجرائم المعلوماتية في العديد من القوانين لكن سنسلط الضوء على أهم هذه القوانين فسوف نتعرض في هذا المبحث إلى للحماية الجزائية للمعلوماتية من جانبه الموضوعي، من خلال قانون العقوبات الجزائري ونصوص الملكية الفكرية والصناعية .

المطلب الأول: الحماية الجزائية للجريمة المعلوماتية في ظل قانون العقوبات الجزائري

نص قانون العقوبات الجزائري على الجريمة المعلوماتية وقد وضع لها صورتين فقد تكون بسيطة وقد تكون مشددة، ولها أركان مثل باقي الجرائم وليس ذلك فقط بل وضع عقوبات محددة على حسب كل جريمة وهذا ما سنبيّنه من خلال هذا المطلب.

الفرع الأول: مفهوم نظام المعالجة الآلية للمعطيات

تعدت تعاريف نظام المعالجة الآلية للمعطيات الذي يعتبر بمثابة الشرط الأول الذي يلزم تحققه حتى نبحث فيما بعد ما إذا كان هناك إعتداء على هذا النظام من عدمه.

أولا: تعريف نظام المعالجة الآلية

عرفه مجلس الشيوخ الفرنسي بأنه " كل مركب يتكون من وحدة أو مجموعة وحدات معالجة، تتكون منها كل من الذاكرة والبرامج والمعطيات وأجهزة الإدخال والإخراج، وأجهزة الربط، التي يربط بينها مجموعة من العلاقات التي عن طريقها يتم تحقيق نتيجة معينة وهي معالجة المعطيات على أن يكون هذا المركب خاضعا لنظام المعالجة الفنية"[1].

أما جانب من الفقه يعرف نظام المعالجة الآلية للمعطيات بأنها: "علم قائم بذاته وبالمختصر فإن كلمة معلوماتية هي مزج مختصر لكلمتين معلومة وكلمة آلية ومعناها المعالجة الآلية للمعلومة ويفهم من المعطيات الفكرية المعالجة اليا هي عمل البرامج

[1] آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، ط2، دار هومة، الجزائر، 2007، ص ص 100،102.

والبيانات الموجودة في الكمبيوتر وعلى شبكة الأنترنت سواء كانت فنية أو أدبية أو علمية أو تجارية أو صناعية فهي تصنف كإنتاج ذهني لأصحابها .[1]

كما قدمت الإتفاقية الدولية للإجرام المعلوماتي تعريفا للنظام المعلوماتي في مادتها الأولى على النحو التالي:

"Système informatique désigne tout dispositif isolè ou ensemble de dispositifs interconnectè ou apparentès , qui assure ou dont un ou plusiers èlèment assurent, en exècution d'un programme, un traitement automatisè de donnèes[2]"

وقد تبنى المشرع الجزائري هذا التعريف و أطلق عليه اسم المنظومة المعلوماتية[3]، التي عرفها في المادة 2/ ب من القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها بأنها :" أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين[4]".

بناءا على التعريفات السابقة، نلخص إلى أن تعريف نظام المعالجة الآلية للمعطيات يعتمد على عنصرين هما:[5]

يتكون من عناصر مادية ومعنوية التي يتكون منها المركب مثل الذاكرة، البرامج، المعطيات، أجهزة الربط.... الخ، وبما أن هذه العناصر واردة على سبيل المثال لا الحصر

---

[1] زيبحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، ب ط، دار الهدى، الجزائر،2011، ص 48.

[2] امال قارة، المرجع السابق، ص 101 .

[3] مختارية بوزيدي، ماهية الجريمة الالكترونية، الملتقى الوطني حول آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري،29 مارس 2017، مركز جيل البحث العلمي الجزائر،ص 12.

[4] القانون رقم 09-04 المؤرخ في 14شعبان عام 1430الموافق ل 5 غشت سنة 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها ج ر عدد 47.

[5] محمد قسمية، الجرائم الماسة بنظام المعالجة الآلية للمعطيات وأطر مكافحتها في قانون العقوبات الجزائري، مؤلف جماعي حول مواجهة الجريمة المعلوماتية، جامعة محمد بوضياف بالمسيلة، ب ع، المنشورات العلمية لكلية الحقوق والعلوم السياسية، أكتوبر 2019، ص 300.

فإن ذلك يفتح المجال لإضافة عناصر جديدة أو حذف بعضها حسبما يستوجبه التطور التقني في هذا المجال.

أما العنصر الفني هو ضرورة خضوع النظام لحماية فنية فالرأي الغالب في الفقه الفرنسي، يرى أن هذا الشرط ليس ضروريا لأن وجوده لا يكون له سوى دور واحد وهو إثبات سوء النية من قام بانتهاك النظام و الدخول إليه بطريقة غير مشروعة ويدخل في ذلك إثبات القصد الجنائي[1]، وبالرجوع إلى التشريع الجزائري نجد أن النصوص المتعلقة بجرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات جاءت خالية من شرط الحماية فإرادة المشرع توجهت إلى استبعاد هذا الشرط لتشمل الحماية الجنائية كل الأنظمة سواء كانت تتمتع بحماية فنية أم لا.

الفرع الثاني: صور الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات

سعى المشرع الجزائري من خلال تعديل قانون العقوبات إلى حماية المصالح المتعلقة بمعطيات الحاسب الآلي وهو ما سنتطرق إليه فهناك الجريمة في صورتها البسيطة وفي صورتها المشددة[2].

أولا: جريمة الدخول أو البقاء غير المصرح بهما بصورتهما البسيطة

لمعاقبة الجاني على إتيان فعل ما ونكون أمام تصرف يعاقب عليه القانون، لابد من توفر الأركان الأساسية للجريمة وهي الركن الشرعي والركن المادي والركن المعنوي.

1) الركن الشرعي

جرم المشرع الجزائري هذه الجريمة في المادة 394 مكرر من قانون العقوبات الجزائري في فقرتها الأولى إذ تنص على "يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من

[1] مختارية بوزيدي، المرجع السابق، ص 13.

[2] محمد قسمية، المرجع السابق، ص 301.

50.000 دج إلى 200.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك."

فتعتبر جريمة الدخول أو البقاء غير المصرح بهما في أنظمة المعالجة الآلية للمعطيات هي من أهم جرائم المعطيات والجرائم المعلوماتية عموما، لأن أغلب جرائم المعطيات لا يمكن ارتكابها إلا بعد الدخول للنظام، فجريمة الدخول هي الباب والحد الفاصل بين الجاني وبين ارتكابه لمختلف جرائم المعطيات الأخرى، لذا حرص المشرع على تجريم كل تواجد غير مشروع داخل أنظمة المعالجة الآلية للمعطيات فجرم الدخول غير مصرح به.

وكذا البقاء بغير تصريح سواء تم ذلك في كل نظام أو جزء منه، كما تتحقق الجريمة سواء أدى هذا التواجد أم لم يؤدي إلى نتائج معينة.

2) الركن المادي

يتمثل السلوك الإجرامي في جريمة الدخول والبقاء غير المصرح بهما في نشاط إجرامي إما في فعل الدخول إلى نظام المعالجة الآلية للمعطيات أو في جزء منه وإما في فعل البقاء في هذا النظام أو في جزء منه.

أ) فعل الدخول إلى نظام المعالجة الآلية للمعطيات

ويقصد بالدخول هنا هو الولوج إلى المعلومات والمعطيات المخزنة داخل النظام فهو ذو طبيعة معنوية وليست مادية[1] فلا يقصد به الدخول إلى المكان الذي يوجد به الحاسوب ونظامه بل يقصد الدخول باستعمال الوسائل الفنية والتقنية إلى النظام المعلوماتي[2].

ولم يحدد المشرع الجزائري الوسيلة المتبعة في الدخول إلى النظام لذلك تقع الجريمة أيا كانت الوسيلة المستعملة في ذلك، ويستوي أن يتم الدخول مباشرة أم بطريقة غير مباشرة،

[1] محمد قسمية، المرجع السابق، ص 301.

[2] نجاة بن مكي، المرجع السابق، ص 179.

كما هو الحال في الدخول عن بعد عن طريق شبكات الاتصال سواء كانت محلية أو عالمية.

وينصرف معنى الدخول في إطار المعلوماتية ليشمل كافة الأفعال التي تسمح بالولوج إلى نظام معلوماتي، ويتحقق الدخول غير مصرح به إلى جهاز الكمبيوتر بالوصول إلى المعلومات والبيانات المخزونة داخل نظام الكمبيوتر دون رضا المسؤول عن النظام أو المعلومات التي يحتوي عليها، فقد يتم الدخول باستعمال أجهزة خاصة تمكنه من كسر شفرة قاعدة المعطيات أو أن يستخدم الشفرة الصحيحة الخاصة بشخص آخر مأذون له بالدخول، وقد يتم ذلك عن طريق استخدام تقنية معينة حيث يقوم واضعو البرامج بترك فواصل في البرامج أثناء إعدادها تسمى أبواب المصيدة تستخدم في إضافة ما يحلو لهم من أوجه التلاعب ويتم ذلك أثناء قيامها بالمعالجة النهائية على اعتبار أن هذا الشيء عادي إذ يمكن لمهندسي الحاسب أن يقوموا باكتشاف هذه الفواصل من أجزاء داخلية للصيانة.

ويستوي أن يتم الدخول إلى قواعد البيانات كلها أو إلى جزء فقط من نظام التشغيل، وتتحقق الصورة الأخيرة إذا تمكن الجاني من كسر شفرة بعض قواعد البيانات أو مواقع المعلومات دون أن يتمكن من اختراق كل مواقع النظام، ولا عبرة في هذه الجريمة بصفة مرتكب الفعل الإجرامي فقد يكون مسؤولا عن العمال والصيانة وقد يكون شخصا منبت الصلة عن النظام الداخل فيه وتوصل إلى الدخول عن طريق حاسب آلي آخر موجود في مكان آخر بواسطة الدخول إلى شبكة المعلومات، فعبرت عنه المادة 394 مكرر من قانون العقوبات بقولها "كل من يدخل أو يبقى[1]".

وبذلك يكفي أن يكون الجاني من الأشخاص الذين ليس لهم الحق في الدخول إلى النظام أو كان دخوله مخالفا لشروط الدخول المنصوص عليها قانونا أو اتفاقاً أو مخالفاً لإرادة من له حق السيطرة على النظام، كما هو الحال إذا كان القانون يفرض سرية معينة بالنسبة

[1] محمد قسمية، المرجع السابق، ص 302.

لبعض الأنظمة مثل أسرار الدولة كما يكون الدخول غير مشروع إذا كان من له حق السيطرة على النظام قد وضع بعض القيود للدخول إليه ولم يحترم الجاني تلك القيود، أو إذا كان يتطلب ضرورة دفع مبلغ من النقود وتم الدخول دون دفع ذلك المبلغ، وعلى ذلك لا تتوفر الجريمة إذا تم الدخول إلى عنصر لا علاقة له بنظام المعالجة الآلية للمعطيات كالدخول إلى برنامج منعزل عن غيره من العناصر، أو أن يقتصر الشخص على مجرد قراءة الشاشة[1].

ب) فعل البقاء في نظام المعالجة الآلية للمعطيات

يقصد به التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام، وقد يتحقق البقاء المعاقب عليه داخل النظام مستقلا عن الدخول إلى النظام كما قد يجتمعا، ويكون البقاء معاقبا عليه استقلالا حين يكون الدخول إلى النظام مشروعا ومن أمثلة ذلك إذا تحقق الدخول إلى النظام بالصدفة أو عن طريق الخطأ أو السهو، إذ كان يجب في هذه الحالة على المتدخل أن يقطع وجوده وينسحب فورا، فإذا بقي رغم ذلك، فإنه يعاقب على جريمة البقاء غير المشروع إذا توفر الركن المعنوي، ويكون البقاء أيضا جريمة في الحالة التي يستمر فيها الجاني باقيا داخل النظام بعد المدّة المحددة له البقاء داخله، أو في الحالة التي يطبع فيها نسخة من المعلومات في الوقت الذي كان مسموح له فيها الرؤية والاطلاع فقط[2].

فالنتيجة الإجرامية في الحالتين واحدة وهي الوصول للنظام غير مصرح للدخول إليه، فالمصلحة التي يحميها القانون هي حماية نظام الكمبيوتر في الحالتين، ويمكن أن يتحقق فعل البقاء وفعل الدخول معا إذا لم يرخص للشخص الدخول إلى نظام المعالجة الآلية

[1] محمد قسمية، المرجع السابق، ص 302.

[2] فيصل بدري، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة لنيل شهادة الدكتوراه تخصص قانون عام، كلية الحقوق، جامعة الجزائر 01 يوسف بن خدة، 2017-2018، ص ص 164، 165.

للمعطيات، وتختلف الطرق التي يستخدمها الجاني في الدخول غير المصرح به إلى جهاز الكمبيوتر ومثال ذلك طريق المختصرات، طرق القناع *...الخ[1].

ومن أمثلة الدخول غير المصرح به قضية (Riley) حيث قام بالدخول إلى مواقع لشركة الاتصالات للقيام بمكالمات هاتفية مجانية دون دفع الاشتراك وذلك بتخمين كلمة السر وفي هذه لا يوجد لمن قام بالدخول[2].

3) الركن المعنوي

جريمة الدخول إلى النظام المعلوماتي أو البقاء فيه من الجرائم العمدية التي تقوم بتوافر القصد الجنائي العام بعنصريه العلم والإرادة، حيث يتوجب أن يكون الجاني عالما بعدم أحقيته في الدخول أو البقاء في النظام المعلوماتي، وأن هذا الفعل مخالف لإرادة صاحب النظام، ومع ذلك يقوم بالدخول إلى النظام أو البقاء فيه، و أن يقوم بذلك الفعل بإرادته الحرة السليمة من أي عيب إذ قد ترتكب الجريمة من شخص واقع تحت الإكراه أو التهديد ...الخ، باستغلال مهاراته التقنية في الدخول لهذه الأنظمة وهذا يكون نافيا للمسؤولية الجنائية.

والملاحظ أن المشرع اشترط في المادة 394 مكرر أن يتم الدخول أو البقاء بطريقة الغش "... كل من يدخل أو يبقى عن طريق الغش "ويقصد بطريق الغش في هذه الحالة سوء نية الجاني حيث يعلم بأن دخول النظام أو البقاء فيه ليس من حقه ومع ذلك يقوم بالدخول، وتستخلص سوء نيته باختراقه لنظام الحماية الخاص بنظام المعالجة، وبالنسبة للبقاء فيستنتج من خلال العمليات والتصرفات التي قام بها الجاني داخل النظام ومع ذلك فإن الغش لا

[1]*طريق القناع: "يقوم المخترق باقناع الحاسوب أنه شخص مرخص له بالدخول". للمزيد انظر عبير بعقيقي، مكافحة الجريمة المعلوماتية في التشريعين الجزائري والإماراتي (دراسة مقارنة)، أطروحة لنيل شهادة الدكتوراه في الحقوق، تخصص النظام الجزائي والسياسة الجزائية المعاصرة، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، 2017-2018، ص 141.

[2]فيصل نسيغة وعبير بعقيقي، الاليات القانونية الموضوعية لمكافحة الجريمة المعلوماتية في التشريع الجزائري، مجلة الباحث للدراسات الأكاديمية، جامعة بسكرة ، عدد 11، جوان 2017، ص 190.

يظهر فقط من خلال عمليات خرق نظام الحماية وإنما أيضاً من خلال الدخول أو البقاء دون وجه حق و يعتبر نظام الحماية إلا وسيلة لإثبات سوء النية أو الغش.

ومن خلال تحليلنا للنص المتعلق بجريمة الدخول والبقاء غير المشروع للنظام المعلوماتي نلاحظ أن المشرع قد أحسن صنعا في صياغة هذه المواد[1].

ثانيا: الصورة المشددة (الحذف، التغيير أو التخريب كنتيجة للدخول أو البقاء غير المصرح بهما):

لقد سعى المشرع الجزائري إلى حماية المعطيات وإتاحتها في الصورة المشددة لجريمة الدخول أو البقاء غير المصرح بهما من خلال الفقرتين الثانية والثالثة من المادة 394 مكرر من ق ع ج حيث نجده وإن كان لا يتطلب نتيجة معينة لقيام جريمة الدخول أو البقاء غير المصرح بهما إلا أنه قد ضاعف العقوبة إذا أدى.

ذلك إلى نتائج معينة تتمثل في محو أو تعديل المعطيات التي يحتويها النظام كما شدد العقوبة إذا أدت الجريمة السابقة إلى تخريب نظام تشغيل المنظومة وجعله غير صالح لأداء وظائفه، ويكفي لتوافر هذا الظرف المشدد وجود علاقة سببية بين الدخول أو البقاء غير المصرح بهما وبين النتيجة الضارة سواء محو أو تعديل المعطيات التي يحتويها النظام، أما عدم صلاحية النظام للقيام بوظائفه فإنه يعني عدم قدرته على تنفيذ المعالجة الآلية للمعطيات بأن يصبح غير قابل للاستخدام ومثال ذلك محو بعض أوامر التشغيل الذي يترتب عليه تعطيل النظام.

وبالرجوع لنص المادة 394 مكرر/3/2 نجد أن النتيجة المشددة التي يتطلبها المشرع الجزائري لايشترط أن تكون مقصودة، فيكفي أن تكون على سبيل الخطأ غير العمدي الذي يأخذ صورة الإهمال أو عدم الإحتراز أو الرعونة.

[1] عبدالوهاب مليايني، أمن المعلومات في بيئة الأعمال الإلكترونية، رسالة لنيل شهادة الدكتوراه في القانون العام، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد تلمسان، 2016-2017، ص 185.

فالظرف المشدد هنا ظرف مادي يكفي أن توجد بينه وبين جريمة الدخول أو البقاء غير المصرح بهما علاقة سببية للقول بتوافره إلا إذا أثبت الجاني انتفاء تلك العلاقة كأن يثبت أن تعديل أو محو المعطيات أو عدم صلاحية النظام للقيام بالوظائف يرجع للقوة القاهرة أو لحادث مفاجئ.

ثالثا: الجرائم الماسة بسلامة المعالجة الآلية للمعطيات

قام المشرع الجزائري بتأمين الحماية اللازمة لضمان سلامة معطيات الحاسب الآلي من خلال تجريمه لبعض الأفعال التي تشكل تلاعبا بتلك المعطيات وقد وردت في المادة 394 مكرر1 من ق ع ج ونجد أن النشاط الإجرامي يرد على محل أو موضوع محدد هو المعطيات تمت معالجتها آليا والمتواجدة داخل نظام أو تشكل جزءا منه، وفيما يلي بيان الأفعال التي تعد تلاعبا في المعطيات :

1)الإدخال: أي إضافة معطيات جديدة على الدعامة الخاصة بها سواء كانت خالية أم كان يوجد عليها معطيات من قبل، كاستخدام بطاقات السحب الممغنطة ليسحب بمقتضاها النقود من أجهزة السحب الآلي باستخدام الرقم السري للدخول لسحب مبلغا من النقود أكثر من المبلغ الموجود في حسابه[1]، كما يتحقق فعل الإدخال في كل حالة يتم فيها إدخال برنامج غريب كفيروس* مثلا أو أي قنبلة معلوماتية* يؤدي لإضافة معطيات جديدة.

[1]قسمية محمد، المرجع السابق، ص 306.

*فيروس: "هي برامج تتكون من عدة أجزاء مكتوبة بإحدى لغات البرمجة بطريقة خاصة تسمح لها بالتحكم في البرامج الأخرى".

* القنابل المعلوماتية: "عبارة عن برامج صغيرة يتم إدخالها بطرق غير مشروعة و مخفية ببرامج أخرى لتدمير وتخريب برامج ومعلومات وبيانات الحاسوب في لحظة محددة". للمزيد انظر: إسماعيل بوتليليس، الجريمة المعلوماتية، مجلة الشرطة العلمية والتقنية، المرجع السابق، ص 12.

2) التعديل: يقصد به تغيير المعلومات الموجودة داخل النظام واستبدالها بمعلومات أخرى، وذلك بإمداده بمعطيات مغايرة تؤدي لنتائج مغايرة عن تلك التي صمم البرنامج لأجلها[1].

3) الإزالة: يقصد به المحو الجزئي أو الكلي للمعلومات المتواجدة داخل النظام أو النقل أو التخزين لها في منطقة خاصة، فهي مرحلة لاحقة على عملية إدخال المعطيات، فالإزالة تفترض الوجود السابق لعملية الإدخال[2].

وبما أن جريمة التلاعب بمعطيات الحاسب الآلي جريمة عمدية لابد من توافر القصد الجنائي العام أي يكون الجاني على علم بكافة العناصر المكونة للركن المادي للجريمة ولو لم يترتب ضرر وتنتفي هذه الجريمة إذا تمت عن طريق الخطأ، أما القصد الجنائي الخاص فلا يتطلب المشرع نية خاصة في هذه الجريمة.

رابعا: الجرائم الماسة بجميع مصالح المعطيات

جرم المشرع الجزائري طائفة من الأفعال تصب كلها في التعامل في معطيات صالحة لترتكب بها إحدى جرائم المعطيات، فحرص للتقليل من الضرر قدر الإمكان فجرم أشكال من التعاملات في المعطيات وذلك بموجب المادة 394 مكرر2 من ق ع ج نبينها فيما يلي:

1)التعامل في معطيات صالحة لارتكاب الجريمة

نصت المادة 394مكرر2 من ق ع ج على مجموعة من الأفعال وهي[3].

أ)التصميم: وهو إيجاد معطيات صالحة لارتكاب الجريمة وعادة ما يقوم بهذا العمل أشخاص متخصصين كمصممي البرامج.

---

[1] نجاة بن مكي، المرجع السابق، ص 188.

[2] عبدالوهاب مليايني، المرجع السابق، ص 194.

[3] محمد قسمية، المرجع السابق، ص307.

ب)البحث: وهو كيفية تصميم هذه المعطيات أي إجراء أبحاث.

ج)التجميع: هو القيام بجمع العديد من المعطيات التي يمكن أن ترتكب بها جريمة الدخول غير المصرح به أو جريمة التلاعب.

د)التوفير: أي تقديم المعطيات وإتاحتها لمن يريدها، وهذا الفعل معاقب عليه أيضا في التشريع الفرنسي ومنصوص عليه في اتفاقية بودابست لسنة 2001.

هـ)**النشر:** أي إذاعة المعطيات محل الجريمة وتمكين الغير من الاطلاع عليها عبر مختلف وسائل النشر.

و)الإتجار: يقصد به تقديم معطيات للغير ويكون ذلك بمقابل ولا يهم إن كان نقديا أو عينيا أو مقابل خدمة

2) **التعامل في معطيات متحصلة من جريمة**

تتحقق جريمة التعامل في معطيات متحصلة من جريمة بأحد الأفعال التالية:

أ)الحيازة : تقوم بسيطرة الجاني على المعطيات المتحصلة من إحدى جرائم المعطيات، وللقول بتوافر السيطرة عدم وجود عقبات واقعية تحول بين الشخص وبين التمتع بهذه المعطيات

ب) الإفشاء: يقصد بها حصول الشخص على معطيات بطريقة غير مشروعة ثم يقدمها إلى أشخاص آخرين

ج) النشر : لم يحدد المشرع وسيلة النشر فقد تكون عن طريق شبكة الإنترنت أو أقراص مضغوطة أو أي وسيلة أخرى ساهمت في النشر السريع وبكفاءة عالية للمعلومات متحصل عليها [1]

د) الإستعمال: كإستعمال شركة ما معطيات أو معلومات عن شركة منافسة لها وهي من أخطر الأفعال وتم الحصول عليها بطريقة غير مشروعة .

[1]فيصل نسيغة وعبير بعقيقي، المرجع السابق، ص 196.

وبما أن جريمة التعامل في معطيات غير مشروعة هي جريمة عمدية تتطلب توافر القصد الجنائي العام لدى الجاني يتجلى ذلك من خلال عبارة "عمدا" وعبارة عن "طريق الغش"[1]

الفرع الثالث :الجزاء المترتب عن جرائم المعلوماتية

تختلف العقوبات المقررة لجرائم الغش المعلوماتي من جريمة لأخرى وتتفق كل الجرائم في بعض القواعد.

أولا : العقوبة المقررة لكل جريمة

أ) الدخول في منظومة معلوماتية أو البقاء فيها: تعاقب المادة 394 مكرر ق ع على هذا الفعل بالحبس من 3أشهر إلى سنة وبغرامة 50.000 دج إلى 200.000 دج وتطبق العقوبات ذاتها على المحاولة، وتضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة.

وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة من 6 أشهر إلى سنتين والغرامة من 50.000 دج إلى 300.000 دج.

ب) المساس بمنظومة معلوماتية : تعاقب المادة 394 مكرر1 على هذا الفعل بالحبس من 6 أشهر إلى 3سنوات وبغرامة من 500.000 دج إلى 4.000.000دج.

ج)الأعمال الأخرى: تعاقب المادة 394 مكرر2 بالحبس من شهرين إلى 3 سنوات وبغرامة 1.000.000دج إلى 10.000.000 دج كل من يقوم عمدا أو عن طريق الغش بـ: تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها إحدى الجرائم المذكورة علاه.

حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المذكورة أعلاه[2].

[1] فيصل نسيغة وعبير بعقيقي، المرجع السابق، ص196.

[2] أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، ط15، دار هومة، الجزائر، 2013، ص 496.

الفرع الرابع: الأحكام المشتركة بين جرائم المعطيات

من استقراء المواد من 394 مكرر3 إلى 394 مكرر7 من ق ع ج نجد أن المشرع قد وضع أحكاما مشتركة بين جميع جرائم المعطيات منها ما يتعلق بالجريمة ومنها ما يتعلق بالعقوبة.

أولا: الأحكام المشتركة المتعلقة بالجريمة منها

1)العقاب على الاتفاق الجنائي: إذ يعاقب المشرع الجزائري على الاشتراك في الاتفاق الجنائي بعقوبة الجريمة التي تم التحضير لها.

2)العقاب على الشروع: إذ نص المشرع صراحة في المادة 394 مكرر7 من ق ع على العقاب على الشروع في ارتكاب جرائم المعطيات بنفس العقوبة المقررة للجريمة المرتكبة.

ثانيا: الأحكام المشتركة المتعلقة بالعقوبة منها

إضافة للعقوبات الأصلية المقررة لجرائم المعطيات، فقد قرر المشرع عقوبات تكميلية أيضا لهذه الجرائم فبخصوص المصادرة والغلق تطرقت لهما المادة 394مكرر6 من ق ع ج.

كما تم تشديد عقوبة الشخص المعنوي المرتكب لجرائم منصوص عيها سابقا بغرامة تقدر5 مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.

وأيضا تم تشديد عقوبة الاعتداء على الهيئات العامة حيث رتب المشرع عقوبة مشددة على جرائم المعطيات إذا كان موضوع النتيجة الإجرامية بعض الهيئات العامة، وذلك بمضاعفة العقوبة المقررة للاعتداء على معطيات وأنظمة أشخاص القانون الخاص ويرجع ذلك لأهمية وحساسية المعطيات المتعلقة بالمصالح العليا للدولة وما تتطلبه من ضمانات أكبر لحمايتها.[1]

[1] محمد قسمية، المرجع السابق، ص ص 310،312.

وقد خص المشرع مؤسسة الدفاع الوطني بالذكر نظرا لأهميتها ودورها في الحفاظ على سلامة التراب الوطني والأمن العام ورد الاعتداءات الداخلية والخارجية التي تهدف للإطاحة بنظام الدولة[1].

المطلب الثاني: الحماية الجزائية في قانون الملكية الفكرية والصناعية

نظرا لنسبية الحماية من خلال النصوص التقليدية لجرائم الأموال نتيجة للطبيعة المميزة للمال المعلوماتي، و لما كانت الحاجة ملحة وضرورية لحماية برامج الحاسب الآلي في الوسط القانوني والتوجه الفعلي من قبل رجال القانون نحو وضع الأطر القانونية لهذه الحماية مما أدى إلى إثارة جدل حول الحماية المناسبة لبرامج الحاسب الآلي، فقد استقر الفكر القانوني مؤخرا على إخضاع برامج الحاسب الآلي لقوانين الملكية الفكرية والصناعية

الفرع الأول: الحماية الجزائية لبرامج الحاسوب من خلال نصوص الملكية الفكرية

يعتبر حق المؤلف من أبرز صور الملكية الفكرية وأهمها، لذلك قامت العديد من الدول سواء عبر تشريعات داخلية أو اتفاقيات دولية بإقرار حماية قانونية لحق المؤلف وكواكبها المشرع الجزائري في ذلك والذي أصدر عدة قوانين لحماية حق المؤلف.

ويشمل نطاق قانون حق المؤلف من حيث الموضوع المصنفات الأدبية والفنية المبتكرة أيا كان نوعها أو طريقة التعبير عنها أو أهميتها أو الغرض منها، ومن أهم هذه المصنفات برامج الكمبيوتر، فنجد أن المشرع الجزائري من خلال نص المادة 4 من الأمر رقم03-05 قد نص صراحة على اعتبار برامج الكمبيوتر كمصنفات أدبية أما على الصعيد الدولي فنجد اتفاقية برن لعام 1979 و تريبس فأقرت الاتفاقية الأولى مبادئ وأسس تحكم الجانب الجزائي للمساس بحق المؤلف ولم تجرم بصفة صريحة تصرفات معينة لترك أمر تحديد جرائم الاعتداء على حقوق المؤلف للتشريعات الداخلية للدول وقد صادقت الجزائر على اتفاقية[2].

[1] محمد قسمية، المرجع السابق، ص ص 310، 312.

[2] فريال لعاقل، المرجع السابق، ص ص 49،50.

برن لانه من شروط الانضمام للمنظمة العالمية للتجارة وذلك بموجب المرسوم الرئاسي(341/97) المؤرخ في 1997/09/13 المتضمن إنضمام الجزائر بتحفظ إلى إتفاقية برن لحماية المصنفات الأدبية والفنية[1].

أولا: الإعتداءات الواردة على برامج الكمبيوتر

نظرا لما تتعرض له برامج الكمبيوتر من جرائم متعددة ومتنوعة فإن أغلب التشريعات المعاصرة الخاصة بحماية المؤلف التي لم تخلو من حماية جزائية لكون الحماية المدنية غير رادعة لهذه الاعتداءات الخطيرة، فالحماية الجزائية أكثر ردعا حيث نص المشرع الجزائري في المواد 151 إلى 159 من قانون رقم 03-05 على جرائم وعقوبات الاعتداء على حقوق المؤلف سنتطرق لهذه الاعتداءات والعقوبة المقررة لها

1)جريمة التقليد

لم يتطرق المشرع الجزائري الى تعريف جريمة التقليد، بل بين فقط الافعال التي تشكل جريمة التقليد يعرفها بعض الفقهاء بأنها "اعتداء مباشر أو غير مباشر على حقوق المؤلف " فجريمة التقليد تتمثل في الاعتداء على حق من حقوق المؤلف المحمي قانونا.

ولقد نص المشرع الجزائري في المادة 151من الأمر 03-05على أنه يعد مرتكب لجنحة التقليد كل من يقوم بالكشف غير المشروع للمصنف أو يمس بسلامته، أو يقوم باستنساخ مصنف أو يقوم باستيراد أو تصدير أو نسخ مقلدة من صنف أو يقوم بتأجير أو وضع رهن التداول لنسخ مقلدة لمصنف، أما المادة 154 منه نصت على أنه يعد مرتكب لجنحة التقليد كل من يشارك بعمله أو بالوسائل التي يحوزها للمساس بحقوق المؤلف، كما نصت المادة 155 منه على أنه يعد مرتكب لجنحة التقليد كل من يرفض عمدا دفع المكافئة المستحقة للمؤلف[2].

[1] نجاة بن مكي، المرجع السابق، ص 162.

[2] فريال لعاقل، المرجع السابق ، ص 50.

2) الجرائم الملحقة بجرائم التقليد

نصت على هذه الجرائم الفقرات الثالثة والرابعة والخامسة من المادة 151من الأمر 03-05

- استيراد أو تصدير نسخ مقلدة من مصنف أو أداء فني.
- بيع نسخ مقلدة أو أداء فني.
- رفض عمدا دفع المكافأة المستحقة للمؤلف .

ثانيا: الجزاءات المقررة لجرائم الاعتداء على برامج الكمبيوتر

هناك عقوبات أصلية وعقوبات تكميلية مخصصة لهذا النوع من الجرائم.

قرر المشرع الجزائري بموجب المواد 153،156،157،158،159 من الأمر 03-05 متعلق بحقوق المؤلف والحقوق المجاورة جزاءات على كل من يعتدي على حقوق المؤلف[1].

1) العقوبات الأصلية

تتمثل هذه العقوبة وفقا لنص م 153 من الأمر 03-05 بالحبس من 6 أشهر إلى 3سنوات وغرامة من 500.000 دج إلى 1.000.000 دج سواء كان النشر قد حصل في الجزائر أو خارجها[2].

من هنا يتضح أن المشرع الجزائري منح سلطة تقديرية في النطق بالعقوبة سواء بالنسبة للحبس أو الغرامة المالية.

كما تشدد العقوبة في حالة العود بموجب م 156 من الأمر 03-05.[3]

2) العقوبات التكميلية وتدابير الأمن

تتمثل العقوبات التكميلية في المصادرة ونشر الحكم حيث جاءت المصادرة في المادة 157 من الأمر 03-05 التي نصت على أنه تقرر الجهة القضائية المختصة مصادرة

[1] فيصل بدري ،المرجع السابق ،ص 148.

[2] الأمر رقم 03-05 المؤرخ في 19 جمادى الأولى الموافق 19 يوليو 2003 يتعلق بحقوق المؤلف و الحقوق المجاورة.

[3] نجاة بن مكي، المرجع السابق، ص 174.

المبالغ التي تساوي مبلغ الإيرادات أو أقساط الإيرادات الناتجة عن الاستغلال غير الشرعي للمصنف ومصادرة العتاد المخصص لمباشرة النشاط أو المشروع والنسخ.

وتأمر الجهة القضائية المختصة طبقا للمادة 159 من الأمر 03- 05 جميع الحالات المنصوص عليها في المواد 151، 152 تسليم العتاد أو النسخ المقلدة أو قيمة ذلك كله وكذلك الإيرادات موضوع المصادرة للمؤلف أو لأي مالك حقوق أخرى أو ذوي حقوقهما لتكون عند الحاجة بمثابة تعويض عن الضرر اللاحق بهم و قد جعلها المشرع جوازيه[1].

أما عقوبة نشر الحكم فنص عليها المشرع في المادة 158 من الأمر03-05 فيمكن للقاضي بناء على طلب الطرف المدني الأمر بنشر أحكام الإدانة على نفقة المحكوم عليه على ألا تتعدى المصاريف قيمة الغرامة المحكوم بها.

وفيما يتعلق بتدابير الأمن فنجد المادة 2/156 نصت على عقوبة الغلق فيمكن للجهة القضائية المختصة أن تقرر الغلق المؤقت مدة لا تتعدى 6 أشهر التي يستغلها المقلد أو شريكه أو أن تقرر الغلق النهائي عند الاقتضاء وتعتبر هذه العقوبة جوازيه.

وبالطبع لكي تتمتع البرامج بالحماية يجب توفر شروط المصنف المحمي وأهمها شرط الابتكار وأن يتحقق الاعتداء عليها بإحدى النماذج الإجرامية.

الفرع الثاني: الحماية الجزائية لبرامج الحاسوب في ظل نصوص الملكية الصناعية

لقانون الملكية الصناعية عدة مجالات تتمثل في العلامة التجارية، براءة الاختراع، الرسوم والنماذج وتسمية المنشأ وما يهمنا حماية أموال الإعلام الآلي هو حمايتها من خلال براءات الاختراع [2].

[1] هبة نبيلة هروال، جرائم الإنترنت(دراسة مقارنة)، أطروحة لنيل شهادة الدكتوراه، جامعة أبي بكر بلقايد تلمسان، 2013-2014، ص 225.

[2] آمال قارة، المرجع السابق، ص 64.

أولا: الشرط الواجب توافرها في براءة الاختراع

بصدور الأمر 03-07 المؤرخ في 2003/07/19 المتضمن براءة الاختراع وبالرجوع إلى نصوصه نجد المادة الثانية منه عرفت الاختراع بأنه :" فكرة لمخترع تسمح عمليا بإيجاد حل لمشكل محدد في مجال التقنية" وبشأن الشروط الواجب توافرها في الاختراع كي يقع تحت الحماية فإن الثالثة من ذات الأمر تنص على مايلي: "يمكن أن تقع تحت حماية براءة الاختراع، الاختراعات الجديدة الناتجة عن نشاط اختراعي والقابلة للتطبيق صناعيا"

وعليه فإن قانون الملكية الصناعية يضفي حمايته عن طريق براءة الاختراع، حيث لابد من توافر شروط معينة في الاختراع تتمثل فيمايلي:

1)شرط الإبتكار

2)شرط الجدة

3)القابلية للتطبيق الصناعي

4)المشروعية

إن الفقه التجاري الذي تناول موضوع براءة الاختراع كموضوع من موضوعاته على كون الاختراع ذو صفة مادية، ويتضح ذلك من الشروط الواجب توفرها في الاختراع حتى يتمتع بالحماية القانونية التي تقررها نصوص قانون براءة الاختراع التي لا تطبق إلا على الأشياء المادية الملموسة سواء كان منتجا أو وسيلة خاصة إذ لاحظنا أن كل ذلك في إطار شرط القابلية للاستغلال الصناعي، ليتبين أنه يحتوي على بعد مادي، وهذا ما يفرق على أساسه الفقه التجاري بين الابتكار الصناعي والمصنفات الأدبية ومن هنا فإن الفقه التجاري و إن كان قد اختلف في ترتيب شروط الاختراع التي تؤهله للحصول على البراءة، فإنه متفق على الطابع المادي لهذا الاختراع أو الابتكار الجديد القابل للاستغلال الصناعي .[1]

[1] امال قارة، المرجع السابق، ص 64.

وبناءا على ذلك فإن أحكام قانون براءة الاختراع يمكن أن تطبق على المكونات المادية للحاسب متى توافرت فيها الشروط التي يتطلبها هذا القانون أما مكونات الحاسب غير المادية فلا يمكن أن نطبق النصوص الخاصة بقانون براءة الاختراع وذلك لانتفاء الطابع المادي لها[1].

ثانيا: مدى تطبيق نصوص براءة الاختراع على برامج الكمبيوتر

يرى القائلون بالحماية بقوانين براءة الاختراع أن برامج الحاسوب ولأنها تستعمل للتعامل مع آلات الحاسوب وإدارتها فهي بذلك تصبح جزء منها، ولما كانت البرامج تتضمن إستخدامات جديدة لأفكار أو مبادئ علمية لتشغيل الحاسب فهي من هذه الزاوية تصبح قابلة للبراءة.

المنتقدون فيقولون على الرغم من مزايا الحماية التي توفرها قوانين براءة الاختراع إلا أنه توجد عدة أسباب تحول دون امتداد نصوص براءة الاختراع إلى المكونات غير المادية للحاسب.

حسبما يراه المختصون في الميدان فإنه من الصعب توفير حماية ناجحة للبرمجيات بالرجوع إلى قانون الملكية الصناعية، و يتعلق الأمر خاصة بشرطين لابد من توفرهما في العمل الإبداعي لكي يظفر صاحبه بالبراءة: شرط الجدية والقابلية للاستغلال.[2]

1)شرط الجدة

طبقا للمادة 05 من الأمر 03-07 "يعتبر الاختراع ناتجا عن نشاط اختراعي إذا لم يكن ناجما عن بداهة عن الحالة التقنية"، فيصعب تحققه في البرمجيات هذا من جهة و من جهة أخرى يصعب إثباته، إذ يجب للتقرير بتوافر هذا الشرط أن يكون لدى الجهة التي تقوم بفحص طلبات البراءة قدرا معقولا من الدراية لكي تقرر ما إذا كان قد سبق تقديم اختراعات

[1] آمال قارة، المرجع السابق، ص ص 64،65.

[2] فريال لعاقل، المرجع السابق، ص ص 56، 57.

مشابهة للاختراع المقدم الطلب بشأنه أم لا، الأمر الذي يتطلب أن تكون هذه الجهة على درجة عالية من الكفاءة والتمييز في المجال الذي تتولى بحقه.

وتقرير جدة الاختراع في معظم الأحيان يكون أمرا جزافيا، لما تتميز به من طابع ذهني بحت، قد يكون صعبا على المبرمجين ذاتهم، فكيف يكون الوضع بالنسبة للقاضي عند عرض هذه المسألة عليه[1].

تكمن صعوبة تقييم طابع الجدة بالنسبة للكيانات غير المادية ليس مرده لاعتبارات قانونية، بل يرجع ذلك لعدم توافر الكفاءات اللازمة التي يمكنها فحص الكيان المعنوي، والنظر في مدى توافر شرط الجدة بالنسبة له من عدمه.

2)صعوبة إستغلال الصناعي بالنسبة للكيان المعنوي

يجب أن يكون الاختراع قابلا للاستغلال الصناعي ليتمتع بنصوص الحماية الخاصة ببراءة الاختراع هذا الشرط يفترض أن يكون الاختراع ذا صفة مادية ويجب أن يؤدي استغلاله لمنتج صناعي، أو يمكن الوصول لنتيجة صناعية وكل هذه الأمور تتناقض مع الكيان المعنوي، فالتشريعات المعاصرة بصفة عامة تستبعد البرامج المعلوماتية من مجال الحماية بواسطة براءة الاختراع وذلك راجع لسببين:

أ) تجرد برامج المعلوماتية من أي طابع صناعي وهذا ما أثبتته الإحصائية التي أجرتها المنظمة العالمية للملكية الفكرية عام 1978 التي جاء فيها أن 1% فقط من البرامج يستوفي شرط قابلية الإستغلال الصناعي.

ب) صعوبة البحث في مدى جدة البرامج، لتقدير مدى استحقاقها لبراءة الاختراع.

ويمكن إستثناء الحصول على البراءة بخصوص برامج الإعلام الآلي في حالتين همـــا:

[1] آمال قارة، المرجع السابق، ص66،67.

أن يكون البرنامج جزء من ذاكرة الحاسوب وأن يكون طلب براءة الاختراع ينصب على وسيلة صناعية جديدة ويستخدم البرنامج في تحقيق إحدى مراحلها.

ونجد أن المشرع قد استبعد البرامج المعلوماتية صراحة من مجال الحماية بواسطة براءة الاختراع وذلك طبقا للمادة 07 من الأمر 03-07 المتضمن براءة الاختراع[1].

[1] آمال قارة، المرجع السابق، ص 68.

المبحث الثاني: الأساليب الإجرائية لنصوص الجريمة المعلوماتية في الاتفاقيات الدولية والقانون الجزائري

بالإضافة إلى الجوانب الموضوعية التي تم التطرق لها في المبحث الأول سنخصص هذا المبحث للأساليب الإجرائية لنصوص الجريمة المعلوماتية سنتناول في المطلب الأول المكافحة الإجرائية في الاتفاقيات الدولية أما المطلب الثاني المكافحة الإجرائية في القانون الجزائري.

المطلب الأول: المكافحة الإجرائية في الاتفاقيات الدولية

في مجال المكافحة الإجرائية كان التعاون لدولي ضروريا للتعامل مع هذا الإجرام الجديد الذي قد يمس في آن واحد عدة دول وفي هذا الإطار سنتناول الإجراءات الجديدة المتخذة في كل من اتفاقية بودابست واتفاقية المجلس الأوروبي.

الفرع الأول: الإجراءات الجديدة في لاتفاقية بودابست

نجد أن الإجراءات تتمثل في:

الحفظ السريع للمعطيات المخزنة أي الاحتفاظ بالمعلومات السابقة وتخزينها مع حمايتها[1].

بالإضافة إلى التفتيش المعلوماتي مع وجوب توفر شرط الحصول على إذن رسمي للتفتيش.

كما نصت اتفاقية بودابست على إجراء التنصت كإجراء جديد خاص قد يمس بحقوق الأفراد الخاصة لذلك يجب موافقة السلطات القضائية و مفاده اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية كالخطوط الهاتفية.

[1] نورة طرشي، مكافحة الجريمة المعلوماتي، مذكرة شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة الجزائر 2011،1-2012، ص 95.

ونصت المادة 23 من الاتفاقية على ضرورة تعاون الدول فيما بينها في أوسع نطاق ممكن مع تقليل الصعوبات التي قد تواجه تبادل المعلومات والأدلة كما تناولت الأحكام الخاصة بتسليم المجرمين وشروطهم.

الفرع الثاني: الإجراءات الجديدة في اتفاقية المجلس الأوروبي لسنة 2004

نصت هذه الاتفاقية على مجموعة من الجرائم التي تمس النظام المعلوماتي وبينت الأساليب التحقيقية فيها وهذه الجرائم هي الجرائم المرتكبة ضد سرية وتكامل وتوافر البيانات أو نظم الحاسبات كجرائم التدخل والاختراق على أجهزة الحاسبات الآلية، والجرائم المتصلة بالمحتوى التي يقصد بها الجرائم الخاصة بالإنتاج أو النشر غير مشروع، بالإضافة إلى الجرائم التي تتضمن انتهاكا لحقوق الملكية الفكرية وما يتصل منها من حقوق ومن الأساليب الإجرائية المنصوص عليها في الاتفاقية لدينا:

إرساء كل من إجراء تفتيش و ضبط أنظمة الحاسبات الآلية.

كذلك إجراء الحفظ السريع لبيانات الحاسب المخزونة التي تم جمعها وحفظها فعليا بمعرفة حائز البيانات، وهذا الإجراء هو إجراء تحقيقي جديد وهام، خاصة فيما يتعلق بالجرائم التي ترتكب على شبكة الإنترنت.[1]

وأيضا إجراء الأمر بإصدار نسخة من البيانات، وهنا يمكن للسلطات المختصة من إجبار الشخص على تقديم بيانات الحاسب المخزونة أو المحددة أو أحد عناوين ISP (Internet service provider) المعنية والتي تساهم في التوصل إلى معلومات حول المشترك، وقد أعطت الاتفاقية اهتماما خاصا لإجراء التفتيش والضبط في البيئة المعلوماتية نظرا لكون البيانات فيها تكون في صورة ملموسة، لذلك اعتمدت أيضا على إجراء الجمع الفوري لبيانات الحاسب والذي يعتمد على الجمع الفوري لبيانات النقل والذي يخص أحد البيانات المتعلقة بأحد الاتصالات التي تتم بواسطة نظام الحاسب الآلي.

[1] نورة طرشي، المرجع السابق، ص 97.

كما نصت على إجراء اعتراض بيانات المحتوى والتي تعني اعتراض محتوى الاتصال سواء كان رسالة أو معلومة منقولة.

ودائما في إطار المكافحة الإجرائية في اتفاقية المجلس الأوروبي يجب التنويه إلى دور هذه الاتفاقية في إنشائها لوحدة (EUROJUT) التي مهمتها التعاون بين دول الإتحاد الأوروبي في مجال مكافحة الجريمة المعلوماتية، وذلك بإصدار إجراء جديد جماعي هو أمر القبض الأوروبي (mondatd'arret Europèen) الذي يسمح بتسليم المجرم المعلوماتي بسرعة في أي دول الإتحاد الاوروبي[1].

المطلب الثاني: الجوانب الإجرائية المنصوص عليها في القانون الجزائري

بظهور جرائم المعلومات تفطنت معظم الدول لهذا الخطر وسلكت طريق حماية قواعد المعطيات بإيجاد منظومة قانونية تهدف قانونية متكاملة لحماية الحقوق والحريات بالإضافة إلى توفير مجموعة من الإجراءات والتدابير الوقائية للحماية من الجرائم المعلوماتية.

وفي سنة 2004 قام المشرع بسن مجموعة من القوانين التي تهدف إلى الوقاية من هذه الجرائم من خلال القانون رقم04-15المعدل والمتمم لقانون العقوبات والقانون رقم 09-04 المتعلق بالوقاية ومكافحة الجرائم المتصلة بتكنلوجيا الإعلام والاتصال، كما أسند المشرع الجزائري مكافحة الجرائم المعلوماتية ولا سيما المساس بالأنظمة الآلية لمعالجة المعطيات إلى الأقطاب المتخصصة.

الفرع الأول: الجوانب الإجرائية المنصوص عليها في قانون الإجراءات الجزائية

أولا: إحداث المحاكم الجزائية ذات الاختصاص الموسع التي أجاز لها تمديد اختصاصها للنظر في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات من خلال المواد 37، 40 و 329 من قانون الإجراءات الجزائية[2].

[1] نورة طرشي، المرجع السابق، ص ص 102،103.

[2] مهدي رضا ولخضر رفاف، الجوانب الإجرائية لمواجهة الجريمة المعلوماتية في التشريع الجزائري، مواجهة الجريمة المعلوماتية، المرجع السابق، ص179،180.

ثانيا: تمديد الاختصاص الإقليمي لضباط الشرطة القضائية لمعاينة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات إلى كامل الإقليم الوطني من خلال المادة 16 منه .

ثالثا: قواعد استثنائية في التفتيش ومن بن هذه الإجراءات نذكر ما يلي:

جواز التفتيش في المحلات السكنية وغير السكنية وفي كل ساعات الليل والنهار لمعاينة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بناءاً على إذن مسبق من وكيل الجمهورية المختص وهو ما نصت عليه المادة 47 من قانون الإجراءات الجزائية، كما يمكن قيام ضابط الشرطة القضائية بتفتيش مسكن اي شخص يحتمل أن يحوز أوراقا أو أشياء لها علاقة بجرائم المساس بأنظمة المعالجة الآلية للمعطيات دون حضور صاحب المسكن حسب نص المادة 45 الفقرة الأخيرة من قانون الإجراءات الجزائية.

وتجدر الإشارة إلى أن هذه القواعد الاستثنائية المنصوص عليها في المادة 45 لا تعفي من اتخاذ التدابير اللازمة لضمان إحترام السر المهني عند إجراء التفتيش في محلات يكون أصحابها ملزمون باحترام السر المهني، كما أن جميع هذه الإجراءات الاستثنائية تستوجب الحصول على إذن مسبق من وكيل الجمهورية عندما يتعلق الأمر بحالة تلبس أو بتحقيق ابتدائي.[1]

رابعا: إمكانية استعمال أساليب خاصة للتحري في جرائم المساس بأنظمة المعالجة الآلية للمعطيات ويتعلق الأمر بـ:

اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية، والتقاط وتثبيت وبث وتسجيل الكلام والتقاط الكلام والتقاط صور الأشخاص في الأماكن الخاصة.

وجاءت جميع هذه الصلاحيات الاستثنائية مشروطة بإذن السلطة القضائية كما نص القانون على أن الإذن نفسه ينبغي أن يتضمن الضوابط التي تحول دون التعسف في استعماله.

[1] مختار الاخضري، المرجع السابق، ص61،62.

خامسا: التسرب

نصت المادة 65 مكرر11 من قانون الإجراءات الجزائية على التسرب كوسيلة لمعاينة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وإيقاف مرتكبيها وذلك من خلال قيام ضابط أو عون الشرطة القضائية أو الأشخاص الذين يتم تسخيرهم لغرض التسرب بإيهام المشتبه فيه أنهم يشتركون معه في ارتكاب الجريمة كفاعلين أصليين أو شركاء أو بإخفاء متحصلات الجريمة[1].

سادسا: إمكانية تمديد فترة الحجز للنظر

نص قانون الإجراءات الجزائية على إمكانية تمديد فترة التوقيف للنظر المحددة ب48 ساعة مرة واحدة عندما يتعلق بالتحريفي جرائم المساس بأنظمة المعالجة الآلية للمعطيات في حالات التلبس .

سابعا: استحدثت المادة 35 مكرر من القانون 15-02 المؤرخ في 23 جويلية 2015 المعدل للقانون 66-156 متضمن قانون الإجراءات الجزائية التي نصت على أنه يمكن للنيابة العامة الاستعانة في المسائل الفنية بمساعدين متخصصين لتعزيز قدرة النيابة في معالجة القضايا ذات الطابع التقني وهم خبراء يمكن الاستعانة برأيهم وخبرتهم في التحريات الأولية وخلال مختلف مراحل الدعوى.

الفرع الثاني: القواعد الإجرائية المنصوص عليها في القانون 09-04

جاء القانون 09-04 المؤرخ في 05 أوت 2009 الذي تضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، نص على قواعد للوقاية من الجرائم المعلوماتية ودعم وسائل مكافحتها، وتتمثل أهم الأحكام فيما يلي:[2]

[1] مختار الأخضري، المرجع السابق، ص63.

[2] مهدي رضا ورفاف لخضر، المرجع السابق، ص181.

أولا: الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

عرف القانون 04-09 هذه الجرائم في م 02 كما وضع تعريفات تقنية للمنظومة المعلوماتية والمعطيات المعلوماتية، وأيضا مقدمي الخدمات والمعطيات المتعلقة بحركة السير والاتصالات الإلكترونية ليس ذلك فقط بل وضع قواعد خاصة تجيز مراقبة الاتصالات الإلكترونية وقد نصت المادتين 3و4 على الحالات التي تجيز هذا النوع من المراقبة وهي:

أ) الوقاية من جرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، ويتعلق الأمر هنا بمراقبة وقائية تنطلق من كون الإرهاب تهديدا خطيرا ودائما وقد أحاط المشرع هذه العملية الاستثنائية بضمانات خاصة إذ نص على أن إساءة استعمال المعلومات المتحصل عليها في هذا الإطار تنجز عنه المساءلة الجزائية كما أخضعها لإذن يصدره النائب العام لدى مجلس قضاء الجزائر وفق شروط خاصة ولفترة 6 أشهر قابلة للتجديد.

ب) في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني[1].

ج) لمقتضيات التحريات والتحقيقات القضائية وأيضا في إطار تنفيذ طلبات التعاون القضائي الدولي، كما تضمن قواعد إجرائية خاصة بتفتيش المنظومات المعلوماتية وحجز المعطيات المعلوماتية (المواد من 5 إلى 9) .

د) إلزام مقدمي الخدمات بمساعدة السلطات المكلفة بإجراء التحريات القضائية (م10) بالإضافة إلى قواعد تلزم مقدمي الخدمات بحفظ المعطيات الخاصة بحركة السير للرجوع إليها إذا اقتضت التحريات ذلك وقد يترتب عن الإخلال بهذه الالتزامات عقوبة جزائية في حالة ما إذا أدى ذلك إلى عرقلة حسن سير التحريات القضائية (م 11).[2]

[1] مختار الأخضري، المرجع السابق، ص ص63،64.

[2] مهدي رضا ورفاف لخضر، المرجع السابق، ص 183.

هـ) وتم بموجب هذا القانون إنشاء هيئة وطنية مختصة للوقاية من هذه الجرائم إلا أنه لم يتم تجسيد إنشائها إلا في أواخر سنة 2015 بموجب صدور المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أوكتوبر 2015 الذي حدد تشكيلة وتنظيم وكيفية سير هذه الهيئة ومن بين مهامها المساهمة في تحديث المعايير القانونية في مجال اختصاصها تنشيط وتنسيق عمل السلطة المكلفة بمكافحة الجريمة المعلوماتية ومدها بالمساعدة والاستشارة اللازمة (م14)[1].

و) توسيع الولاية القضائية للمحاكم الجزائرية لتختص بالنظر في الجرائم المرتكبة خارج الإقليم الوطني سواء كان مرتكبها مواطنا جزائريا أم أجنبيا عندما تستهدف مؤسسات الدولة أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني وفق ما نصت عليه م 15.

ي) النص على مبادئ المساعدة القضائية الدولية المتبادلة وكيفيات تبادل المعلومات واتخاذ الإجراءات التحفظية لجمع الأدلة (المادتان16-17) مع إخضاع التعاون الدولي لقيود عدم المساس بالسيادة الوطنية والنظام العام وجواز التعاون بشرط المحافظة على سرية المعلومات المبلغة وهو ما نصت عليه م 18 من ذات القانون[2].

كما أضاف المشرع مرسوم رئاسي رقم 20-05 المؤرخ في 24 جمادى الأولى عام 1441 الموافق ل 20 جانفي 2020 يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية.

[1] عبدالقادر مصطفاوي، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، مجلة الشرطة العلمية والتقنية، المرجع السابق، ص 28.

[2] مختار الأخضري، المرجع السابق، ص 65.

الخاتمة

وفي الأخير، نجد أن الجرائم المعلوماتية لسهولتها فتحت الباب أمام أشخاص لهم نية سيئة الحصول على المال بأي طريقة، ولولا التقدم التكنولوجي لما ظهرت هذه الجرائم فكافحها المشرع الجزائري بترسانة من النصوص القانونية رغم تأخره في سنها عكس المشرع الإماراتي.

ولقد تعرضنا في هذا البحث إلى أحكام الجريمة المعلوماتية بما فيها تعريفاتها وأنواعها وأركانها كما تطرقنا إلى طرق الوقاية من هذه الجريمة وكيفية مكافحتها على المستوى الوطني والدولي ومن ناحية ثانية تناولنا الجوانب الموضوعية في نصوص الجريمة المعلوماتية وفي كل من قانون العقوبات و قانون الملكية الفكرية والصناعية بالإضافة الى قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها بالإضافة الى الجوانب الإجرائية

ومن بين النتائج التي تحصلنا عليها من خلال هذا البحث ما يلي:

- للجريمة المعلوماتية عدة خصائص من بينها صعبة الإثبات وأنها عابرة للحدود.
- لم يحدد المشرع الجزائري الوسيلة التي تتم بها الجريمة المعلوماتية لأنها قد ترتكب مستقبلا بأي وسيلة حيث ترك هنا المجال مفتوحا حتى تتسع دائرة الإجرام.
- من بين دوافع لارتكاب الجريمة المعلوماتية مكاسب مادية والانتقام من الغير.
- تم تمديد الاختصاص الإقليمي لضباط الشرطة القضائية لمعاينة الجرائم المعلوماتية الى كامل الإقليم الوطني.
- يعتبر قانون 09-04 أفضل القوانين الموجودة في الجرائم المعلوماتية فنجد أن المشرع الجزائري تميز عن غيره في هذا المجال لأنه لا يوجد مشرع تكلم عن القانون الاجرائي في الجرائم المعلوماتية .

ومن بين الاقتراحات:

– يجب التبليغ عن الجريمة المعلوماتية لأن الخوف من التشهير يجعل الجريمة المعلوماتية في تزايد مستمر فالأفضل الإبلاغ عنها ونشر الوعي لمحاربة هذه الجرائم.

– وضع قوانين أكثر مرونة لمواكبة سرعة تقدم الحاسب الالي في كل المجالات.

–حبذا لو بين مدة الحماية الخاصة ببرامج لأنه سكت عنها و هذا ما يجعلنا نطبق الحماية المقررة لباقي المصنفات الأدبية.

– ندعو المشرع الجزائري إلى تجريم مجموعة من الجرائم كبيع المخدرات الرقمية والاتجار بالبشر والعديد من الجرائم الاخرى.

– وضع حماية إلكترونية للمواقع المهمة في الدولة مثل وزارات والبنوك والمستشفيات.

قائمة المراجع

قائمة المراجع

أولا: القوانين

1)القانون رقم رقم 16-01 المتضمن التعديل الدستوري المؤرخ في 6 مارس 2016 ج ر عدد 14.

2)القانون الإتحادي رقم 2 لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات منشور في العدد رقم 442 من الجريدة الرسمية لدولة الإمارات العربية المتحدة.

3)قانون 09-04 المؤرخ في 5أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم تكنولوجيا الإعلام والإتصال ومكافحتها، ج ر عدد 47 سنة 2009.

الأمر رقم 03-05 المؤرخ في 19 جمادى الأولى الموافق 19 يوليو 2003 يتعلق بحقوق المؤلف و الحقوق المجاورة.

ثانيا: المراجع

أولا: الكتب

1) أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، ط15، دار هومة، الجزائر، 2013.

2) امال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، ط2، دار هومة،الجزائر،2007.

3)حنان ريحان مبارك المضحكي، الجرائم المعلوماتية، ط1، منشورات الحلبي الحقوقية، لبنان،2014.

4) خالد ممدوح إبراهيم، الجرائم المعلوماتية، ط1، دار الفكر الجامعي، مصر، 2009.

5)زيدان زيبحة الجريمة المعلوماتية في التشريع الجزائري و الدولي، ب ط، دار الهدى، الجزائر، 2011.

6) طارق ابراهيم الدسوقي عطية، الأمن المعلوماتي، ب ط، دار الجامعة الجديدة، الإسكندرية، 2009.

7)عبد الكريم الردايدة، الجرائم المستحدثة، ط1، دار الحامد، الأردن، 2013.

8)عبدالله عبد الكريم عبدالله، جرائم المعلومات والإنترنت، ط1، منشورات الحلبي، لبنان، 2017.

9)علي جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص و الحكومة، ط1، منشورات زين الحقوقية، بيروت،2013.

10)غانم مرضي الشمري، الجرائم المعلوماتية، ط1، الدار العلمية الدولية،الأردن،2016.

11)نجاة بن مكي، السياسة الجنائية لمكافحة جرائم، ط1، دار الخلدونية، الجزائر، 2017.

ثانيا: المذكرات:

1)أمينة بوشعرة وسهام موساوي، الإطار القانوني للجريمة الالكترونية، (دراسة مقارنة)، مذكرة لنيل شهادة الماستر، تخصص القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة ميرة، بجاية 2017-2018.

2)حسين ربيعي، اليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة لنيل شهادة الدكتوراه، تخصص قانون العقوبات وعلوم جنائية، كليى الحقوق والعلوم السياسية، جامعة باتنة1، 2015-2016.

3)عبد الرحمان نشادي، الجرائم المعلوماتية في وسائل الإتصال الحديثة، أطروحة لنيل شهادة الدكتوراه، في علوم الإعلام والإتصال، كلية الإعلام والإتصال، جامعة الجزائر3، 2016-2017.

4)عبدالوهاب ملياني، أمن المعلومات في بيئة الأعمال الإلكترونية، رسالة لنيل شهادة الدكتوراه في القانون العام، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد تلمسان، 2016-2017.

5)عبير بعقيقي، مكافحة الجريمة المعلوماتية في التشريعين الجزائري والاماراتي دراسة مقارنة ، أطروحة لنيل شهادة الدكتوراه في الحقوق ، تخصص النظام الجزائي و السياسة الجزائية المعاصرة ، كلية الحقوق والعلوم السياسية ، جامعة محمد خيضر بسكرة، 2017-2018.

6) فريال لعاقل، الجريمة المعلوماتية في ظل التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون العام، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة اكلي محندأولحاج،البويرة،2014-2015.

7) فيصل بدري، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة لنيل شهادة الدكتوراه تخصص قانون عام، كلية الحقوق، جامعة الجزائر 01 يوسف بن خدة، 2017-2018.

8) نورة طرشي، مكافحة الجريمة المعلوماتي، مذكرة شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة الجزائر 2011،1-2012.

9) هبة نبيلة هروال، جرائم الإنترنت(دراسة مقارنة)، أطروحة لنيل شهادة الدكتوراه، جامعة أبي بكر بلقايد تلمسان، 2013-2014، ص 225.

ثالثا: المقالات

1)إسماعيل بوتليليس وعبدالقادر مصطفاوي ووافية ديوبي، الجريمة المعلوماتية، مجلة الشرطة العلمية والتقنية، الأمن الوطني، عدد 4جويلية 2019.

2)حسين ربيعي، المجرم المعلوماتي (شخصيته وأصنافه)، مجلة العلوم الإنسانية، جامعة محمد خيضر بسكر، عدد40، جوان 2015.

3)عبدالقادر مصطفاوي، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، مجلة الشرطة العلمية والتقنية.

4) فيصل نسيغة وعبير بعقيقي ،الاليات القانونية الموضوعية لمكافحة الجريمة المعلوماتية في التشريع الجزائري، مجلة الباحث للدراسات الاكاديمية، جامعة بسكرة عدد11، جوان 2017.

5) محمد قسمية، مهدي رضا ولخضر رفاف الجرائم الماسة بنظام المعالجة الآلية للمعطيات وأطر مكافحتها في قانون العقوبات الجزائري، مؤلف جماعي حول مواجهة الجريمة المعلوماتية، جامعة محمد بوضياف بالمسيلة، ب ع، المنشورات العلمية لكلية الحقوق والعلوم السياسية، أكتوبر 2019.

6) مختـــار الاخضـــري، الاطـــار القـــانوني لمواجهـــة جـــرائم المعلوماتيـــة وجـــرائم الفضـــاء الإفتراضـــي، المجلـــة القضـــائية، المديريـــة العامـــة للشـؤون القضـــائية والقانونيـــة، العـــدد 66، 2010.

رابعا: المداخلات

1)مختارية بوزيدي، ماهية الجريمة الالكترونية، الملتقى الوطني حول اليات مكافحة الجرائم الالكترونية في التشريع الجزائري، 29 مارس 2017، مركز جيل البحث العلمي الجزائر.

فهرس المحتويات