الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة محمد بوضياف المسيلة

كلية الحقوق والعلوم السياسية **ميدان: الحقوق**

قسم الحقوق **تخصص: قانون إداري**

مذكرة مكملة لنيل شهادة ماستر أكاديمي بعنوان:

الآليات القانونية لمكافحة الجريمة المعلوماتية في القانون الجزائري

إعداد الطالبتين: **إشراف الأستاذ:**

بوشنافة لميس **د/ مسعودي هشام**

بن شهرة مروة

لجنة المناقشة

الاسم واللقب	الرتبة	الصفة
زيتوني محمد	أستاذ محاضر أ	رئيسا
مسعودي هشام	أستاذ محاضر أ	مشرفا ومقررا
ميمون جمال الدين	أستاذ محاضر أ	ممتحنا

السنة الجامعية:2021-2022

ملحق بالقرار رقم ....1082.... المؤرخ في .....2020 - 12 - 27.....
الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي: جامعة محمد بوضياف - المسيلة -

نموذج التصريح الشرفي
الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

أنا الممضي أسفله،

السيد(ة): بوشاقة لميس ... الصفة: طالب، أستاذ باحث طالبة .....

الحامل(ة) لبطاقة التعريف الوطنية رقم: 126xxxxx والصادرة بتاريخ 25 ماي 2016 .....

المسجل(ة) بكلية / معهد الحقوق والعلوم السياسة قسم الحقوق .....

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

عنوانها: مذكرة ماستر .....

الجريمة المعلوماتية وآليات مكافحتها في التشريع الجزائري .....

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

التاريخ: 28/12/2020

توقيع المعني (ة)

ملحق بالقرار رقم .....1082..... المؤرخ في .....

الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي: جامعة محمد بوضياف - المسيلة -

نموذج التصريح الشرفي

الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

أنا الممضي أسفله،

السيد(ة): ..... الصفة: طالب، أستاذ باحث .....

الحامل(ة) لبطاقة التعريف الوطنية رقم: 198231568 والصادرة بتاريخ 2017

المسجل(ة) بكلية / معهد ..... قسم .....

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

عنوانها: مذكرة تخرج ماستر

آليات القانون الجنائي لمكافحة الجريمة المعلوماتية في القانون الجزائري

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

التاريخ: 28/06/2022

توقيع المعني (ة)

استمارة معلومات

المعلومات الشخصية:

الاسم لمبس اللقب بو نتاقة

اسم الأب علي اسم ولقب الأم حبيبي مريم

تاريخ الازدياد 1997/06/06 مكان الازدياد عين الملح

رقم الهاتف

البريد الالكتروني

العنوان الشخصي حي الورد بوعادة 25/28

الباكالوريا:

المعدل 10,17 الشعبة/التخصص آداب وفلسفة سنة الحصول على شهادة الباكالوريا: 2016

الليسانس:

تخصص الليسانس: قانون عام الدفعة/ سنة التخرج: 2020

الماستر:

تخصص الماستر قانون إداري الدفعة/ سنة التخرج: 2022

المعدل الترتيبي للماستر (المعدل العام)

الوضعية المهنية:

موظف: ☐ عاطل عن العمل: ☐

في حالة موظف:

وظيف عمومي قطاع خاص:

المصلحة المستخدمة اسم المؤسسة / الشركة:

الرتبة في العمل:

الصيغة:

موظف دائم موظف في إطار عقود: نوع العقد:

امضاء الطالب

استمارة معلومات

الصورة

المعلومات الشخصية:

الاسم: مروة اللقب: بن شهرة

اسم الأب: بدير اسم ولقب الأم: عيساوة السعدية

تاريخ الازدياد: 25-06-1994 مكان الازدياد: بوسعادة

رقم الهاتف: 06.58.85.00.88

البريد الالكتروني: Benchahramaroua@gmail.com

العنوان الشخصي: حي 24 فيفري 235117

الباكالوريا:

المعدل: 10,63 الشعبة/التخصص: آداب وفلسفة سنة الحصول على شهادة الباكالوريا: 2017

الليسانس:

تخصص الليسانس: قانون عام الدفعة/ سنة التخرج: 2020

الماستر:

تخصص الماستر: قانون اداري الدفعة/ سنة التخرج: 2022

المعدل الترتيبي للماستر: (المعدل العام)

الوضعية المهنية:

موظف: ☒ عاطل عن العمل: ☐

في حالة موظف:

وظيف عمومي: قطاع خاص:

المصلحة المستخدمة: اسم المؤسسة / الشركة:

الرتبة في العمل:

الصيغة:

موظف دائم: موظف في إطار عقود: نوع العقد:

امضاء الطالب

شكر و عرفان

قال رسول الله صلى الله عليه وسلم (من لا يشكر الناس لا يشكره الله)

أولا نحمد الله ونشكره على منحنا القدرة لإتمام هذا العمل المتواضع كما نتقدم بالشكر الجزيل إلى كل من ساهم في إتمام هذا العمل ونخص بالذكر الأولياء الأعزاء.

جميع الأساتذة وخاصة الأستاذ المشرف (مسعودي هشام) الذي لم يبخل علينا بتوصياته ونصائحه والى كل الأصدقاء جزاهم الله خيرا.

إلى كل من ساهم بالكلمة الطيبة في إعداد هذا العمل المتواضع سائلين المولى تبارك وتعالى أن يجزيهم عنا وعن الأمة الإسلامية كل خير وانه ولي التوفيق

إهداء

أولا لك الحمد ربي على كثر فضللك وجميل عطائك وجودك ، الحمد لله ربي ومهما حمدنا فلن نستوفي حمدك. والصلاة والسلام على من لا نبي بعد.

اهدي عملي إلى وطني العزيز الجزائر الصامدة والشامخة، إلى الإنسان الذي علمني كيف يكون الصبر طريق النجاح، إلى من لم تمنحه الحياة عمرا طويلا، إلى روح لطالما أردتها بجانبي في هذه اللحظة إلى أبي (رحمه الله).

إلى من تتسارع لها عبارات الحب والامتنان أمي الغالية.

إلى من تسابقوا وقدموا واحدا تلوا الآخر إخوتي و أخواتي واخص بالذكر (سهام، خديجة، الخنساء)

إهداء من القلب إلى صديقاتي وزميلاتي واخص بالذكر زميلتي في العمل والتي كانت سندا لي (مروة)

إلى كل من ساهموا لإنجاح مشروع تخرجي هذا بدعمهم المتواصل الى كل من كان له دور في مساندتي (اسمهان، أحلام)

كما اهدي هذا العمل المتواضع إلى كل من شارك في مساعدتي

إلى جميع أساتذة كلية الحقوق ولجامعة محمد بوضياف المسيلة .وخاصة الأستاذ المشرف (مسعودي هشام) الذي لم يبخل علينا بتوصياته ونصائحه.

إلى روح أخي الطاهرة التي لم تراه عيناي عمار

إلى كل من ساهم ولو بكلمة طيبة في إعداد هذا العمل المتواضع. سائلين المولى تبارك وتعالى أن يجزيهم عنا كل الخير انه ولي ذلك والقادر عليه.

إهداء

الحمد لله الذي زين دربي بالعلم ووفقنا لإنجاز هذا العمل.

اهدي ثمرة جهدي المتواضع إلى القلب الرحيم الذي رعاني و أول كلمة نطق بها لساني

أمي الحبيبة قرة عيني والحب الفياض ورمز الهناء أبي العزيز إلى من هم في البيت إخوتي وأخواتي وبنات خالاتي

والشكر موصول إلى كل معلم أفادنا بعلمه من أولى المراحل الدراسية حتى هذه اللحظة ، وأخص بالذكر الأستاذ المشرف (مسعودي هشام).

اهدي عملي هذا إلى صديقاتي العزيزات (لميس ، اسمهان ، أحلام ، شيماء ،ميساء ،لزهراء ، فيروز، خلود) اللواتي كن حافزا وشمعة الوصول والانجاز لهذا العمل المتواضع.

إلى كل هؤلاء وهؤلاء اهدي عملي وعصارة جهدي ونسال الله أن تبقى مرجعا نافعا للجميع ،ويجعل هذا العمل خالصا لوجهه .

بن شهرة مروة

مقدمة

تسير عجلة الزمن بديهيا فتغير الحياة وتختلف الأمور عما كانت عليه في السابق وتسير شيئا فشيئا نحو التطور والتقدم حسب تطور العقل البشري، وهذا ما تؤكده الحقائق التاريخية والأحداث المتسارعة والمتتبع لمراحل هذا التغير والتطور لابد أن يقف على ما وصل إليه عقل الإنسان عبر مراحل العصور المتعاقبة، اليوم نحن في القرن الواحد و العشرين الذي شهد تطورا ملحوظا لم تعرفه البشرية من قبل، فيه كل أنواع الابتكار والاختراع العلمي والحضاري والتكنولوجي الذي قفز بنا أشواطا كبيرة ومن ذلك كله الثورة التكنولوجية الهائلة التي يعرفها ويعيشها إنسان ما بعد سنة 2000، فنحن نشهد لحظات تاريخية متميزة من حيث الشبكة العنكبوتية الضخمة ومجالاتها المتشعبة وآثارها على حياة الأفراد والمجتمعات والدول. فوسائل التواصل الاجتماعي اليوم نستطيع أن نقول عنها بأنَّها قد أصبحت محور الحياة ونقطة انطلاق لكل الأعمال في شتى الميادين. فالباحث والعالِم والمثقف والسياسي إن أراد خوض مغامرة علمية أو سياسة فطريقتهم الوحيدة هي هذه الوسيلة الهامة والناس إذا أرادوا التواصل حتى في العلاقات الاجتماعية المختلفة فهذا سبيلهم الوحيد، والأكيد أنَّ لهذه الوسائل إيجابيات عديدة سهلت على إنسان اليوم حياته وغيرت نمطها تماما واختصرت له المسافات وسرعت له المعلومة وأراحته كثيرا ولكن في المقابل يجب أن لا نُغفل الجوانب السلبية، ومنها الحرب في مجال المعلوماتية أو ما يسمى بالجريمة السبريانية ومالها من أثر على أمن وسلامة الدول، فالجريمة المعلوماتية تتمثل فيما يقوم به أشخاص معنيون ومختصون في هذا المجال من أجل اختراق أسرار بعض الدول والأفراد والاطلاع على معلومات تتعلق بأمن وسلامة واقتصاد دول لها علاقات مختلفة فيما بينها سواء كانت علاقات عداوة او مشاكل سياسية أو اقتصادية أو حتى الدول الصديقة تكون هذه الجرائم السبريانية حاضرة فيما بينها، فكل دولة تسعى لتأمين نفسها من خلال معرفة كل ما يتعلق

بالدول الأخرى من خلال تعيين انسان له باع وعلم في هذا المجال، فالحرب اليوم لم تعد تقتصر على السلاح فحسب بل أصبحنا اليوم نتحدث عن نمط جديد من الجريمة أساسه الذكاء الخارق، لم نتعود عليه وليس من الأمور المألوفة ويتمثل في الجريمة المعلوماتية التي اضحت ضرورية تواكب نوع الافعال المرتكبة من إنسان القرن الواحد والعشرين مما دفع بفقهاء القانون لمناقشة جدوى وضع قوانين لمواجهة آثار هذه الجرائم لأنَّ البحث في المواجهة القانونية للأنظمة المعلوماتية مسألة معقدة وصعبة، فمواجهة هذا النوع لا يحتاج فقط لرجال القانون والأحكام القضائية، بل لابد من أهل اختصاص في الجانب الفني والتقني للمعلوماتية. فتطبيق القواعد التقليدية للقانون لا يجدي نفعا في مثل هذا النوع من الجرائم، وبالتالي سوف يتعطل جهاز العدالة في مواجهة ومكافحة الجريمة المعلوماتية. وفي بحثنا هذا نحاول الوقوف على نقاط مهمة ذات صلة بموضوع الجريمة المعلوماتية من حيث صعوبة إثباتها، ومعرفة مرتكبيها وهذا بسبب استخدام تقنيات عالية الدقة في هذا النوع من الجرائم، ولهذا يجب علينا التحليل الدقيق لمفهوم الجريمة المعلوماتية ومحلها وحدودها وحيثياتها من أجل كيفية التعامل معها ومدى إخضاعها للمقاييس والضوابط والقواعد القانونية الممارسة ضد الجريمة العادية التقليدية في ظل نقص وشُح في النصوص التشريعية المتعلقة بهذا النوع من الجرائم التكنولوجية، وبهذا نجد أنفسنا أمام العديد من التساؤلات التي تلزمنا بالإجابة عنها وتتمثل في :

- ما المفهوم الحقيقي والدقيق للجريمة المعلوماتية ؟
- ماهي أهم القوانين التي أوجدها المشرع للتصدي للجريمة المعلوماتية ؟
- هل القوانين المستحدثة من طرف المشرع الجزائري كافية لمواجهة هذا النوع من الجرائم ؟.

وللإجابة عن هذه الإشكالية المطروحة والتساؤلات الفرعية التي تفرض نفسها قمنا بهذا البحث الذي حاولنا من خلاله بالتحليل والتفسير والدراسة في حدود ما أُتيح لنا من مراجع ومعلومات من خلال تقديم

- مفهوم الجريمة المعلوماتية وحدودها وحيثياتها وكذا مدى فعالية القوانين التي سنها المشرع الجزائري اليوم.
- وفي سبيل تحقيق هدف بحثنا ودراستنا وإعطائها الأهمية والمكانة اللازمة تتبعنا المنهجية التالية: وفيها تطرقنا للموضوع بصفة عامة من خلال محاولة إعطاء نظرة عامة وشاملة للجريمة المعلوماتية كنوع من الجرائم التكنولوجية التي أصحبت من أهم وأكثر الجرائم الموجودة في عالمنا اليوم. وبعد ا دخلنا في عمق الموضوع من خلال فصلين:

الفصل الأول : تناولنا فيه مفهوم الجريمة المعلوماتية وخصائصها والطبيعة القانونية وكذا انوع الجرائم المعلوماتية، وأيضا الجرائم المعلوماتية الواقعة على النظام المعلوماتي المتعلقة بالاعتداء على المكونات المختلف للنظام المعلوماتي .

الفصل الثاني : تطرقنا إلى المكافحة الإجرائية للجريمة المعلوماتية بالدراسة والتحليل من خلال مفهوم المكافحة الإجرائية للجريمة المعلوماتية وأسبابها بالإضافة إلى الإجراءات المنصوص عليها وفقا للاتفاقيات الدولية وكذا نطاق المكافحة الإجرائية للجريمة المعلوماتية وفي الأخير دور المشرع الجزائري في الآليات القانونية والإجراءات اللازمة لمواجهة والتصدي للجريمة المعلوماتية وفقا للنصوص القانونية التي اعتمدها في مكافحة الجرائم المعلوماتية التي تمس بالحياة العامة للأشخاص والتي تشكل خطرا على الامن القومي للدول

وفي خاتمة موضوعنا نتناول التحديات والصعوبات التي تعترض المتابعات الجزائية في الجريمة المعلوماتية وماهي المقترحات لمواجهة الانماط الجديدة للجريمة المعلوماتية.

الفصل الأول

ماهية الجريمة المعلوماتية

الفصل الأول: ماهية الجريمة المعلوماتية

أضحت الجريمة تهدد الأمن والاستقرار العالميين وليس فقط الأمن الداخلي ، نتيجة لتشعبها عبر الحدود الوطنية، وذلك نظرا لظهور أنماط جديدة أو مستحدثة لم يعرفها العالم من قبل، حيث أصبح المجرمون يستغلون مختلف الوسائل التي أنتجها هذا العصر في تطوير وتوسيع نشاطاتهم الإجرامية، ومن بين ما يستعملونه كوسائل لارتكاب جرائمهم شبكات الأنترنت وأجهزة الكومبيوتر مما أدى إلى تزايد المخاطر. وتتمثل هذه المخاطر في إمكانية تدمير برامج وبيانات شخصية أو عامة. وهذا ما يسمى اليوم " بالجريمة المعلوماتية " وتجدر الإشارة إلى أنَّ فقهاء القانون لم يتوصلوا إلى مفهوم دقيق لذلك النوع من الجرائم ، وهذا ما يؤكد هذا النوع من الجريمة ظاهرة معقدة كونها تمس عديد من مجالات الحياة نظرا لسرعة انتشارها واستخدامها، وهذا ما أدَّى إلى تعذر الوصول إلى مفهوم واضح وشامل لهذه الجريمة[1] ولهذا سنعالج هذا الفصل في مبحثين تناولنا في المبحث الأول مفهوم الجريمة المعلوماتية الدي ينقسم الى ثلاث مطالب الاول تناولنا فيه تعريف الجريمة المعلوماتية والمطلب الثاني تطرقنا الى خصائص الجريمة المعلوماتية و المطلب الثالث الطبيعة القانونية للجريمة المعلوماتية . أما المبحث الثاني تناولنا فيه أنواع الجرائم المعلوماتية وهو بدلك انقسم الى ثلاث مطالب المطلب الأول الجرائم المعلوماتية الواقعة باستعمال نظام المعلوماتي والمطلب الثاني الجرائم المعلوماتية التي تتم على نظام المعلوماتي والمطلب الثالث جرائم الاعتداء على المعلومات المدرجة بالنظام المعلوماتي.

[1] محمد هشام فريجه، النظام القانوني للجريمة المعلوماتية وصعوبات تحقيق الأمن الإلكتروني، كلية الحقوق والعلوم السياسية، جامعة المسيلة ، الجزائر، تاريخ استقبال المقال 25/ 02/ 2018، تاريخ قبول نشر09/ 05/ 2018، المقال تاريخ نشر المقال 2018/07/10،ص2.

المبحث الاول : مفهوم الجريمة المعلوماتية

إنَّ للجريمة المعلوماتية عدة مسميات، فهي جريمة الكومبيوتر والأنترنت، وهناك من يطلق عليها اسم الجريمة الالكترونية وهناك من يسميها بالجرائم المستحدثة ولكن قبل التطرق إلى تعريف الجريمة المعلوماتية بشكل دقيق وواسع[1] يجب الوقوف عند مفهوم كل من المعلومات والمعلوماتية فا المعلومات هي كلمة معلومة ولا يوجد في وقتنا الحاضر إجماع في الفقه أو القانون على تعريف جامع ومانع للمعلومة فقد عرَّفها القانون الفرنسي رقم 652/82 الخاص بالاتصالات السمعية والبصرية بانها رنين صور الوثائق أو الوسائل من أي نوع . كما عرَّفها بعض الفقهاء بأنَّها " تلك التي تضيف شيئا ما إلى النموذج العقلي وإلى الانطباع الذهني الذي نعرفه عن العالم الخارجي في لحظة معينة. أما المعلوماتية هي ظاهرة اجتماعية وعلمية نشأت وازدهرت مع تقدم الحضارة الإنسانية، تُستعمل كوصف للوقت الحالي و تتكون من مقطعين الأول كلمة المعلومات و الثاني كلمة آلي أو أوتوماتيك التي تعني المعالجة الآلية للمعلومات[2] وعليه قمنا بتقسيم هدا المبحث الى ثلاث مطالب تناولنا فيه تعريف الجريمة المعلوماتية والمطلب الثاني تطرقنا الى خصائص الجريمة المعلوماتية و المطلب الثالث الطبيعة القانونية للجريمة المعلوماتية وسنتناول هده المطالب كالتالي

المطلب الاول: تعريف الجريمة المعلوماتية

لقد تعددت المصطلحات المستخدمة للدلالة على هذه الجريمة وتحديد مفهومها ، فهناك من يطلق عليها إسم جرائم الحاسبات أواساءت استخدام الحاسبات أو الجرائم المرتبطة أو

[1] محمد هشام فريجه، المرجع السابق،ص5.

[2] عيشة خلدون، محاضرات الجريمة المعلوماتية، السنة اولى ماستر، تخصص قانون جنائي والعلوم الجنائي، جامعة الجزائر،سنة2021، ص 1.

المتعلقة بالحاسبات أو الجرائم الإلكترونية وجرائم الكومبيوتر و جرائم المعلوماتية التي تعتبر التسمية الأقرب لهذا النوع من الجرائم وكلها مصطلحات انعكست على تعريف هذه الجريمة التي اختلف الفقه حول إعطائها تعريف جامع ومانع، حيث عرَّفها البعض أنَّها جريمة ضد المال مرتبطة باستخدام المعالجة الآلية للمعلومات، وأيضا تُعرَّف على أنَّها الاعتداءات غير القانونية التي تُرتكب بواسطة المعلوماتية بغرض تحقيق الربح . كما عُرِّفت بأنَها مجموعة من الأعمال المرتبطة بالمعلوماتية التي يمكن أن تكون جديرة بالعقاب، او أنَّها مجموعة الجرائم المتعلقة بعلم المعالجة المنطقية للمعلومات وهناك من رجح تعريف منظمة التعاون الاقتصادي والتنمية الخاص باستبيان الغش المعلوماتي عام 1982 والوارد في تقرير بلجيكا الذي بين بأنَّها " عبارة عن كل فعل او امتناع من شأنه الاعتداء على الأموال المادية والمعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل تقنية المعلومات[1] ومن خلال هده التعريفات سنتطرق الى تحديد كل من تعريف الضيق للجريمة المعلوماتية في الفرع الأول والتعريف الواسع في الفرع الثاني

الفرع الأول: التعريف الضيق للجريمة المعلوماتية

انطلق أنصار التعريف الضيق للجريمة المعلوماتية من النقطة المتعلقة بضرورة تحديد العلاقة بين المعلوماتية والأفعال غير المشروعة لتحديد ما إذا كانت تلك الأفعال تدخل في نطاق الجريمة المعلوماتية أم لا، بعبارة أخرى حتى تشكل الأفعال غير المشروعة جريمة معلوماتية يجب أن تكون موجهة ضد " الأموال المعلوماتية" مع إقصاء تلك الأفعال المتمثلة في استخدام الإعلام الآلي كوسيلة للاعتداء على الغير، سواء الأشخاص أو الأموال والثقة العامة.

[1] عيشة خلدون، المرجع السابق،ص1،ص2.

والتعريف المقترح في هذا الصدد من طرف الفقيه Sieber ورد فيه ما يلي[1]: est considère comme crime informatique tout comportement illégal ou non autorise qui concerne un traitement automatique de données ou de transmission de données

يقول الخبراء بأنَّ هذا التعريف غير علمي ويفضلون الأنجلوساكسونية طريقة الجرد أو القائمة المفتوحة ويضعون قائمة للافعال الغير مشروعة التي تدخل في نطاق الجريمة المعلوماتية بصفة حصرية[2]

- الغش
- التزوير المعلوماتي
- المساس بالمعطيات أو البرامج
- العرقلة
- إعادة نسخ البرامج

كما أنَّ منظمة التعاون الاقتصادي قدَّمت تعريفا للجريمة المعلوماتية " أنَّها كل سلوك غير مشروع أو غير مصرَّح به يتعلق بالمعالجة الآلية للبيانات ونقلها."

وهناك اتجاه فقهي آخر يتزعمه الفقيه "قراري" ضيَّق من مجال الجريمة المعلوماتية وقصرها على الاعتداءات الموجهة ضد الكيان المنطقي للمعلوماتية إذ شكك في اعتبار الاعتداءات الوارد على الكيان المادي للمعلوماتية من الجرائم المعلوماتية، و تبريره في ذلك أنَّه مادامت

[1] Luca :.le droit de l'informatique :themis.p496 .

[2] Masse :rapport final du conseil de l'Europe sur la criminalité en relation avec l'ordinateur 1988 p56

العناصر المادية المعلوماتية يمكن أن تخضع لأحكام جريمة السرقة ، فإن الاعتداء عليها لا يعد جريمة معلوماتية وأفصح الفقيه "قراري" عن رأيه هذا بقوله " إنَّ سرقة شريط ممغنط أو اسطوانة أو حتى الكومبيوتر ذاته لا يمكن أن تتدرج تحت تسمية الجريمة المعلوماتية .

الفرع الثاني: التعريف الواسع للجريمة المعلوماتية

يدخل هذا التعريف في نطاق الجريمة المعلوماتية كل فعل أو امتناع عمدي نشأ عن الاستخدام غير المشروع لتقنية المعلوماتية، ويهدف إلى الاعتداء على الأموال المادية أو المعنوية [1].

كما عرَّفها الفقيه الألماني تيدمان الجريمة المعلوماتية بأنَّها " تشمل كل أشكال السلوك غير المشروع الذي يُرتكب باستخدام الحاسب.[2]

عرَّفها الفقيه Leslie D.Ball بأنَّها فعل إجرامي يُستخدم الحاسب في ارتكابه كأداة رئيسية[3].

عرَّفها الفقيهان Totty et Hardcastle بأنَّها تلك الجرائم التي يكون قد وقع في مراحل ارتكابها بعض العمليات الفعلية داخل نظام الحاسب، وبعبارة أخرى هي الجرائم التي يكون دور الحاسب فيها إيجابيا أكثر منه سلبيا.

[1] Champy essai de définition de la fraube informatiques. rs.c.i .1988.

[2] Tiedeman. Sraube et autres délits d'assure commis à l'aibe l'ordinateur elctrouniqe. R.d.p .c.1984. n7 p61.

[3] Toty and hardCastle : computer related crine information technologie anbtchelaw u.k.1986.p26.

ويوسع البعض مفهوم الجريمة المعلوماتية لتشمل أي فعل متعمد مرتبط بأي وجه بالحاسبات، يتسبب في تكبد أو إمكانية تكبد المجني عليه للخسارة أو حصول أو إمكانية حصول مرتكبه على مكسب .

كما وسع الخبير الأمريكي (Parker) في تعريفها بأنَّها " كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية ترتبت عنه خسارة تَلحق بالمجني عليه أو مكسب يحققه الجاني .

و تجدر الإشارة إلى أنَّ الإخفاق في تعريف الجريمة المعلوماتية يفسره وجود اتجاه يسبغ بسهولة وصف الجريمة المعلوماتية على أية واقعة يلعب فيها الحاسب دورا عرضيا أو ثانويا.

إنَّ إعطاء هذا التعريف الواسع للجريمة المعلوماتية يدخل في نطاقها كل التصرفات غير المشروعة التي لها علاقة بالحاسوب أيا كانت هاته العلاقة وأيا كان دور الحاسوب فيها سواء كان وسيلة أو مناسبة لارتكاب التصرفات غير المشروعة أو كان موضوعا لها .

و يمكن حصر هذه الحالات كالتالي:

1- الحالات التي يكون فيها الإعلام الآلي كمناسبة لارتكاب الجريمة.

2- الحالات التي تكون فيها المعلوماتية كأداة لارتكاب الجريمة.

3- الحالات التي تكون فيها المعلوماتية كموضوع للجريمة.

إنَّ الاعتماد في تعريف الجريمة المعلوماتية على الوسيلة المستخدمة في ارتكابها أو المناسبة التي ارتكبت في إطار متقدم لأنَّه لتعريف الجريمة المعلوماتية وجب الرجوع إلى العمل الأساسي المكون لها، وليس فحسب إلى الوسائل المستخدمة لارتكابه وليس لمجرد أنَّ الحاسب قد استخدم في جريمة أن تعتبرها من الجرائم المعلوماتية .

المطلب الثاني: خصائص الجريمة المعلوماتية

إنّ ارتباط الجريمة المعلوماتية بجهاز الحاسوب وشبكة الانترنت أضفى عليها مجموعة من الخصائص المميزة لهذه الجريمة عن الجرائم التقليدية و هي:

1-الجريمة المعلوماتية متعدية الحدود أو جريمة عابرة للدول: المجتمع المعلوماتي لا يعترف بالحدود الجغرافية فهو مجتمع منفتح عبر شبكات تخترق الزمان و المكان دون أن تخضع لحرس الحدود فبعد ظهور شبكات المعلومات لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة فالمقدرة التي تتمتع بها الحواسيب وشبكاته في نقل كميات كبيرة من المعلومات وتبادلها بين أنظمة يفصل بينها آلاف الأميال قد أدت إلى نتيجة مفادها أنَّ أماكن متعددة في دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة في آن واحد، فالسهولة في حركة المعلومات عبر أنظمة التقنية الحديثة جعل بالإمكان ارتكاب جريمة عن طريق حاسوب موجود في دولة معينة بينما يتحقق الفعل الإجرامي في دولة أخرى.

هذه الطبيعة التي تتميز بها الجريمة المعلوماتية كونها جريمة عابرة للحدود خلقت العديد من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي لهذه الجريمة وكذلك حول تحديد القانون الواجب تطبيقه بالإضافة إلى إشكاليات تتعلق بإجراءات الملاحقة القضائية أو غير ذلك من النقاط التي تثيرها الجرائم العابرة للحدود بشكل عام[1].

2- صعوبة اثبات الجريمة المعلوماتية : حيث يصعب في كثير من الأحيان العثور على أثر مادي للجريمة المعلوماتية والسبب في ذلك في يعود إلى استخدام الجاني وسائل فنية وتقنية معقَّدة في كثير من الأحيان، كما يتمثل السلوك المكون للركن المادي فيها

[1] نهلة عبد القادر المومني، الجرائم المعلوماتية، ماجيستير في القانون الجنائي المعلوماتي، دارالثقافة،عمان،ط2010،ص 50،ص51.

بعمل سريع قد لا يستغرق أكثر من بعض ثواني، علاوة على سهولة محو الدليل والتلاعب به في الوقت الذي تفتقر فيه هذه الجرائم إلى الدليل المادي التقليدي، لذا فهذه الجرائم لا تترك أثرا لها بعد ارتكابها علاوة على صعوبة الاحتفاظ الفني بآثارها إن وجدت فليست أموال أو مجوهرات مفقودة وإنما هي أرقام تتغير في السِّجلات، ولذا فإنَّ معظم الجرائم المعلوماتية تمَّ اكتشافها بالمصادفة وبعد وقت طويل من ارتكابها[1].

3- صعوبة اكتشاف الجريمة المعلوماتية : فقد تقع جرائم معلوماتية معينة ولا يشعر أحد بأنَّ هناك جريمة إلَّا بعد مرور وقت طويل وربما لا تُكشف نهائيا والسبب في ذلك يعود إلى الجرائم المعلوماتية عادة تقع في بيئة افتراضية غير ملموسة في غالب الأحيان ولا يمكن استشعارها بشكل عادي محسوس فالجرائم المعلوماتية في أكثر صورها خفية لا يلاحظها المجني عليه أو لا يدري حتى بوقوعها والإمعان في حجب السلوك المكون بها وإخفائه عن طريق التلاعب غير المرئي في النبضات أو الذبذبات الإلكترونية التي تُسجل البيانات عن طريقها أمرا ليس عسيرا في الكثير من الأحوال بحكم توافر المعرفة و الخبرة في مجال الحاسبات غالبا لدى مرتكبها، كما أنَّ المجني عليه يلعب دورا رئيسيا في صعوبة اكتشاف وقوع الجريمة المعلوماتية حيث تحرس أكثر الجهات التي تتعرض أنظمتها المعلوماتية للانتهاك أو تُمنى بخسائر فادحة من جراء ذلك على عدم الكشف حتى بين موظفيها عما تعرضت له ونكتفي عادة باتخاذ إجراءات إدارية داخلية دون الإبلاغ عنها للسلطات المختصة تجنبا للإضرار بسمعتها ومكانتها وهو الثقة في كفاءتها .[2]

---

[1] محمد بن أحمد علي المقصودي، الجرائم المعلوماتية خصائصها و كيفية مواجهته قانونيا، محاضرات بمعهد الإدارة العامة، الرياض، تاريخ النشر 5 أفريل 2016،ص114.

[2] شول بن شهرة، مراد مشوش، مجلة المستقبل للدراسات القانونية والسياسية، لعدد الأول، معهد الحقوق والعلوم السياسية آفلو الأغواط، جوان سنة2020،ص5.

4- أسلوب ارتكاب الجريمة المعلوماتية: ذاتية الجرائم المعلوماتية تبرز بصورة أكثر وضوحا في أسلوب ارتكابها وطريقتها فإذا كانت الجرائم التقليدية تتطلب نوعا من المجهود العضلي الذي قد يكون في صورة ممارسة العنف والإذاء كما هو الحال في جريمة القتل أو الاختطاف ، أو في صورة الخلع أو الكسر وتقليد المفاتيح كما هو الحال في جريمة السرقة .... فإنَّ الجرائم المعلوماتية هي هادئة بطبيعتها لا تحتاج إلى العنف بل كل ما تحتاج إليه هو القدرة على التعامل مع جهاز الحاسوب بمستوى تقني يوظَّف في ارتكاب الأفعال غير المشروعة .[1]

وتحتاج كذلك إلى وجود شبكة المعلومات الدولية مع وجود مجرم يوظف خبرته أو قدرته على التعامل مع الشبكة للقيام بجرائم مختلفة كالتجسس أو اختراق خصوصيات الغير او التغرير بالقاصرين كل ذلك دون الحاجة إلى سفك الدماء.

5- الجريمة المعلوماتية تتم بالتعاون بأكثر من شخص : تتميز الجريمة المعلوماتية أنَّها تتم عادة بتعاون أكثر من شخص على ارتكابها إضرارا بالجهة المجني عليها وغالبا ما يشترك في إخراج الجريمة إلى حيِّز الوجود شخص متخصص في تقنيات الحاسوب والأنترنت يقوم بالجانب الفني من المشروع الإجرامي ، وشخص آخر من المحيط ومن خارج المؤسسة المجني عليها لتغطية عملية التلاعب وتحويل المكاسب إليه.

والاشتراك في إخراج الجريمة المعلوماتية إلى حيِّز الوجود قد يكون اشتراكا سلبيا وهو الذي يترجم بالصمت من جانب من يعلم بوقوع الجريمة في محاولة منه لتسهيل اتمامها، وقد يكون اشتراكا إيجابيا وهو غالبا كذلك يتمثل في مساعدة فنية أو مادية .

[1] نهلة عبد القادر المومني، المرجع السابق، ص57.

6- خصوصية مجرمي المعلوماتية: المجرم الذي يقترف الجريمة المعلوماتية الذي يطلق عليه المجرم المعلوماتي يتسم بخصائص معينة تميزه عن المجرم الذي يقترف الجرائم التقليدية (المجرم التقليدي) فإذا كانت الجرائم التقليدية لا أثر فيها للمستوى العلمي والمعرفي للمجرم في عملية ارتكابها – باعتبارها قاعدة عامة – فإنَّ الأمر يختلف بالنسبة للجرائم المعلوماتية فهي جرائم فنية تقنية في الغالب الأعم ، ومن يرتكبها عادة يكون من ذوي الاختصاص في مجال تقنية المعلومات أو على الأقل شخص لديه حد أدنى من المعرفة والقدرة على استعمال جهاز الحاسوب والتعامل مع شبكة الانترنت .

فعلى سبيل المثال فإنّ الجرائم المعلوماتية ذات طابع اقتصادي مثل التحويل الإلكتروني غير المشروع للأموال يتطلب مهارة وقدرة فنية وتقنية عالية جدا من قبل مرتكبها[1] .

المطلب الثالث: الطبيعة القانونية للجريمة المعلوماتية:

مما لاشك فيه أنَّ دراسة الجرائم بشكل عام والجرائم المعلوماتية بشكل خاص تدخل في نطاق دراسة القسم الخاص بقانون العقوبات ذلك الفرع المختص بدراسة كل جريمة على حدا متناولا عناصرها الأساسية والعقوبة المقررة لها إلّا أنَّ الجرائم المعلوماتية تمثل ظاهرة لجريمة ذات طبيعة خاصة تتعلق بالقانون الجنائي المعلوماتي[2]، على اعتبار أنَّ معظم هذا النمط من الجرائم يُرتكب ضمن نطاق المعالجة الإلكترونية للبيانات سواء إن كان في تجميعها أو في تجهيزها أم إدخالها إلى الحاسب المرتبط بشبكة المعلومات والغرض الحصول على معلومات معينة، كما قد ترتكب هذه الجرائم في مجال معالجة الكلمات أو معالجة النصوص وهذا النوع الأخير من الجرائم لا يعد أن يكون طريقة أوتوماتيكية تمكن المستخدم من تحرير

[1] نهلة عبد القادر المومني، المرجع السابق،ص58،ص59.

[2] محمد سامي الشوا، ثورة المعلومات و انعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة،سنة1994،ص 61.

وثائق ونصوص على الحاسوب مع توفير إمكانية التصحيح والتعديل والمسح والتخزين والاسترجاع والطباعة[1].

فجميع تلك العمليات هي وثيقة الصلة بالجرائم محل بحث وعليه لابد للجاني من استيعابها فضلا عن أنَّ الجاني قد يتعامل مع مفردات جديدة كالبرامج والمعطيات التي تشكل محل اعتداء أو تستخدم وسيلة له[2]، ولما كان لهذه الجرائم طبيعة خاصة هي قدرة شبكة المعلومات على نقل وتبادل معلومات ذات طابع شخصي وعام في آن واحد كالاعتداء على الخصوصية والعلَّة في ذلك توسع بنوك المعلومات بأنواعها .

علاوة على توسع الأفراد وسعيهم إلى ربط حواسبهم بالشبكة المذكورة مما يطرح تساؤلا حول طبيعة الخدمات والتطبيقات في هذه الشبكة ليتسنى معرفة ماهية النصوص والقوانين التي يجب تطبيقها على خدمات نشر المواقع وتبادل المعلومات فيها بشكل عام وبشكل خاص معرفة النظام القانوني للمسؤولية التي تفرض تطبيقها على الأشخاص المسؤولين من هذا النشر أو التبادل[3] بمعنى آخر هل يمكن وصف الخدمات والتطبيقات في شبكة المعلومات بأنَّها داخلة ضمن أحكام خدمات البريد أو التخابر الخاص أم أنَّها تدخل ضمن مفهوم الصحافة والمطبوعات والوسائل السمعية والبصرية أو مؤسسات التلفزيون والإذاعة[4]، أو هل أنَّه في كل الأحوال يجب اعتبار شبكة معلومات الأنترنت فضاء جديدا للمعلومات لا علاقة

[1] أحمد السمدان، النظام القانوني لحماية برامج الكمبيوتر، مجلة الحقوقي،الكويت،1987،ص124.

[2] جميل عبد الباقي، الجوانب الاجرائية للجرائم المتعلقة بالأنترنت، دار النهضة العربية، القاهرة،2001، ص96.

[3] طوني ميشال عيسى، التنظيم القانوني لشبكة الانترنت، طبعة 1، دار صابر للمنشورات، بيروت،2002، ص 373.

[4] جميل عبد الباقي صغير، المواجهة الجنائية لقرصنة البرامج التلفزيوني المدفوعة، دار النهضة العربية،القاهرة،2001،ص 11.

بشبكة البريد والاتصالات الخاصة ولا بعلم القواعد والمبادئ العامة حول مسؤولية واجبة التطبيق على الخدمات و التطبيقات فيها[1].

إنَّ التحري عن النظام القانوني الملائم لطبيعة الجرائم المعلوماتية عبر شبكة المعلومات يهدف بشكل أساسي إلى معرفة ما هي النصوص القانونية الوضعية التي يجب تطبيقها على خدمات نشر المواقع والمعلومات فيها فضلا عن معرفة النظام القانوني للمسؤولية الذي يفترض تطبيقه على الأشخاص المسؤولين عن هذا النشر وخصوصا لتأرجح موقف الدول بهذا الشأن، من هذا يتضح أنَّ الطبيعة القانونية الخاصة لهذه الجرائم من خلال المجال الذي يمكن أن ترتكب فيه .ومن جانب آخر المحل الذي يقع عليه الاعتداء المذكور .

فالتطور السريع في مجال المعلوماتية قد يفسح المجال لاقتناء الوسائل الإلكترونية تمكن المتجاوزين من استخدامها في ارتكاب جرائم مختلفة لأنّ الإجرام المعلوماتي يتعلق بكل سلوك غير مشروع فيما يتعلق بالمعالجة الآلية للبيانات وإدخال المعلومات ونقلها ومن ثمَّ يتحتم ضمه إلى نطاق القانون الجنائي على الرغم من أنَّ معظم نصوصه عاجزة عن مواكبة التطور المعلوماتي أو لما يحويه من فراغ تشريعي في هذا المجال[2] .

ومن جانب آخر تتخذ هذه الجرائم طبيعة خاصة من حيث تكييفها القانوني إذ لم تكن القواعد التقليدية مخصصة لهذه الظواهر الإجرامية المستحدثة، فالنصوص التقليدية وُضعت وفقا لمعايير معينة في حين كان مفهوم الحقوق الشخصية في شبكة المعلومات هو الذي يردُ على إنتاج الفكر البشري وهو يتعلق بشخص المرء وأمواله وممتلكاته كما أن تطبيق النصوص التقليدية على الجرائم المعلوماتية يثير مشاكل عديدة في مقدمتها مسألة الإثبات[3]

[1] طوني مشال عيسى، المرجع السابق، ص 388 و ما بعدها.

[2] عبد الستار سالم الكبيسي، المسؤولية الجنائية الناشئة عن استعمال الحاسوب، سلسلةالمائدةالحرة من ندوة القانون والحاسوب، بيت الحكمة،بغداد،1999، ص137.

[3] جميل عبد الباقي صغير، الجوانب الاجرائية، المرجع السابق، ص 4.

كالحصول على أثر مادي إذ يمكن الجاني محو أدلة في وقت قصير لا يتجاوز لحظات وخاصة في حالة تفتيش الشبكات أو عمليات اعتراض الاتصال فقد تكون البيانات التي يُجرى البحث عنها مشفرة الدخول إلَّا لأحد العاملين على الشبكة ومن هنا تُثار مسألة مدى مشروعية إجباره على فك الشفرة [1] و مما يزيد صعوبة الأمر بملاحقة جناة الجرائم المعلوماتية للذين يقيمون في دولة آخرى.

المبحث الثاني: أنواع الجرائم المعلوماتية

إنَّ أنواع الجرائم المعلوماتية كثيرة حيث لم يوضع لها معايير محددة من أجل تصنيفها وها راجع إلى التطور المستمر للشبكة والخدمات التي تقدمها وقد تضاربت الآراء لتحديد انواع تلك النوع من الجرائم فهناك من عددها بحسب موضوع الجريمة وآخر قسَّمها بحسب طريقة ارتكابها وقد صنفها معهد العدالة القومي بالولايات المتحدة الأمريكية عام 1985 بحسب علاقتها بالجرائم التقليدية ، الصنف الأول يتمثل في الجرائم المنصوص عليها في قانون العقوبات متى ارتكبت باستعمال الشبكة، أما الصنف الثاني تضمن دعم الأنشطة الإجرامية ويتعلق الأمر بما تلعبه الشبكة من دور في دعم جرائم غسيل الأموال ، المخدرات الاتجار بالأسلحة واستعمال للشبكة كسوق للترويج غير المشروع في هذه المجالات و الصنف الثالث بجرائم الدخول في نظام المعالجة الآلية للمعطيات، وتقع على البيانات والمعلومات المكونة للحاسوب وتغييرها أو تعديلها أو حذفها مما يغير مجرى عمل الحاسوب و الصنف الرابع فتضمن جرائم الاتصال وتشمل كل ما يرتبط بالهاتف وما يمكن أن يقع عليها من انتهاكات باستغلال ثغرات شبكة الانترنت، وأخيرا صنف الجرائم المتعلقة بالاعتداء على حقوق الملكية

[1] هلال عبدلاه أحمد،التزام الشاهد بالإعلان الجرائم المعلوماتية،ط1، دار النهضة العربية،القاهرة،1997،ص 66

الفكرية الأدبية والفنية ويتمثل في عملية نسخ البرامج دون إذن صاحبها وتسويقها واستغلالها بأي صورة طبقا لقانون حماية الملكية الفكرية والأدبية [1].

ونتطرق لهدا المبحث الى ثلاث مطالب المطلب الأول الجرائم المعلوماتية الواقعة باستعمال نظام المعلوماتي، المطلب الثاني الجرائم المعلوماتية التي تتم على نظام المعلوماتي والمطلب الثالث جرائم الاعتداء على المعلومات المدرجة بالنظام المعلوماتي.

المطلب الأول: الجرائم المعلوماتية الواقعة باستعمال النظام المعلوماتي

ينقسم هدا المطلب الى أربع فروع الأول يتضمن الجرائم الواقعة على الأموال، والثاني الجرائم الواقعة على الأشخاص و الثالث الجرائم الواقعة على مؤسسات الدولة والمؤسسات الأمنية والعسكرية و الفرع الرابع الجرائم الواقعة على حقوق الملكية الفكرية والادبية والفنية، وهنا لا يكون النظام المعلوماتي هو محل الجريمة بل يكون الحاسب الآلي هو الوسيلة لتسهيل النتيجة الإجرامية باستخدام النظام المعلوماتي، ويكون الهدف من ورائها الربح بطريقة غير مشروعة، الاعتداء على أموال الغير، الاعتداء على أمن الدولة و أسرارها.

الفرع الأول: الجرائم الواقعة على الأموال.

أصبحت المعاملات الشراء والبيع والإيجار تتم عبر الشبكة المعلوماتية، وما انجر عليها من وسائل الدفع والوفاء، فابتكرت معه طرق ووسائل للسطو على هذا التداول المالي بطريقة غير مشروعة كالتحويل الإلكتروني ، السرقة، القرصنة، وغيرها.

1-السرقة الواقعة على البنوك : يتم سرقة المال بالطرق المعلوماتية عن طريق اختلاس البيانات والمعلومات الشخصية للمجني عليهم، والاستخدام لشخصية الضحية ليقوم

[1] سورية ديش،أنواع الجرائم الإلكترونية و اجراءات مكافحتها، حامعة جيلالي اليابس، سيدي بالعباس،الجزائر،ص 240، ص 241.

بعملية السرقة المتخفية ما يؤدي بالبنك إلى التحويل البنكي للأموال الإلكتروني أو المادي إلى الجاني، حيث يستخدم الجاني الحاسب الآلي لدخول شبكة الأنترنت و الوصول إلى المصارف والبنوك، وتحويل الأموال الخاصة بالعملات إلى حسابات أخرى[1].

وعملية السرقة الإلكترونية كالاستيلاء على ماكينات الصرف الآلي والبنوك يتم فيها نسخ البيانات الإلكترونية لبطاقة الصرَّاف الآلي، ومن ثمَّ استخدامها لصرف أموال من حسابات الضحية أو إنشاء صفحة أنترنت مماثلة جدا لموقع أحد البنوك الكبرى أو المؤسسات المالية الضخمة لتطلب من العميل إدخال بياناته اوتحديث معلوماته بقصد الحصول على بياناته المصرفية وسرقة رسائل البريد الواردة من مصادر مجهولة التي توهم صاحب البريد الإلكتروني بفوزه بإحدى الجوائز أو اليانصيب وتطالبه بموافاة الجهة برقم حسابه المصرفي والأمثلة كثيرة ....

2-تجارة المخدرات عبر الأنترنت : تتعلق بالترويج للمخدرات وبيعها والتحريض على استخدامها، و صناعتها بمختلف أنواعها.

3-غسيل الأموال: تُمارس عبر الانترنت حيث استفاد الجناة ما وصلت إليه عصر التقنية المعلوماتية لتوسيع نشاطهم غير المشروع في غسيل أموالهم بتوفير السرعة، وتفادي الحدود الجغرافية، والقوانين المعيقة لغسيل الأموال وكذا لتشفير عملياتهم وسهولة نقل الاموال واستثمارها لإعطائها الصبغة الشرعية[2] .

4- الاستعمال غير الشرعي للبطاقات الائتمانية : رافق استخدام البطاقات الائتمانية الاستيلاء عليها باعتبارها نقود الكترونية وذلك إما بسرقة أرقام البطاقات ثم بيع

[1] عباس أبو شامة، التعريف بالظواهر الاجرامية المستحدثة، الندوة العلمية للظواهر العلمية المستحدثة وسبل مواجهتها، تونس،أيام 29،30 جوان،1999.

[2] صالحة العمري، جريمة غسيل الأموال وطرق مكافحتها، مجلة الاجتهاد القضائي، مخبر أثر الاجتهاد القضائي على حركة التشريع ، العدد الخامس، جامعة محمد يخدر، بسكرة، ص 179.

المعلومات للآخرين من خلال الحصول على كلمة السر المدرجة في ملفات أنظمة الحاسب الآلي للضحية عن طريق الاحتيال ، وذلك بإيهامه بحصول ربح، فيقدم الضحية معلومات يُمكن الجاني من التصرف في ماله أو إساءة استخدام الغير لبطاقة الائتمانية[1]، كأن يقوم السارق باستعمال البطاقة للحصول على السلع والخدمات أو سحب مبالغ مالية بموجبها من أجهزة التوزيع الآلي أو السحب باستخدام بطاقات مزورة[2].

الفرع الثاني: الجرائم الواقعة على الأشخاص

فرغم الإيجابيات والفوائد التي جاءت بها الشبكة المعلوماتية والتسهيلات المقدمة للفرد، إلَّا أنَّها جعلته أكثر عرضة للانتهاك، ومنها:

1- جريمة التهديد: وهو الوعيد ويقصد به زرع الخوف في النفس، بالضغط على إرادة الإنسان وتخويفه من أضرار ما ستلحقه أو ما ستلحق أشخاص له بهم صلة، ويجب أن يكون التهديد على قدر من الجسامة المتمثلة بالوعيد بإلحاق الأذى ضد نفس المجني عليه أو ماله أو ضد نفس أو مال الغير، ولا يشترط أن يتم إلحاق الأذى فعلا أي تنفيذ الوعيد، لأنَّها تشكل جريمة أخرى قائمة بذاتها، تخرج من إطار التهديد إلى التنفيذ الفعلي، وقد يكون التهديد مصحوبا بالأمر أو طلب القيام بفعل أو الامتناع عن الفعل أو لمجرد الانتقام ولقد أصبحت الأنترنت الوسيلة لارتكاب جرائم التهديد والتي تحتوي في حد ذاتها عدة رسائل لإيصال التهديد للمجني عليه لما تتضمنه من نوافذ وجدت للمعرفة كالبريد الإلكتروني أو الويب ...

[1] يوسف صغير، الجريمة المرتكبة عبر الانترنت، ماجستير في قانون الأعمال، كلية الحقوق والعلوم السياسية،حامعة مولود معمري، تيزي وزوو، 2013، ص45.

[2] أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، القاهرة، طبعة الثانية، 2006، ص 196.

2- انتحال شخصية: وهو استخدام شخصية فرد للاستفادة من ماله أو سمعته أو مكانته ولقد تميزت بسرعة الانتشار خاصة في الأوساط التجارية وتتم قدر كبير من المعلومات الشخصية المراد انتحال شخصيته، للاستفادة منها لارتكاب جرائمه عن طريق استدراج الشخص ليدلي بمعلوماته الشخصية الكاملة كالاسم ،والعنوان الشخصي. رقم بطاقة الائتمان للتمكن من الوصول لماله أو سمعته ..... عن طريق الغش[1].

3-انتحال شخصية أحد المواقع: ويتم ذلك عن طريق اختراق احد المواقع للسيطرة عليه ليقوم بتركيب برنامج خاص به ، كاسم المواقع المشهورة[2] .

4-جرائم السب والقذف: للمساس بشرف الغير وسمعتهم، واعتبارهم ويكون القذف والسب كتابيا أو عن طريق المطبوعات أو رسوم عبر البريد الإلكتروني أو الصوتي وصفحات الويب بعبارات تمس الشرف، فيقوم المجرم بنشر معلومات تكون مغلوطة عن الضحية وقد يكون شخصا طبيعيا أو معنويا لتصل المعلومات المراد نشرها إلى أعداد كبيرة من مستخدمي الأنترنت.

5-المواقع الإباحية والدعارة : وجود مواقع على شبكة الأنترنت تحرِّض على ممارسة الجنس للكبار والقصَّر وذلك بنشر صور جنسية للتحريض على ممارسة المحرمات والجرائم المخلة بالحياء عن طريق صور أفلام، رسائل ... بالإضافة إلى انتشار الصور ومقاطع الفيديو المخلة بالآداب على مواقع الأنترنت من قِبل الغزو الفكري لكي يتداولها الشباب وإفساد أفكارهم وإضعاف إيمانهم، وتوفر الشبكة تسهيلا للدعارة

[1] سورية ديش، المرجع السابقً،ص241،ص242.

[2] محمد بن عبد الله بن علي المنشاوي، جرائم الأنترنت في المجتمع السعودي، ماجيستير في العلوم الشرقية، أكاديمية نايف، العربية للعلوم الأمنية، الرياض ،2003، ص 55.

عبر الالاف من المواقع الاباحية وتسوق الدعارة وتستثمر لها مبالغ ضخمة مع استخدام احدث التقنيات[1].

6- التشهير وتشويه السمعة: يقوم المجرم بنشر معلومات قد تكون سرية أو مضلِّلة أو مغلوطة عن ضحيته والذي قد يكون فردا أو مؤسسة تجارية أو سياسية.

تتعدَّد الوسائل المستخدمة في هذا النوع من الجرائم لكن في مقدمة هذه الوسائل إنشاء موقع على الشبكة يحوي المعلومات المطلوب نشرها أو إرسال هذه المعلومات عبر القوائم البريدية إلى أعداد كبيرة من المستخدمين و يُضم لهذه الجرائم كذلك تشويه السمعة الشائعات و الأخبار الكاذبة لمحاربة الرموز الفكرية والسياسية وحتى الدينية من أجل تشكيك الناس في مصداقية هؤلاء الأفراد وقد يكون الهدف من ذلك هو الابتزاز.

كل هذه الجرائم الماسة بالأشخاص تدخل ضمن الحياة الخاصة للأفراد التي كفلها القانون وفي مقدمته الدستور الجزائري حيث تنص المادة 40 [2]منه " تضمن الدولة عدم انتهاك حرمة الإنسان". وعليه يمكن استخدام الشبكة المعلوماتية في الاعتداء على حرمة الفرد وحياته الخاصة والحريات العامة للأفراد وهو مخالف للقانون ومُعاقب عليه.

الفرع الثالث : الجرائم الواقعة عى مؤسسات الدولة والمؤسسات الأمنية والعسكرية

من أهم الجرائم التي تهدف للمساس بمؤسسات الدولة والمؤسسات الأمنية والعسكرية جرائم الإرهاب الإلكتروني التي تتم عن طريق جرائم الاختراقات وتدمير المواقع الإستراتيجية

[1] سورية ديش، المرجع السابق، صً242،ص 243.

[2] ينظر للمادة1/40من الدستور 1996، ج ر، رقم 76، المؤرخة في 8 ديسمبر1996،المعدل والمتمم بالقانون رقم1/16 المؤرخ في 6 مارس 2016، ج ر، رقم 14المؤرخة في 7 مارس 2016.

الحكومية واختراق المواقع الرسمية والشخصية فمثلا تمت مهاجمة نظام البانتاغون سنة 1995 حوالي 250000 مرة نجحت حوالي 160000 عملية اختراق[1].

يتميز الإرهاب الإلكتروني لكونه جريمة عابرة للحدود، صعبة الإثبات تتم عادة بتعاون أكثر من شخص ومن مظاهرها مثلا نجد الإشادة بالأعمال الإرهابية ، إنشاء المواقع الإرهابية الإلكترونية ومن أمثلتها موقع " النداء " وهو الموقع الرسمي لتنظيم القاعدة ، " ذروة السنام " وهي صحيفة إلكترونية لتنظيم القاعدة .

" البتار" مجلة عسكرية إلكترونية لتنظيم القاعدة، ومن نماذج الحروب الرقمية نجد الهجمة العسكرية الروسية على مواقع حكومية جورجية أدَّت إلى إلحاق أضرار معنوية بالجيش الجورجي وخلال سنة 2010 تعرضت المحطات النووية الإيرانية لهجوم دودة الكترونية مصدرها الولايات المتحدة الأمريكية وإسرائيل أدَّت إلى تعطيل أجهزة الطرد المركزي وتسببت في تباطؤ البرنامج النووي الإيراني، وفي نفس السنة نال موقع ويكيليكس شهرة كبيرة بسبب التسريبات التي نشرها وتتعلق ب 90000 وثيقة سرية حول الحرب في أفغانستان ونشر 480 وثيقة حول الحرب في العراق وتتعلق بوثائق سرية مسربة من مراسلات وزارة الخارجية الأمريكية ، و يُعدُّ ويكيليكس واحدا من أقوى و أهم المنظمات المجهولة التي تحتوي على عدد هائل ومجهول من الهاكرز.

نجد كذلك جرائم التجسس يقوم المجرمون بالتجسس على الدول والمنظمات والشخصيات والمؤسسات الوطنية والدولية، وتستهدف بخاصة التجسس العسكري، السياسي و الاقتصادي وذلك باستخدام التقنية المعلوماتية، وتمارس من قِبل دولة على دولة أو من شركة على شركة..... وذلك بالاطلاع على المعلومات الخاصة المؤَمنة في جهاز آلي، وغير مسموح بالاطلاع عليه كأن تكون من قبل أسرار الدولة .

[1] أمير فرج يوسف، الجرائم المعلوماتية على شبكة الانترنت، دار المطبوعات الجامعية، الاسكندرية، 2009،ص208.

الفرع الرابع: الجرائم الواقعة على حقوق الملكية الفكرية والأدبية والفنية

يمكن أن يكون النظام المعلوماتي وسيلة فعَّالة للاعتداء على حقوق الملكية الفكرية و الأدبية ومثال ذلك استخدام النظام المعلوماتي في السطو على بنوك المعلومات التي تتضمنها برامج نظام معلوماتي آخر أو حالة تخزين واستخدام هذه المعلومات أو التفريط فيها دون إذن صاحبها، ذلك أنَّ استخدام معلومة معينة دون إذن صاحبها يتضمن اعتداء على حق من الحقوق المعنوية إضافة إلى كونه اعتداء على قيمتها المالية كون أنَّ للمعلومة قيمة أدبية بجانب قيمتها المادية ويندرج ضمن الحقوق الفكرية، كذلك براءات الاختراع إذ تمثل فكرة للمخترع تحتوي على حق معنوي و آخر مالي للمخترع[1]، وقد نص المشرع الجزائري على حقوق الملكية الفكرية وبراءة الاختراع من خلال عدة نصوص قانونية نذكر من بينها :

المادة 38 من الدستور الجزائري التي تنص على أنَّ:" حرية الابتكار الفكري والفني والعلمي مضمونة للمواطن".

حقوق المؤلف يحميها القانون. لا يجوز حجز أي مطبوع أو تسجيل أو أية وسيلة أخرى من وسائل التبليغ والإعلام إلَّا بمقتضى أمر قضائي

الأمر 03 / 05 المؤرخ في 19 جويلية 2003 المتعلق بحقوق المؤلف والحقوق المجاورة والأمر 07/03 المؤرخ في 19 جويلية 2003 المتعلق ببراءات الاختراع.

[1] أحمد خليفة الملط ،الجرائم المعلوماتية، دار الفكر الجامعي، الطبعة الثالثة،2006،ص184.

"المطلب الثاني: الجرائم المعلوماتية التي تتم على النظام المعلوماتي

إضافة إلى الجرائم المعلوماتية التي تقع باستخدام النظام المعلوماتي، هناك نوع آخر من الجرائم المعلوماتية بالاعتماد على التصنيف الذي يقوم على محل الجريمة المعلوماتية، يتمثل في الجرائم الواقعة على النظام المعلوماتي التي قد تستهدف إمَّا المكونات المادية للنظام المعلوماتي أو المكونات المنطقية أو المعلومات المدرجة بالنظام المعلوماتي وهذا ما سنتطرق إليه بالتفصيل من خلال الفروع التالية

الفرع الأول : جرائم الاعتداء على المكونات المادية للنظام المعلوماتي

يقصد بالمكونات المادية للنظام المعلوماتي تلك الأجهزة والمعدات الملحقة به والتي تستخدم في تشغيله كالأسطوانات، الشرائط و الكابلات ..... والنتيجة للطبيعة المادية لهذه المكونات فالاعتداء عليها يكون عن طريق جرائم عادية و تقليدية[1]، كأن تكون محل للسرقة أو خيانة الأمانة أو الإتلاف العمدي كإحراقها أو ضرب الآلات بشيء ثقيل أو حاد أو العبث بمفاتيح التشغيل أو خربشة الشريط أو إفساد اسطوانات التشغيل مغناطيسيا بتعريضها إلى أي مجال مغناطيسي مُتلف، ويترتب على هذا الإتلاف خسائر كبيرة[2]، ومن أمثلة ذلك ما حدث في فرنسا حيث أدَّى إلى إتلاف معدَّات مؤسسة كبيرة متخصصة في بيع الأنظمة وتوثيق المعلومات الحسابية إلى خسائر مالية معتبرة قُدِّرت ب 5 ملايين فرنك فرنسي[3] ويرى البعض من الفقهاء أنَّه يندرج ضمن هذه الطائفة من الجرائم المعلوماتية سرقة وقت الآلة، فقد يلجأ العاملين بالنظام المعلوماتي إلى استخدامه في أعمال خاصة بهم وعليه تكون واقعة

---

[1] أحمد خليفة المنط، المرجع السابق، ص 176.

[2] دكي دكي أمين حسونة، جرائم الكمبيوتر والجرائم الاخرى في مجال التكتيك المعلوماتي، المؤتمر السادس للجمعيةالمصريةللقانون الجنائي ،القاهرة،من25 الى 28 اكتوبر1993، ص471.

[3] Rose (philipp) op –cit p58 –59

السرقة مُنْصبة على وقت الجهاز الذي يمكن تقويمه ماليا وليس على الأشياء المادية بمعنى الكلمة[1].

وتجدر الإشارة إلى أنَّ خطورة واقعة السرقة لا تكمن في الشيء المسروق لضآلة قيمته بل بالمقارنة بما تحتويه هذه المكونات المادية من معلومات تقدر خسارتها بأموال طائلة.

الفرع الثاني: الجرائم الواقعة على البرامج التطبيقية

تستلزم هذه الطائفة من الجرائم المعلوماتية معرفة فنية عالية في مجال البرمجة، وقد تقع هذه الجرائم إمَّا على البرامج التطبيقية و إمَّا على برامج التشغيل وسنتطرق إلى هاتين الصورتين فيما يلي:

1-تعديل البرنامج: الهدف الرئيسي من تعديل هذه البرامج يتمثل في اختلاس النقود وتكثر هذه الجرائم في مجال الحسابات[2] أوّلا ثم التلاعب فيه لتحقيق أكبر قدر من الاستفادة المادية

ومن أمثلة ذلك قيام مبرمج بأحد البنوك الأمريكية بإدارة الحسابات بتعديل برنامج بإضافة دولار واحد على كل حساب يزيد عن عشرة دولارات وقام بقيد المصاريف الزائدة في حساب خاص به أطلق عليه اسم Zzwick وحصل على إثر ذلك على مئات الدولارات كل شهر وكان من الممكن يستمر هذا العمل الإجرامي لولا أنَّ البنك أراد بمناسبة تأسيس شركة جديدة للدعاية أن يكافئ أوّل وآخر عميل له ليكتشف عدم وجود ما يدعى Zzwick[3] ، وهناك نظام آخر يسمى "Salami" ويتم الاختلاس بموجب هذا النظام باستقطاع مبالغ زهيدة وعلى

[1] André Lucas. Le droit de lenformatiqe poris puf 1987.P519/521

[2] احمد خليفة الملط، المرجع السابق، ص173.

[3] Dulauroy et rocco (a.m) l'informatique nouvelle. Avril 1976.les escrocs a l'informatique. Les nouvelles économistes. Les octobres.1979.n202.

فترات زمنية طويلة ومتباينة من خلال صفقات عديدة لا يترتب عليها تحقيق فائدة كبيرة، وقد حقق بموجب هذا البرنامج أحد المستخدمين الأمريكيين بإحدى المنشآت التجارية الكبرى يدعى E.Royce في خلال ست سنوات ما يقرب 2 مليون دولار[1].

2- التلاعب في البرنامج : يأخذ التلاعب في البرنامج عدة أشكال فقد يتم عن طريق استعمال القنبلة المنطقية[2] أو عن طريق قيام أحد المبرمجين بزرع برنامج فرعي غير مسموح به في البرنامج الأصلي يسمح له بالدخول غير المشروع في العناصر الضرورية لأي نظام معلوماتي ويصعب اكتشاف هذا البرنامج لصغره ودقته[3] وهي عبارة عن برنامج اوجزء من برنامج ينفذ في لحظة محددة اوكل فترة زمنية منتظمة ويتم وضعه في شبكة معلوماتية بهدف او حالة فحوى النظام بغرض تسهيل تنفيذ عمل غير مشروع.

الفرع الثالث: الجرائم الواقعة على برامج التشغيل

تُعدُّ برامج التشغيل تلك البرامج المسؤولة عن عمل النظام المعلوماتي من حيث قيامها بتنظيم و ضبط ترتيب التعليمات الخاصة بالنظام، وتقوم الجريمة المعلوماتية في هذه الصورة عن طريق تزويد البرنامج بمجموعة تعليمات إضافية يسْهل الوصول إليها بواسطة شفرة تسمح الحصول على جميع المعطيات التي يتضمنها النظام المعلوماتي[4]، ويتحقق هذا النوع من الجرائم المعلوماتية في شكلين :

أولا: المصيدة

[1] أحمد خليفة الملط، المرجع السابق، ص 174.

[2] أحمد خليفة الملط،المرجع السابق،ص545.

[3] وقد قام مبرمج بأحد البنوك زرع برنامج فرعي بمنشئة بالكيانات المنطقية بإدارة حسابات يتجاهل كل عمليات السحب التي تتم من قبله عن طريق بطاقات أو شيكات حسابية اد يتحمل البنك نتيجة دلك هده الحسابات في باب ميزانية الادارة.

[4] أحمد خليفة المنط، المرجع السابق،ص175.

تتمثل هذه الصورة في إعداد المبرمج برنامج به أخطاء وعيوب عمدا، لا يُكتشف بعضها عند استخدام البرنامج ، إذ يترك المبرمج ممرات خيالية وفواصل وتفرعات في البرنامج حتى يستطيع فيما بعد تنفيذ التعديلات الضرورية بإدخال تفرعات إضافية أو إحداث مخارج وسيطة للولوج داخل النظام المعلوماتي و الوصول إلى كل المعلومات التي تحويها الذاكرة .

و بهذه التقنية يمكن للمبرمج استخدام البرنامج في أي وقت وِفق أهوائه وبذلك يصبح هو المهيمن على النظام وعلى صاحب العمل المعتدى عليه[1].

ثانيا: تصميم برنامج وهمي

وتقوم هذه الصورة من خلال قيام المبرمج بوضع برنامج يصعب اكتشافه مخصص خصيصا لارتكاب الجريمة ومراقبة تنفيذها، ومن أمثلة ذلك قيام إحدى شركات التأمين الأمريكية في مدينة لوس أنجلس بواسطة مبرمجيها تصميم برنامج وهمي يقوم بتصنيع وثائق تأمين لأشخاص وهميين بلغ عددهم 46000 بهدف تقاضي هذه الشركة من اتحاد شركات التأمين عمولات من نظيرتها.

وقد قام مبرمج بأحد البنوك زرع لرنامج فرعي بمنشاة بالكيانات المنطقية بادارة الحسابات يتجاهل كل عمليات السحب التى تتم من قبله عن طريق بطاقات او شكات حسابية اذ يتحمل البنك نتيجة ذلك هذه الحسابات في باب ميزانية الادارة ،تقاضي هذه الشركة من اتحاد شركات التأمين عمولات من نظيراتها[2].

[1] محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضةالعربية،1994،ص82.

[2] Equity fuding life insurence l'informatique nouvelle mai.1976

المطلب الثالث : جرائم الاعتداء على المعلومات المدرجة بالنظام المعلوماتي

للمعلومة المعالجة آليا أهمية كبيرة باعتبارها أساس عمل النظام المعلوماتي ولما لها من قيمة اقتصادية وبهذا تعد هدفا للجرائم المعلوماتية من خلال التلاعب فيها أو عن طريق إتلافها وها ما سنتطرق إليه فيما يأتي :

الفرع الأول: التلاعب في المعلومات

يتم التلاعب في المعلومات الموجودة داخل النظام المعلوماتي بطريق مباشر أو غير مباشر فأمَّا التلاعب المباشر فيتم عن طريق إدخال معلومات بمعرفة المسؤول عن القسم المعلوماتي و يأخذ هذا التلاعب عدَّة صور كضم المستخدمين غير الموجودين بالعمل لاسيما في المنشآت التي تضم عددا كبيرا من العاملين المؤقتين ودائمي التغيير بهدف الحصول على مرتباتهم[1] أو بالإبقاء على ملفات مستخدمين تركوا العمل للحصول على مبالغ مالية شهرية أو عن طريق عمل التحويلات لمبالغ وهمية لدى العاملين بالبنوك باستخدام النظام المعلوماتي بالبنك وتسجيلها وإعادة ترحيلها وإرسالها إلى حساب آخر في بنك آخر بهدف اختلاس تلك النقود[2]، في حين التلاعب غير المباشر يتم عن طريق التدخل غير المباشر لدى المعلومات المسجلة بالنظام المعلوماتي باستخدام أحد وسائط التخزين أو بواسطة التلاعب عن بعد باستخدام أدوات معينة .ومعرفة أرقام وشفرات الحسابات[3] ويتخذ ذلك عدة صور من بينها التلاعب في الشرائط الممغنطة وقد قام في هذا الصدد أحد الموظفين بأحد فروع الشركة الفرنسية ISOVENS IGOBAIN بإرسال شريط ممغنط

---

[1] قام احد المسؤولين عن القسم المالي بإحدى الشركات الفرنسية اختلاس اكثر من مليون فرنك فرنسي ووضعه في حسابه وحساب شركائه باستعمال هاته الطريقة.

[2] وقد تم ضبط المستخدم يعمل لدى فرع مصرفي تابع لبنك INBO–suej بفرنسا كونه حول مبالغ تقدر بسبعة ملايين فرنك فرنسي.

[3] أحمد خليفة الملط، المرجع السابق، 179.

يحتوي139 إذن دفع، وعند معالجته بالبنك بالقسم المعلوماتي تمَّ رفض نسخه لِعَيب في طول الشريط ، وقد قال الخبراء أنَّه لو نجحت هذه العملية لتمَّ النصب على البنك بحوالي 21 مليون فرنك فرنسي[1].

كما قد يتحقق التلاعب غير المباشر في المعلومات عن طريق التلاعب عن بعد باستخدام الجاني كلمة السر أو مفتاح الشفرة أو أداة ربط بالمركز المعلوماتي لأي جهة، وتكمن خطورة هذه الصورة في إمكانية تسلل الجاني إلى المعلومات المخزنة بالنظام المعلوماتي و الحصول على المنفعة المالية التي يريدها من مسافات بعيدة.

الفرع الثاني : إتلاف المعلومات

قد يهدف الجاني من خلال ارتكابه الجريمة المعلوماتية إلى إتلاف المعلومات المخزنة بالنظام المعلوماتي ويتَّخذ الإتلاف عدَّة صور فقد يتم عن طريق طرق الإتلاف العادية كالحريق أو الضرب أو السرقة أو عن طريق استبدال أو محو معلومات ، ويشكل استبدال المعلومات نوعا من جرائم الغش أو التزوير المعلوماتي وهو على درجة كبيرة من الخطورة لأنَّه في حالة نجاحه يستمر لوقت طويل قبل اكتشافه ويتولد عنه مكاسب كبيرة بمجرد استبدال رقم بآخر أو إحلال رقم مكان آخر[2] فمثلا هناك مجموعة من المستخدمين الإداريين استطاعوا خلال سنوات قليلة مضاعفة رواتبهم عن طريق النظام المعلوماتي[3] وقد استعمل شخص يدعى Vladimir loriblitt بإسرائيل طريقة تدعى ب Bluff إذ كان يعمل بوزارة المالية وقام بإدخال فواتير وهمية لا حصر لها وتحويل ما تم سداده من هذه الفواتير لحساب الشركات الوهمية التي اصطنعها .

[1] Trip de paris. 12 e me ch. Corre. Jugement. Du 13 janv. 1982.dalloz s 1982.p502.

[2] أحمد خليفة الملط، المرجع السابق،ص182.

[3] محمد سامي الشوا، المرجع السابق، ص75.

وأمَّا محو المعلومة فهو من أسهل طرق الإتلاف كون أنَّه من خصائص الجرائم المعلوماتية، قدرة الجاني على محو آثار جريمته في فترة وجيزة جدا لا تتعدى الضغط على زر بسيط في لوحة المفاتيح أو البرنامج عن طريق الفأرة فمثلا قام شخصان باختلاس مبلغ يقدر ب 61000 دولار مرسلة من شركات التأمين إلى إحدى المراكز الجامعية عن طريق محو الحسابات القائمة في سجلات النظام المعلوماتي الخاص بالمركز وجعلها غير قابلة للتحصيل.[1]

[1] le monde informatique 21 fév1983 sous le titre « le délinquance en cal belanc se parte lien.

الفصل الثاني

المكافحة الإجرائية للجريمة المعلوماتية

الفصل الثاني: المكافحة الإجرائية للجريمة المعلوماتية

نظرا للأهمية التي تلعبها المكافحة الإجرائية للجريمة المعلوماتية في إطار المكافحة الموضوعية قمنا بتقسيم هذا الفصل الى مبحثين وذلك على النحو التالي المبحث الأول يتضمن مفهوم المكافحة الاجرائية للجريمة المعلوماتية والذي تم تقسيمه الى مطلبين المطلب الاول تناولنا فيه تعريف المكافحة الاجرائية للجريمة المعلوماتية وأسبابها أما المطلب الثاني فتضمن الاجراءات المنصوص عليها في الاتفاقيات الدولية.

أما المبحث الثاني فتناولنا فيه نطاق المكافحة الاجرائية للجريمة المعلوماتية وهو بدوره تم تقسيمه الى ثلاث مطالب حيث تناولنا في المطلب الاول معاينة مسرح الجرائم المعلوماتية وتفتيشها أما المطلب الثاني فتطرقنا من خلالها الى القواعد العامة للتفتيش النظام المعلوماتي واخيرا تناولنا في المطلب الثالث مكافحة الجريمة المعلوماتية في القانون الجزائري .

المبحث الأول: مفهوم المكافحة الإجرائية للجريمة المعلوماتية

سوف نتناول من خلال هذا المبحث مطلبين هما:

المطلب الأول يتضمن تعريف المكافحة الإجرائية وأسبابها، بينما يتضمن المطلب الثاني الإجراءات المنصوص عليها في الاتفاقيات الدولية.

المطلب الأول: تعريف المكافحة الإجرائية وأسبابها

لقيام الجريمة لابد من توافر الأركان المنصوص عليها في قانون العقوبات والمتمثلة في الركن المادي، المعنوي والشرعي، فإذا توافرت هذه الأركان نكون أمام جريمة تامة يعاقب عليها القانون.حيث تمر فيها الدعوى بمراحل معينه ابتداء من مرحلة الاستدلال أو مرحلة البحث والتحري مرورا بمرحلة التحقيق وأخيرا مرحلة المحاكمة، التي فيها يصدر الحكم النهائي إما بإدانة المتهم أو براءته. لكن في ظل التطور العلمي والتكنولوجية الذي شهده العالم ظهرت جرائم جديدة بحيث أصبحت الأساليب القديمة لا ترقى لمجابهتها، إذ حاولت التشريعات مكافحة هذا النوع من الجرائم من الناحية الموضوعية وذلك بسّن تشريعات جديدة أو تعديل التشريعات تماشيا مع المبدأ السائد في قانون العقوبات وهو مبدأ الشرعية الذي ينص على أنه: " لا جريمة ولا عقوبة إلاّ بنص", [1]ولكن الإشكال كان يكمن في قصور الجانب الإجرائي في مكافحة هذا النوع من الجرائم وذلك للأسباب التالية[2]:

1- وجود الجريمة المعلوماتية في بيئة لا تعتمد التعاملات فيها على الوثائق والمستندات المكتوبة بل تعتمد على نبضات الكترونية غير مرئية لا يمكن قراءتها إلا بواسطة الحاسبات الآلية؛

[1] انظر المادة الأولى

[2] نورة طرشي، مكافحة الجريمة المعلوماتية, مذكرة لنيل شهادة الماجستير في القانون الجنائي، جامعة الجزائر 1، كلية الحقوق، 2012/2011، ص 96.

2- البيانات التي يمكن استخدامها كأدلة ضد الفاعل، يمكن في وقت قصير جدا العبث بها أو محوها بالكامل وبالتالي لا اثر للجريمة بعد ارتكابها؛

3-أثار الجرائم المعلوماتية تعتمد على الخداع في ارتكابها، والتضليل في التعرف على مرتكبيها، فالمعتدون والجانحون في المجال المعلوماتي لهم القدرات الفائقة على إخفاء هويتهم عند ارتكابهم لجرائمهم كونهم في غالب الأحيان ذوي دراية ومعرفة عالية بتقنيات المعلوماتية المتطورة؛

4-سرعة التطور العلمي في المجال المعلوماتي، قد يؤدي إلى تغيير أنواع الجريمة المعلوماتية وظهور جرائم جديدة مرتبطة بهذا التطور وبالتالي صعوبة تحديد الإجراءات لضبط هذه الجرائم سلفا.

لهذه الأسباب سارعت الدول المتطورة في المجال المعلوماتي إلى تعديل تشريعاتها الإجرائية وهذا بغية تسهيل إجراءات الدعوى العمومية بالنسبة للجهات القضائية القائمة على التحري والضبط والتحقيق والمحاكمة، وقبل التطرق إلى هذه الإجراءات ينبغي أولا معرفة مفهوم قانون الإجراءات الجزائية. حيث عرف بأنه: "مجموعة قواعد قانونية تحدد سبل المطالبة بتطبيق القانون على من خرق أحكامه بمخالفة أوامره ونواهيه عن طريق الإجراءات الأولية التي يقوم بها جهاز الضبطية القضائية وعن طريق الدعوى العمومية التي تحركها وتباشرها النيابة العامة, وهناك من يعرفه بأنه مجموعة القواعد القانونية التي تحدد طرق القواعد التي تحدد طرق الجهات القضائية التي لها الحق في متابعة الجاني من يوم اقتراف الجريمة إلى غاية صدور حكم نهائي وبات في الدعوى العمومية" .

وهناك من يعرفه بأنه: "مجموعة القواعد القانونية التي تحدد طرق الجهات القضائية التي لها الحق في متابعة الجاني من يوم اقتراف الجريمة إلى غاية صدور حكم نهائي وبات في الدعوى العمومية"[1].

فمدلول هذه التعاريف هو أن الدعوى العمومية هي نسبة السلوك الإجرامي إلى شخص معين وقبل نسبتها إليه لابد من التأكد من توافر عناصر المسؤولية الجنائية حتى

[1] دليلة مباركي، محاضرات في قانون الإجراءات الجزائية، موجهة لطلبة سنة ثانية ليسانس حقوق، كلية الحقوق –باتنة–، سنة 2021 /2022، ص3 .

يمكن تقديمه للقضاء ليحكم عليه بالعقوبة المقررة في قانون العقوبات، فالأفعال المذكورة من نسبة السلوك الإجرامي إلى شخص وتجميع القرائن والأدلة ضده وإسناد التهمة له ولكافة الأفعال المرتكبة مخالفة للقانون, يجب على المشرع في مجال الإجرام المعلوماتي النص على قواعد وأسس العقاب عليها وتنظيم الإجراءات الجنائية المتبعة وقت الاستدلالات والتحقيق الجنائي والمحاكمة ذلك لأن الجريمة المعلوماتية تختلف عن الجريمة التقليدية، رغم أن طرق تحريك الدعوى فيها هي نفسها المتبعة في الجرائم التقليدية إلا أن خصوصيات أو ميزات الجريمة المعلوماتية المستحدثة تفرض وجود إجراءات جديدة تتبع لكشف عنها بالإضافة للإجراءات التقليدية المطبقة بأشكال مستحدثة تبعا لنوع الإجرام.

المطلب الثاني: الإجراءات المنصوص عليها في الاتفاقيات الدولية

شهدت الجرائم المعلوماتية تطورا ملحوظا منذ نشأتها فقد تعددت صور الجرائم المعلوماتية وتنوعت فانقسمت إلى قسمين، جرائم واقعة ضد النظام المعلوماتي وجرائم ترتكب بواسطة النظام المعلوماتي. أدت إلى ظهور تحديات جديدة للمنظومة القانونية على المستوى الدولي، لذلك بدا التعاون الدولي ضروريا للتعامل مع هذا الإجرام في مجال المكافحة الإجرائية الذي قد يمس في آنٍ واحدة عدة دول، وفي هذا الإطار سنتناول ثلاث إجراءات متخذة في كل من اتفاقية بودابست، اتفاقية المجلس الأوربي سنة 2004 والإجراءات المنصوص عليها في ريو دي جانيرو.

الفرع الأول: الإجراءات المنصوص عليها في اتفاقية بودابست

حرص مجلس أوربا على التصدي للاستخدام غير المشروع للحاسبات وشبكات المعلومات وتتجلى ذلك في اتفاقية بودابست الموقعة في 23 نوفمبر 2001 المتعلقة بالجرائم المعلوماتية، كما سميت باتفاقية الجريمة عبر العالم الافتراضي، حتى تكون المرجع القانوني المساعد للدول في مواجهة الجريمة المعلوماتية، وقعت عليها 43 دولة أوروبية الأعضاء في المجلس الأوربي وغيرها من الدول الأخرى، إذ تأخذ في الاعتبار أن هدف مجلس أوربا هو

تحقيق وحدة أكبر بين أعضائه[1]، وإيمانا منها بأن المكافحة الفعالة للجريمة الإلكترونية تستلزم تعزيز التعاون الدولي في المسائل الجنائية وتسريع وتيرته والتوظيف بشكل جيد[2].

كما ترمي هذه الاتفاقية بشكل أساسي إلى مواءمة عناصر القانون الموضوعي الجنائي المحلي والأحكام المتصلة بالجرائم ثم مجال الجريمة الإلكترونية، والتنصيص على صلاحيات القانون الإجرائي الجنائي الداخلي اللازم للتحقيق في هذه الجرائم ومتابعتها قضائيا. علاوة الجرائم الأخرى التي ترتكب عن طريق نظام الكمبيوتر أو التي تكون الأدلة المتصلة بها في شكل الكتروني والى إنشاء نظام سريع وفعال للتعاون الدولي.

بناءا على ذلك تتضمن الاتفاقية أربعة فصول الأول استخدام المصطلحات، الثاني التدابير الواجب اتخاذها على الصعيد الوطني(قسم قانون جنائي، موضوعي)، الباب الثالث التعاون الدولي والباب الرابع الأحكام الختامية .

يتطرق القسم الأول من الباب الثاني (مسائل القانون الموضوعي) إلى أحكام التجريم والأحكام الأخرى ذات الصلة في مجال الجريمة الالكترونية أو الجريمة المتصلة بالكمبيوتر. يحدد أولا 9 جرائم مصنفة في 4فئات مختلفة، ثم يتناول المسؤولية الفرعية والعقوبات.

وتعرف الاتفاقية الجرائم التالية: النفاذ، الولوج غير القانوني ، الاعتراض غير القانوني وتداخل البيانات، تداخل النظام ، إساءة استخدام الأجهزة والتزوير المتصل بالكمبيوتر والاحتيال المتصل بالكومبيوتر ،الجرائم المتصلة بحق التأليف والنشر والحقوق المجاورة، أما بالنسبة للقسم الثاني من الباب الثاني (المسائل المتعلقة بالقانون الإجرائي) الذي يتجاوز نطاقه الجرائم المحددة في القسم الأول، من حيث أنه ينطبق على أي جريمة ترتكب بواسطة نظام الكومبيوتر أو تكون الأدلة بها في شكل الكتروني أولا.

---

[1] "الاتفاقية المتعلقة بالجريمة الالكترونية بوداباست"،الصادرة عن مجلس اوربا–مجموعة المعاهدات الاوروبية –،رقم 185،بتاريخ 23 نوفمبر 2001،ص2.

[2] الاتفاقية المتعقلة بالجريمة الالكترونية ، المرجع نفسه2.

الشروط والضمانات المشتركة التي تنطبق على جميع الصلاحيات الإجرائية في هذا الفصل ثم يحدد الصلاحيات الإجرائية التالية: التعجيل بحفظ البيانات المخزنة، التعجيل في حفظ بيانات الحركة والإفصاح الجزائي عنها، أمر تقديم بيانات الحركة في الوقت الحقيقي، اعتراض بيانات المحتوى وينتهي بأحكام الولاية القضائية .

كما يتضمن الباب الثالث الأحكام المتعلقة بالمساعدة المتبادلة التقليدية والمتصلة بالجريمة الالكترونية. فضلا عن قواعد تسليم المجرمين ويتناول هذا الفصل المساعدة المتبادلة التقليدية في حالتين:

أولا: غياب الأساس القانوني (معاهدة تشريع متبادل وما إلى ذلك) بين الأطراف وفي هذه الحالة تطبق أحكامه .

ثانيا: وجود الأساس القانوني وفي هذه الحالة تنطبق الترتيبات القائمة أيضا على المساعدة بموجب هذه الاتفاقية، وتنطبق المساعدة الخاصة بالجريمة الالكترونية أو الجريمة المتصلة على كلا الحالتين وتغطي مع مراعاة الشروط الإضافية. نفس نطاق الصلاحيات الإجرائية المحددة في الفصل الثاني، إضافة إلى ذلك يتضمن الفصل الثالث حكما بشأن نوع محدد من النفاذ العابر للحدود إلى بيانات مخزنة على الحواسيب، والذي لا يتطلب المساعدة المتبادلة عبر الموافقة، أو عندما تكون متاحة للجمهور وبنص على إنشاء شبكة على مدار 24 ساعة طوال أيام الأسبوع بغية ضمان المساعدة السريعة بين الأطراف .

وفي الأخير يتضمن الباب الرابع الأحكام الختامية التي تكرر الأحكام الموحدة في معاهدات مجلس اروبا مع الاستثناءات.[1]

ولاتفاقية بودابست دور الكبير في مكافحة الجريمة المعلوماتية، حيث لم تكتف بإرساء قواعد المكافحة الموضوعية فقط، بل تعرض في موادها لمعالجة المشكلات الإجرائية

[1] التقرير التفسيري لاتفاقية الجريمة الالكترونية، مجلس اوربا، سلسلة المعاهدات.
الأوروبية،رقم183،بودابست،في23نوفمبر/تشرين الثاني 2001 ،4،5.

التي تعترض سبل المكافحة بعد ما أدركت الدول المنظمة أو الموقعة أن مواجهة الجريمة وملاحظة مرتكبيها وضبطهم لتوقيع الجزاءات عليهم لا يمكن أن يتم بصورة فردية خاصة، وأن أهم ميزة للجرائم المعلوماتية هي أن الجرائم عابرة للحدود لاتقف أمام اقترافها أي عائق جغرافي. لذلك أرست اتفاقية بودابست بعض المبادئ الإجرائية التي يجب إتباعها وهي المبادئ الإجرائية وتتمثل في :

1- تنسيق عناصر الجرائم التي لها علاقة بالقانون الجنائي الأساسي الوطني والنصوص ذات الصلة بموضوع جرائم الحاسب الآلي، ثم توفير للقانون الجنائي الإجرائي الوطني السلطات الضرورية في التحقيق، وملاحظة الجرائم المعلوماتية وجرائم أخرى ترتكب بواسطة وسيلة المعلومات أو في إطار يوجد به أدلة الكترونية؛

2- وضع نظام سريع وفعال للتعاون الدولي، حيث تناولت هذه الاتفاقية في قسمها الثاني وصف بعض الإجراءات التي يجب اتخاذها على الصعيد المحلي والتي تخدم التحريات الجنائية، التي تجرى حول الجرائم التي ترتكب عن طريق المنظومة المعلوماتية وجمع الأدلة ذات الطابع الالكتروني والمرتبطة بالجريمة؛

وقد بينت هذه الاتفاقية أن أصعب المشاكل في مجال مكافحة الجرائم في عالم الشبكات هو صعوبة تحديد هوية المرتكب ومداها وتأثيرها ، بالإضافة إلى سرعة تلاشي البيانات الالكترونية التي يمكن تعديلها ونقلها ومحوها في ثوان معدودة ، وللتصدي لهذه الصعوبات أقرت الاتفاقية (بودباست) الإجراءات التقليدية لمكافحة الجرائم المعلوماتية في المناخ التكنولوجي الحديث، كإجراء التفتيش والمصادرة، وبالمقابل وضعت إجراءات جديدة لمكافحة الجريمة المعلوماتية وهذه الإجراءات تقوم على مبادئ أساسية عامة، هي التزام دول الأطراف في الاتفاقية بإقرار الإجراءات التشريعية وإجراءات أخرى إذا استلزم الأمر يتناسب مع القانون المنصوص عليها لخدمة التحريات والإجراءات الخاصة؛

3- وجوب إقرار الدول الموقعة عليها، بأن قانونها الداخلي يتضمن معلومات رقمية الكترونية تستخدم كأدلة أمام القضاء وذلك في إطار الإجراء الجنائي وأيا كانت طبيعة الجريمة الجنائية المطلوب متابعتها؛

4- على الدول الأعضاء أن تقوم بتفعيل بعض الإجراءات النابعة من قانونها الداخلي، أما كيفية تطبيق سريان هذه الصلاحيات والإجراءات في إطار نظامها القضائي وتطبيق الصلاحيات والإجراءات في بعض الحالات الخاصة. يجب أن يتبع من التشريعات والإجراءات الداخلية لكل طرف وهذه الإجراءات الداخلية يجب أن تتضمن شروطا ووسائل الحماية التي قد تكون دستورية بالنص عليها في دساتير هذه الدولة، كالمادة 48 من الدستور الجزائري لسنة 2020[1]، أو التشريعية أو تحددها السلطات القضائية المختصة كأعضاء الضبطية القضائية وأعضاء النيابة العامة ورجال القضاء والموظفون المعهود إليهم بمقتضى القوانين الإجرائية الداخلية لكل بلد. كما يجب أن تتوازن مع شروط تطبيق القانون وحماية حقوق الإنسان الأساسية وحرياته كحق الإنسان في حرمة حياته الخاصة[2].

كما نصت الاتفاقية على بعض الإجراءات الجنائية الجديدة لمكافحة الجريمة المعلوماتية وهي الحفظ السريع للمعطيات المخزنة، تجميع المعلومات الخاصة بالمشتركين والتفتيش المعلوماتي:[3]

أ- الحفظ السريع للمعطيات المخزنة: نصت على هذا الإجراء كل من المادتين 16و 17 من الاتفاقية، يقصد به الاحتفاظ بالمعلومات السابقة وتخزينها مع حمايتها من كل ما يمكن أن يفسدها أو يتلف توعيتها؛

---

[1] انظر المادة 48من دستور الجزائري لسنة 2020التي تنص على أنه :"تضمن الدولة عدم انتهاك حرمة المسكن فلا تفتيش الا بأمر مكتوب صادر عن السلطة القضائية".

[2] علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دار الجامعة الجديدة،2008،ص77ومابعدها، نقلا عن .. نورة طرشي، المرجع السابق، ص 101.

[3] نورة طرشي، المرجع السابق، ص 102-104.

ب- تجميع المعلومات الخاصة بالمشتركين: نصت الاتفاقية بوداباست كذالك في اطار التحقيق الجنائي على أهمية المعلومات الخاصة بالمشتركين لتحديد هوية الفاعل في الجريمة المعلوماتية وهذه المعلومات تشمل تلك المرتبطة بالاستعانة بالخدمة والمدة التي يشترك في الشخص في الخدمة كأن تتضمن مثلا حفظ رقم الهاتف او العنوان الالكتروني أو عنوان الموقع ..... الخ؛

ت- التفتيش المعلوماتي: كما نصت الاتفاقية على اجراء التفتيش، أي تفتيش البيانات في المادة 19 منها وقد بينت أنه يجب توفر شرط للحصول على اذن رسمي للتفتيش. بعد الاعتقاد بتوفير البيانات في مكان محدد يساعد على اثبات وقوع جريمة معلوماتية محددة بمقتضى القوانين الداخلية وتفتيش البيانات المعلوماتية والمعطيات يتم تجميعها في الوقت المتاح للتفتيش مع وجوب توفر شرط الحصول على اذن رسمي للتفتيش؛

كما نصت المادة 31 فيما يتعلق بالبحث عن البيانات المعلوماتية على وجوب أحكام اجرائية اضافة لضمان الحصول على البيانات المراد استعمالها كدليل ويجب أن تكون لها نفس فاعلية التفتيش ومصادرة الدعائم المادية للمعلوماتية.

كما تلزم المادة الدول الأطراف تحويل سلطاتها المختصة بمكافحة الجريمة الحق في فحص والدخول على المعطيات المعلوماتية الموجودة في نظم المعلومات أو أي جزء منها والاعتراض في الوقت الفعلي لها من أجل امكان جمع الأدلة الالكترونية؛

ث- اجراء التنصت: وهو اجراء جديد في اطار المكافحة الاجرائية للجريمة المعلوماتية كما أنه اجراء خاص قد يمس بحقوق الأفراد الخاصة، لذلك لا يجوز اعتباره اجراء قانوني الا اذا اتخذ بموافقة السلطات القضائية، ومفاد هذا الاجراء هو اعتراض المرسالات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية كالخطوط الهاتفية ووضع الترتيبات التقنية بدون موافقة المعنين من اجل التقاط وتثبيت وبث تسجيل الكلام المتفوه به من طرف

شخص أو أشخاص يتواجدون في امكنة خاصة وذلك من أجل التحري والوصول الى ادلة تثبت قيام الجريمة؛

ج- التعاون الدولي : ولتفعيل الاجراءات السابقة نصت الاتفاقية في المادة 23 على ضرورة تعاون الدول فيما بينها في أوسع نطاق ممكن مع تقليل الصعوبات التي قد تواجه تبادل المعلومات والادلة حتى تتم بصورة سريعة على المستوى الدولي

كما وضحت المفهوم العام لالتزام التعاون الدولي في مجال الجرائم الالكترونية المتعلقة بنظم المعلوماتية، كما تناولت الاحكام الخاصة بتسليم المجرمين وشروط التسليم الذي يطبق في حالة الجرائم المنصوص عليها في المواد 2الى 11 منها والتي يعاقب عليها قانون الدولتين المعنيين بالتسليم بالسجن لمدة قصوى لا تقل عن سنة أو بعقوبة أكثر صرامة في المادة 24 منها.

كما خلصت هذه الاتفاقية بعد دخولها حيز التصديق الى انها اتفاقية ذات طابع توجيهي ملزم في مادتها الثانية. وناقشت مشكلة تحديد المصطلحات القانونية التي تستعمل في مجال المكافحة المستعملة الاجرائية للجريمة المعلوماتية هل نبقي على مصطلحات التقليدية المستعملة في الجرائم التقليدية أم نستخدم مصطلحات معلوماتية جديدة أقرب الى مجال التكنولوجيا مع مناقشة مسألة التطور .[1]

الفرع الثاني: الإجراءات المنصوص عليها في اتفاقية المجلس الاوربي لسنة 2004

تعد اتفاقية الجرائم المعلوماتية للمجلس الاوربي من أحدث الاتفاقيات لمكافحة الجريمة المعلوماتية على المستوى الدولي، وقد صدرت عن المجلس الاوربي بعد أن وقعت عليها 32 دولة ودخلت حيز التطبيق في أول جولية 2004 .

[1] www.conventions,coe,int23 novembre 2001

نصت هذه الاتفاقية على مجموعة من الجرائم التي تمس النظام المعلوماتي وبينت الاساليب التحقيقية فيها وهذه الجرائم هي الجرائم المرتكبة ضد سرية وتكامل وتوافر البيانات أو نظم الحاسبات كجرام التدخل والاختراق على أجهزة الحاسبات الآلية، ثم الجرائم التي تتضمن انتهاكا لحقوق الملكية الفكرية وما يتصل منها من حقوق ومن الاساليب لدينا [1]:

أ- إرساء كل من إجراء تفتيش وضبط أنظمة الحاسبات الآلية؛

ب- 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؛

ت- إجراء الأمر بإصدار نسخة من البيانات وهذا الإجراء يمكن السلطات المختصة من إجبار الشخص على تقديم بيانات الحاسب المخزونة أو المحددة أو أحد عناوين ISP Internet service provider المعنية والتي تساهم في التوصل إلى المعلومات حول المشترك، وقد أعطت الاتفاقية (اتفاقية المجلس الأوروبي) اهتماما خاصا لإجراء تفتيش 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 الالي ؛

ث- كما نصت هذه الاتفاقية على إجراء اعتراض بيانات المحتوى والتي تعني اعتراض محتوى الاتصال سواء كان رسالة أو معلومة منقولة ولزيادة فاعليتها على المستوى الدولي، تبين هذه الاتفاقية الخطوات المتبعة لمكافحة الجريمة المعلوماتية في كل من اجتماع (ابيك في بنكوك سنة 2002 لمكافحة الجريمة المعلوماتية) وتوصيات اجتماع

[1] طارق ابراهيم الدسوقي عطية, الأمن المعلوماتي النظام القانوني للحماية المعلوماتية ,دار الجامعة الجديدة, ط 1 ,2009 ,ص 498.

منظمة الدول الأمريكية بنيويورك سنة 2004، ومؤتمر الجريمة المعلوماتية في ستراسبورغ في ماي 2005، ودائما في إطار المكافحة الإجرائية في اتفاقية المجلس الأوروبي يجب التنويه إلى دور هذه الاتفاقية في إنشائها لوحدة Eupojut التي مهمتها التعاون بين دول الاتحاد الأوربي في مجال مكافحة الجريمة المعلوماتية، تعاون السلطات القضائية للدول الأعضاء في هذا الاتحاد بمكافحة الجريمة المعلوماتية وذلك بإصدار إجراء جديد جماعي هو أمر القبض الأوروبي الذي يسمح بتسليم بالمجرم المعلوماتي بسرعة في أي دولة من دول الاتحاد الأوروبي.[1]

الفرع الثالث: الإجراءات الجديدة في مؤتمر ريو ديجانيرو1994

انعقد مؤتمر الدولي 15 للجمعية الدولية لقانون العقوبات في 4سبتمبر 1994 بريو دي جانيرو بالبرازيل لدراسة المبادئ العامة المتعلقة بالقانون الإجرائي الخاص بالجريمة المعلوماتية

وقد أرسى هذا المؤتمر مجموعة من المبادئ يجب العمل بها حتى نستطيع إقامة نظام إجرائي خاص بهذه الجرائم وهذه المبادئ تتلخص في:

- وضع تحت تصرف سلطات التحقيق والتحري مكان قسرية أو جبرية كافية تتعادل مع الحماية الكافية لحقوق الإنسان وحرمة الحياة الخاصة ب الافراد
- تجنب تعسف السلطات الرسمية بوضع القيود وتقرير أوجه الحماية لحقوق الإنسان
- تقرير أن الانتهاكات غير المشروعة التي يمارسها رجال السلطة العامة يمكن أن تبطل الدليل المتحصل عليه من تقرير مسؤولية جنائية لرجال السلطة العامة اللذين ينتهكون القانون

وقد خرج المؤتمر بتوصيات لنجاح وفعالية المكافحة الإجرائية للجريمة المعلوماتية بوجوب العمل بالإجراءات التالية:

[1] http://eur-lex.europ a .eu/lexuri sw/lex uni serv.do luri=cele x3 2002 fo 584 :fr.ht ml.

- تحديد واجبات التعاون الفعال من جانب المجني عليهم والشهود وغيرهم من مستخدمي تكنولوجيا المعلومات
- السماح للسلطات العامة باعتراض الاتصالات داخل نظام الحاسب الالي ذاته أو بينه ونظم الحاسبات الأخرى مع استخدام الأدلة التي يتم الحصول عليها في الإجراءات أمام المحاكم
- تنفيذ المكنات القسرية والجبرية المنوطة برجال السلطات يجب أن يكون مناسبا مع الطابع الخطير الانتهاك كما يجب ،بسبب الحد الأدنى من إعاقة الأنشطة القانونية للفرد عند بدء التحريات يجب الأخذ بعين الاعتبار القيم المالية التقليدية وكل القيم المرتبطة ببيئة تكنولوجيا المعلومات كضياع فرصة اقتصادية أو انتهاك حرمة الحياة الخاصة أو كلفه إعادة بناء تكامل البيانات كما كانت من قبل.

ضرورة إدخال بعض التغييرات التشريعية في حالة الضرورة, كما في حالات قبول ومصداقية الأدلة التي قد تثير مشاكل تطبيقها في مجال الجرائم المعلوماتية، هذا وقد أوصى مؤتمر ريو داجانيرو الدولي الخامس عشر في مجال حركة اصلاح الإجراءات الجنائية وإرساء قواعد حماية حقوق الإنسان بمجموعة من التوصيات أهمها [1]:

- توصية ٠١: حماية حقوق الإنسان يجب أن تكون مكفولة في كل مراحل الدعوى الجنائية ؛
- توصية ٠٢: استفادة المتهم من قرينة البراءة في كل مراحل الإجراءات حتى صدور حكم يحوز قوة السير المقضي فيه ؛
- توصية ١٠: كل إجراء يتخذ بواسطة سلطة رسمية كالإجراءات المتخذة من طرف مأمور الضبط القضائي ويمس الحقوق الأساسية للمتهم يجب أن يكون مسموحا به عن طريق السلطة القضائية المختصة كالقاضي مثلا وخاصه لرقابتها ؛

[1] علي حسن محمد الطوالبة, المرجع السابق,ص215.

- توصية١٢: وسائل الإثبات التي تمس بطريقة خطيرة وخاصة الحق في الخصوصية والسرية كإجراء التنصت على المحادثات التليفونية ، ولاتكون مقبولة الا بقرار سابق من القاضي وفي الحالات المقررة قانونا ؛
- التوصية١٨: كل الأدلة التي يتم الحصول عليها عن طريق انتهاك حق أساسي للمتهم والأدلة المستمدة منها تكون باطلة ولا يمكن مراعاتها في أي لحظة؛
- التوصية٢٠: لا يجبر أحد على المساعدة بطريقة مباشرة أو غير مباشرة على اتهام نفسه جنائيا كما أنه للمتهم الحق في الصمت وثمنه لا يستخدم كدليل ضده.

المبحث الثاني: نطاق المكافحة الاجرائية للجريمة المعلوماتية

سنتطرق في هذا المبحث الى نطاق المكافحة الإجرائية للجريمة المعلوماتية بدراسة كل من الاجراءات التالية المعاينة, التفتيش والقواعد العامة لتفتيش النظام المعلوماتي كما سنرى مكافحة الجريمة المعلوماتية في القانون الجزائري

المطلب الاول: معاينة مسرح الجرائم المعلوماتية وتفتيشها

لم تكتف التشريعات الحديثة بحماية معطيات الحاسب الالي بصفة عامة من خلال تجريم صور الاعتداء عليها أي حماية موضوعية, وانما نظرا لخطورة الاجرام الالكتروني في حد ذاته لكون محل الجريمة مجموعة معطيات هي عبارة عن الحقيقة عن ذبذبات الكترونية يسهل على الجاني القيام بعمل اجرامي عليها دون ترك اثار ودون أن يستغرق هذا العمل وقتا طويلا, وهو ما جعلها صعبة الاكتشاف والاثبات ادى الى ذلك الى ظهور مشكلات اجرائية في هذا النطاق حيث أن المحقق أو ضابط الشرطة القضائية أو القاضي نفسه في حيرة أمام هذه الجرائم نظرا لقصور التشريع الاجرائي خاصة وأن هذه الجرائم حديثة ولا يمكن تطبيق النصوص التقليدية من جهة وعدم القدرة الكافية والفنية لرجال القانون لاكتسابها.

لذلك وضعت مجموعة من الاجراءات منها ما يعتبر قاسما مشتركا بين الجرائم التقليدية والجرائم الحاسة بالمعطيات ومنها لا يطبق إلا على الجريمة المعلوماتية, يمكن تقسيمها اجراءات شخصية ومادية وهذه الأخيرة تتمثل في التقنية و التفتيش سنتعرض في ما يلي:

الفرع الأول: معاينة مسرح الجرائم المعلوماتية

ان الدعوى العمومية باعتبارها الوسيلة القانونية لاستفتاء حق الدولة في العقاب

نبدأ اجرائها بمرحلة البحث والتحري أي مرحلة الاستدلالات, التي تهدف الى البحث عن الجريمة والكشف عن مرتكبيها, وان الاجراءات الجزائية المتخذة خلال هذه المرحلة تتولاها أجهزة الشرطة القضائية (الضباط) وتتمثل الاجراءات كما ذكرنا سابقا في المعاينة و التفتيش

يقصد بالمعاينة التقنية هي المكان أو المسرح الذي ارتكبت فيه الجريمة, أو الوعاء الاساسي الذي يحتوي على أخطر الادلة الجنائية التي يخلفها الجاني وراءه في أعقاب اقترافه الجريمة وفي لحظة يكون فيها اضطرابه العصبي والذهني قد بلغ قمة الانفعال بصورة لا تبيح لمراجعة الدقيقة لأعماله وازالة الاثار التي يخلفها في مكان الحادث (المجرم) مهما كانت دقته سوف يترك وراءه ما قد يشير الى شخصيته[1], ولذلك كان من الواجب على ضباط الشرطة القضائية الانتقال الى ذلك المكان لمعاينة واثبات الاثار المادية للجريمة والمحافظة عليها واثبات حالة الاماكن والاشخاص, وكل ما يفيد في كشف الحقيقة, وكذا اخطار النيابة فورا بانتقاله لكي تنتقل بدورها الى محل الجريمة في حالة الجناية المتلبس بها[2]. ويقصد بالمعاينة رؤية بالعين لمكان أو شخص أو شيء لإثبات حالته وضبط كل ما يلزم لكشف

[1] ابتسام بغو, اجراءات المتابعة الجزائية في الجريمة المعلوماتية, مذكرة تكميلية لنيل شهادة ماستر في القانون, قانون جنائي, جامعة العربي بن مهيدي أم بواقي,2015,2016,ص 7/6 .

[2] انظر المادة 31 قانون اجراءات جزائية المصري ....الانتقال فورا الى مكان الجريمة ....

الحقيقة, وهي تقتضي في ذلك سرعة الانتقال الى محل تلك الواقعة حيث يقوم ضابط الشرطة القضائية بجمع الدلائل والقرائن التي يستدل بها عن الجريمة والتثبيت المباشر لحالة الاشخاص والاشياء والاماكن ذات الصلة بالحادث وهي المرحلة الأولى للاستدلال حول ملابسات اية جريمة, ونظرا لاختلاف الجريمة المعلوماتية كثيرا عن الجرائم التقليدية نظرا لكون مسرحها الاجرامي قد يتعدى حدود الدولة فان المعاينة التقنية تتم باتباع مجموعة من الاجراءات الخاصة.

وتظهر أهمية المعاينة في انها تنقل لجهات التحقيق والمحاكمة صورة مجملة لموقع الجريمة بكل ما يحتويه هذا الموقع من تفصيلات سواء تعلقت التفصيلات بمكانه أو وصفه من الداخل والاثار الموجودة به, والتي تنقلها بالجريمة وجمالا كل ما يمكن جهات الشرطة والقضاء من وضع تصور لكيفية وقوع الجريمة واستخلاص بعض الادلة من المادة التي تم جمعها[1], وقد نصت المادة 42 من قانون الاجراءات الجزائية الجزائري على المعاينة بشكل عام كإجراء يتم في مرحلة الاستدلالات, وهو مخول لجهاز الضبطية القضائية سواء في الحالة العادية أو حالات التلبس[2], ويترتب على تغيير أو تعديل يطرأ على مكان وقوع الجريمة الجزاءات المنصوص عليها في المادة 43 قانون اجراءات الجزائية الجزائري, وحتى يكون التفتيش في بيئة الكترونية لابد أن يتم على مستويين تتمثل في مسرح الجريمة التقليدي, وأيضا تفتيش المكونات المعنوية للحاسوب والتي تمثل مسرح الجريمة الافتراضي[3].

[1] نبيلة هبة هروال, الجوانب الاجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات, دار الفكر الجامعي, الاسكندرية ,2013,ص216.

[2] عبد الله ماجد العكايلة, الوجيز في الضبطية القضائية, ط 1,دار الثقافة للنشر والتوزيع, عمان ,2010,ص65 .

[3] عبد الفتاح بيومي حجازي, مبادئ الاجراءات الجنائية في جرائم الكمبيوتر الانترنت,ط1,دار الفكر الجامعي ,الاسكندرية ,2006,ص160 .

فاذا كانت المعاينة في الجرائم التقليدية تتم في مسرح الجريمة العادي فان الجريمة المعلوماتية تتم المعاينة فيها على مستويين المسرح التقليدي الجرائم الواقعة على المكونات المادية وهو المسرح الذي يقع عادة خارج بيئة الحاسوب ويتكون من المكونات المادية للمكان الذي وقعت فيه الجريمة وهو قريب من مسرح الجريمة التقليدية, ومن أمثلة هذه الجرائم تلك الواقعة على أشرطة الحاسب fd والكابلات الخاصة به وشاشة العرض الملحق به ومفاتيح التشغيل والاقراص, وغيرها من مكونات الحاسب الالي ذات الطابع المادي المحسوس[1], والمسرح الافتراضي الجرائم الواقعة على المكونات الغير المادية أو بواسطتها يقع عادة داخل البيئة الالكترونية, ويتكون من البيانات الرقمية التي تتواجد داخل الحاسوب في ذاكرة الاقراص الصلبة الموجودة بداخله, وفي مقدمة هذه الجرائم الواقعة على برامج الحاسب الالي او بياناته او تتم بواسطتها, وكذالك الجرائم التي تتم بطريقة الانترنت والحاسوب المعلوماتية اشكال مختلفة تختلف بحسب نوعية الجريمة المرتكبة على أن هناك طرقا عامة تتوافق مع طبيعة الاتصال بالانترنت او الوسيلة التي تستخدم مثلا وسيلة تصوير شاشة الحاسوب والتي تكون بواسطة الة تصوير تقليدية او عن طريق استخدام برمجة حاسوب متخصصة في اخذ صورة لما يظهر على الشاشة وهذا ما يصطلح عليه تجميد مخرجات الشاشة وغيرها.

الفرع الثاني: اجراءات تفتيش الانظمة المعلوماتية

يعتبر التفتيش اجراء من اجراءات البحث والتحقيق, ويهدف الى البحث عن ادلة مادية لجناية أو جنحة تحق وقوعها بمكان يتمتع بالحرمة أو تفتيش شخص, وان اجراء التفتيش أهمية بالغة وخطورة معتبرة على الحياة الخاصة ولهذا نص عليه المشرع الجزائري بمقتضى قواعد

[1] المادة 03 قانون اجراءات جزائية جزائري.

دستورية [1]حيث تضمن الدولة عدم انتهاك حرمة منزل مسكن, فلا تفتيش إلا بمقتضى القانون وفي اطار احترامه فلا تفتيش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة هذا بالإضافة الى نصوص قانون الاجراءات الجزائية وايضا القانون 04 09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاتصال ومكافحتها.

ويعرف التفتيش لغة التفتيش لغة من فعل فتش اي يبحث عن شيء, واصطلاحا هو البحث عن الشيء في مكان سره ويعتبر اجراء من اجراءات التحقيق وليس من اجراءات الاستدلال بأجماع من معظم التشريعات كالتشريع الجزائري مادة 44 من قانون الاجراءات الجزائية الجزائري والفرنسي و المصري المادة 94 من قانون اجراءات جزائية وهو اجراء يقوم به مأمور الضبط القضائي ويؤديه بالشكل القانوني المحدد له.

ان الهدف من التفتيش هو ضبط الادلة المادية الكشف عن الجريمة فكل ما يضبطه مأمور الضبط القضائي بعد عملية التفتيش من أشياء متعلقة بالجريمة هو الاثر المباشر للتفتيش فالضبط اذن يعد ايضا اجراء من اجراءات التحقيق بوضع اليد على الشيء وحبسه والمحافظة عليه للحصول على دليل لمصلحة التحقيق عن طريق اثبات واقعة معينة[2].

يقصد بمحل التفتيش المستودع الذي يحتفظ فيه المرء بالأشياء المادية التي تتضمن سره والسر الذي يحميه القانون, هو ذلك الذي يستودع في محل له حرمة كالسكن أو الشخص أو السيارة أو الرسائل وبالتالي فقد يكون محل ذلك التفتيش أما مسكنا أو شخصا وسيارة مع مراعاة الاجراءات القانونية المقررة.

ومحل التفتيش في جرائم الحاسب الالي يعتبر النافذة التي تطل بها الانترنت على العالم والشبكة التي تشمل مكوناتها الخادم والمزود الالي وغيرها, فان اجراء التفتيش في الجريمة

[1] المادة 48 من الدستور 2020.
[2] نورة طرشي, المرجع السابق,ص117.

المعلوماتية يحتاج الى تقنيات خاصة تختلف عن الحالات التفتيش العادية التقليدية لان تفتيش نظم المعلومات ليست سهلة وتتطلب دراية ومعرفة بملفات أجهزة الاعلام الالي وأماكن اخفاء المعلومات فيها لانه يسهل اتلافها كليا او جزئيا كما يصعب تحديد مكان الدليل [1]

وبالتالي ففي اطار جرائم الانترنت يقع التفتيش حل موضوعين اثنين هما [2]:

أ- تفتيش مكونات الحاسب الالي(المادية والمعنوية)

ب- تفتيش الشبكات المعلوماتية المتصلة بالحاسوب (التفتيش عن بعد) وهو ما سنتناوله:

أ- تفتيش مكونات الحاسب الالي: يعرف الحاسب الالي بانه كل جهاز الكتروني يستطيع ترجمته اوامر مكتوبة بتسلسل منطقي لتنفيذ عمليات ادخال او اخراج معلومات[3], تخضع المكونات المادية لنظام المعالجة الالية للمعطيات لإجراءات التفتيش المنصوص عليها في المادة 44 ق,اج,ج [4], اي انه يجب مراعاة مكان وجود ذلك الحاسوب أثناء مباشرة ذلك الاجراء فيما اذا كان مكان عام أو خاص لأن صفة المكان أهمية خاصة في مجال التفتيش, ولا يجوز القيام بإجراء التفتيش إلا بأذن مكتوب صادر عن وكيل الجمهورية او قاضي التحقيق وبعد الحصول على رضا صريح من صاحب المسكن ويجب كتابته بخط يد صاحب الشأن وتوقيعه اما اذا تعذر على صاحب الشأن الحضور وقت اجراء التفتيش, ضابط الشرطة القضائية ملزم بأن يكلفه بتعيين ممثل له واذا امتنع عن ذلك وكان هاربا استدعى الضابط بحضور تلك العملية شاهدين من غير الموظفين الخاضعين لسلطته 7 كما يجب ان يتم ذلك الاجراء في المواعيد المحددة قانونا وهي من الساعة الخامسة

[1] نبيلة هروال, المرجع السابق,ص234.

[2] ابتسام يغو, المرجع السابق, ص 14.

[3] محمد حماد مرهج الهيتي, جرائم الحاسوب, ط1,دار المناهج للنشر والتوزيع,الاسكندرية,2012, ص22.

[4] تنص المادة 44 قانون اجراءات الجزائية الجزائري على (لا يجوز لضباط الشرطة القضائية اجراء تفتيش الا بموجب اذن مكتوب صادر عن وكيل جمهورية او قاضي تحقيق)يتضح من نص المادة أن التفتيش يقع على الاشياء والاوراق التي لها علاقة بالجريمة.

صباحا الى الساعة الثامنة مساءا إلا في الحالات الخاصة خاصة فيما يتعلق بالجرائم الخطيرة ومن بينها الجريمة المعلوماتية التي لا تشترط المواعيد وانما في كل وقت من اليل والنهار

أما فيما يتعلق بالتفتيش عن الجريمة التي وقعت على المكونات المعنوية للحاسوب ويقصد بها أنظمة الكومبيوتر والبيانات المخزنة فيه التي جري التلاعب فيا أو تغييرها وغيرها من الوسائط التي تساعد على تخزين المعلومات[1].

يرى البعض أن التفتيش يمتد الى سجلات البيانات الموجودة في موقع اخر , يشترط ن تكون البيانات الخاصة ضرورية بإظهار الحقيقة وهو ما تبناه القانون المقارن حول تفتيش الانظمة المعلوماتية, فقد منحت المادة 251 من قانون الاجراءات اليوناني سلطات التحقيق امكانية القيام بأي شيئ يكون ضروريا لجمع الدليل وكذلك المادة 487 من القانون الكندي والانجليزي والفرنسي وفي الولايات المتحدة الامريكية .

وبالتالي فان النصوص القانونية التي أرست القواعد التي تحكم التفتيش تم سنها قبل أن يعرف القانون الاشياء غير المادية, وبالتالي فالنصوص التقليدية لا يمكن اعمالها مباشرة على النظم المعلوماتية لأن قياسها على الاشياء المادية سيكون منافيا للشرعية الاجرائية.

تفتيش الشبكات المعلوماتية المتصلة بالحاسوب (التفتيش عن بعد): يقصد به تفتيش حاسوب المتهم عندما يكون متصلا بغيره من الحواسيب عبر شبكة اخرى في دولة اخرى

وطبقا للمادة 205 من القانون 04/09 [2]أجاز المشرع تمديد التفتيش الى هذه المنظومة بعد اعلام السلطة القضائية المختصة مسبقا بذلك متى دعت الضرورة الى الاعتقاد بأن

[1] خالد عياد الحلمي, اجراءات التحري والتحقيق في جرائم الكمبيوتر والانترنت,طبعة01,دار الثقافة للنشر والتوزيع,عمان,2011,ص159.

[2] انظر المادة 05 من القانون 04/09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحته المؤرخ في 50 اوت 2009 الجريدة الرسمية العدد47 المؤرخة في 16 اوت 2009 .

المعطيات المبحوث عنها مخزنة في منظومة معلوماتية اخرى أن هذه الاخيرة يمكن الدخول اليها من المنظومة الاولى في اطار اقليم الدولة.

اما اذا تبين أن المعطيات المبحوث عنها والتي يمكن الدخول اليها انطلاقا من المنظومة الاولى مخزنة في منظومة معلوماتية تقع خارج الاقليم الوطني فان التفتيش أو الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة .

المطلب الثالث: القواعد العامة للتفتيش النظام المعلوماتي

تحرص أغلبية القوانين على احاطة التفتيش بشروط وضمانات أساسية بوصفه اجراء يمس صميم الحرية الشخصية, الغرض منها تحقيق الموازنة الضرورية بين مصلحة المجتمع وبين حقوق المتهم لذلك حرصت مختلف القوانين والتشريعات على اخضاعه الى قواعد شكلية واخرى موضوعية سنتناولها بالدراسة في الفرعين التالين:

الفرع الاول: القواعد الشكلية

تتلخص هذه القواعد كما يلي :[1]

1- اجراء التفتيش بحضور أشخاص معينين بالقانون من بين هذه الاشخاص لدينا المتهم والقائم بالتفتيش وشاهدين, المادة 45 من قانون الاجراءات الجزائية الجزائري تنص على ان التفتيش يتم بحضور المتهم أو من يجوز أن يمثله يتم التفتيش بحضور المتهم أو من يجوز أن يمثله وضابط الشرطة القضائية القائم بالتفتيش واذا تعذر حضور المتهم أو من يجوز أن يمثله يتم التفتيش بحضور شاهدين من غير الموظفين الخاضعين لسلطته, غير أنه كاستثناء على هذه القواعد نص المشرع الجزائري في الفقرة الاخيرة من المادة 45

[1] نورة طرشي, المرجع السابق, ص128.

من قانون اجراءات الجزائية الجزائري على أنه لا تطبق هذه الاحكام اذا تعلق الامر بالجرائم الماسة بأنظمة المعالجة الالية للمعطيات

2- اعداد محضر خاص بالتفتيش ويكون بتكليف القائم بالتفتيش

3- أن يتم التفتيش بأسلوب الي أي أن يكون التفتيش على عامة الكترونية وهو بضرورة الحاسب الالي

4- أن يتم التفتيش من طرف فريق يتكون من خبراء

5- اذن التفتيش لابد أن يكون مسببا

-6 الميعاد الزمني لأجراء التفتيش, حيث اختلفت التشريعات الاجرائية في وقت تنفيذ التفتيش ومن بينهم المشرع الجزائري ذهب الى حظر التفتيش للمساكن وما في حكمها في اوقات معينة [1]وهناك حالات استثنائية

خرج فيها عن هذه القاعدة الأصل ان يكون التفتيش من الساعة الخامسة صباحا الى الساعة الثامنة مساءا والا كان التفتيش باطلا غير انه في بعض الجرائم خرج المشرع الجزائري عن القاعدة العامة لميعاد التفتيش واجاز التفتيش في جميع الاوقات 24 ساعة في بعض الجرائم مذكورة على سبيل الحصر ومن بينها جرائم المساس بأنظمة المعالجة الالية للمعطيات

بالإضافة الى تحديد هوية أعضاء فريق التفتيش يجب على القائم بالتفتيش اتخاذ الخطوات التالية عند تنفيذ اذن التفتيش والتي تتلخص في ما يلي:

- تأمين حماية مسرح الجريمة بتضمين القوة الكهربائية واجهزة خدمة شبكة الانترنت
- ابعاد المتهم عم مكان النظام ان كان قريبا منه
- أخذ الحيطة من تمكن المتهم الدخول عن بعد للنظام المعلوماتي

[1] المادة 47 قانون الاجراءات الجزائية الجزائري.

- الدخول الى الموقع ببطيء كي لا يتم تشويه او اتلاف الدليل
- عدم لمس لوحة المفاتيح لان ذلك قد يستلزم استخدام برامج أخرى احتيالية او صعبة
- يجب العناية بالملاحظات وكلمات السر ورموز الشفرة الى غيرها من العمليات والاجراءات الفنية التي تساعد على الكشف عن الجريمة المراد اثباتها [1]

الفرع الثاني: القواعد الموضوعية

تتلخص القواعد الموضوعية لتفتيش النظم المعلوماتية في قواعد التالية:

أ- وقوع الجريمة المعلوماتية مصنفة على انها جناية او جنحة مثلما هو الحال في القواعد الموضوعية التقليدية, يشترط الفقه الجنائي الاجرائي في القانون المقارن هذا الشرط رغم عدم الوصول الى تعريف موحد للجريمة المعلوماتية المستمر الحاصل والذي سيحصل مستقيلا مما يؤدي للاصطدام بمبدأ الشرعية, كما يجب ان تكون هذه الجريمة المعلوماتية قد وقعت بالفعل بحيث لا يجوز الامر بالتفتيش لضبط الادلة عن جريمة مستقبلية.

ب-اتهام شخص او أشخاص معينين بارتكاب الجريمة المعلوماتية او المشاركة فيها ويقتضي هذا الشرط أن تتوافر في حق الشخص المراد تفتيشه في شخصه او مسكنه دلائل كافية تدعو بانه قد ساهم في ارتكاب الجريمة المعلوماتية سواء بوصفه فاعلا أو شريكا فاذا انتفت هذه الدلائل سيصدر قاضي التحقيق امرا بالا وجه للمتابعة مثلما فعل القانون الامريكي في قانونه الجزائي عند انتفاء السبب المعقول للاعتقاد بان الشخص قد ارتكب الجريمة والقانون الفرنسي في المادة 177 من قانون الاجراءات الجزائية[2].

[1] عفيفي كامل عفيفي, جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون, منشورات الحلبي الحقوقية, طبعة ثانية, 2007, ص65 .

[2] عمر محمد بن يونس, الاجراءات الجنائية عبر الانترنت في القانون الامريكي, رسالة دكتوراه, كلية الحقوق, جامعة عين شمس ,2004.

ت–توافر امارات قوية او قرائن تفيد في كشف الحقيقة في مجال الاجرام المعلوماتي والمقصود بالأمارات القوية والقرائن تلك الادلة على وجود أشياء او اجهزة او معدات معلوماتية تفيد في كشف الحقيقة لدى المتهم المعلوماتي او غيره تفيد في اثبات حصول جريمة أم لا .

ث–تفتيش نظم المعلوماتية بناءا على موافقة المتهم, بالنسبة لإجراءات لا يوجد في أي من التشريعات نص خاص بها, لذلك تطبق القواعد العامة اذا ما كنا بصدد التفتيش بناءا على موافقة المتهم, حيث تنص المادة 76 من قانون الاجراءات الجزائية الفرنسي على انه يتم هذا التفتيش بتخلي المتهم عن الحماية التي كلفها له القانون لأن الأصل هو عدم جواز التفتيش دون موافقة صريحة من المتهم[1].

بالإضافة الى :

1– سبب التفتيش: حتى يكون التفتيش صحيحا لابد أن تكون هناك جريمة قد وقعت وهي جريمة معلوماتية[2], وهو ما أكدته المادة 5 من القانون 09/04

2– الغاية من التفتيش: لابد أن يكون التفتيش يقصد ضبط أشياء تتعلق بالجريمة أو تفيد في كشف الحقيقة والكشف عن أشياء تتعلق بالجريمة أو تفيد في كشف الحقيقة والكشف عن أشياء تتعلق بالجريمة أو تفيد في اظهار الحقيقة طبقا للنص المادة 44 ق.اج.ج

ولذلك يكون باطلا التفتيش الذي يجري لغاية اخرى

3– محل التفتيش هو المستودع الذي يحفظ فيه المرء بالأشياء المادية التي تضمن سره ومحل التفتيش في جرائم الانترنات هو الحاسب الالي الذي يعتبر النافذة التي تطل بها الانترنات, فقد يكون محل الحاسب الالي مكان أو عقار ما أو يكون بصحبة مالكه أو حائزه أو المكونات المادية او المعنوية للحاسب الالي ويقصد به هو المكان الذي يحتفظ فيه

[1] نورة طرشي, المرجع السابق,131.
[2] نبيلة هبة هروال, المرجع السابق, ص229.

الجاني أو المجرم بجميع الوسائل التي ارتكب بها الجريمة او يتمثل في المعلومات والاثار الموجودة والمحزنة على الحاسوب الموجود اما في مكان اقامة المشتبه فيه مثلا او المكونات المادية و المعنوية للحاسب الالي .

4- اذن التفتيش: طبقا للتشريع الجزائري فان الاذن لابد أن يكون مكتوب من طرف اما وكيل الجمهورية أو قاضي التحقيق المختص.

اضافة لما ذكر من الشروط فان هناك شروطا اخرى يضيفها القانون الانجليزي الأمريكي وهي:

- أن تكون الموافقة حقيقية خالية من الخداع والزيف.
- ووجوب اثباتها من طرف مأمور الضبط القضائي وأنها تمت دون عنف أو اكراه .

المطلب الثالث: مكافحة الجريمة المعلوماتية في القانون الجزائري

رغبة من المشرع الجزائري في التصدي لظاهرة الإجرام الالكتروني وما يصاحبها من أضرار معتبرة على الأفراد وعلى المؤسسات الدولة من جهة ومحاولة منه لتدارك الفراغ التشريعي القائم في هذا المجال من جهة أخرى، عمد منذ الألفية الثانية إلى تعديل العديد من القوانين الوطنية بما فيها الجانب الموضوعي والجانب الإجرائي من قانون العقوبات ،كما قام باستحداث قوانين أخرى خاصة لضمان الحماية الجنائية للمعاملات الإلكترونية، فقد حاول المشرع الجزائري إصدار قوانين عامة وخاصة وهياكل وأجهزة للتصدي للجرائم الالكترونية، فهناك جهود معتبرة قام بها المشرع الجزائري في محاربة قراصنة الإنترنت وإحالتهم قانونا على المحاكم ،متأثرا بجل الدول العربية التي وضعت قوانين لمكافحة الجريمة الإلكترونية ومن أهم الأمور التي أولها المشرع الجزائري أهمية قصوى أمن الدولة والحفاظ على النظام العام .

الفرع الاول: الاجراءات القانونية الخاصة بالجرائم المعلوماتية في قانون الاجراءات الجزائية

لقد أدرك المشرع الجزائري جيدا بأن المواجهة الفعالة للإجرام الالكتروني لا تكون فقط بإرساء قواعد قانونية موضوعية ذات طبيعة ردعية, انما لابد من مصاحبة هذه القواعد بقواعد اخرى اجرائية وقائية وتحفيظيه, والتي من شأنها ان تتفادى وقوع الجريمة الالكترونية أو على الأقل الكشف عنها في وقت مبكر يسمح بتدارك مخاطرها.

أولا: اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

الاعتراض والتسجيل والالتقاط والتسرب هي عدة تسميات يمكن اختزالها في مصطلح واحد هو "المراقبة" التي لا تخرج عن كونها رقابة مشروعة لشخص أو مراسلات مكتوبة أو مسموعة أو مرئية, نتيجة الاشتباه في تصرفات غير قانونية وذلك بصورة لا يحس معها الغير بمباشرتها لطابع السرية التي يكتنفها.

بالرجوع الى نص المادة 65 مكرر المستحدثة بموجب القانون رقم:22/06 المعدل والمتمم لقانون الاجراءات الجزائية نجد أن المشرع يحدد هاته الاساليب والتي تتمثل فيما يلي:

1- اعتراض المراسلات: يقصد بالمراسلات قانونا هي جميع الخطابات المكتوبة, سواء ارسلت بواسطة البريد أو رسول خاص, وكذالك المطبوعات والطرود والبرقيات التي توجد لدى مكاتب البريد, غير ان ما يلاحظ هو أن المشرع الجزائري حدد هذه المراسلات في الاتصالات السلكية واللاسلكية. [1]

[1] ابراهيم يامة, أساليب التحري الخاصة بالجريمة المنظمة في القانونين الجزائري والفرنسي, دفاتر السياسة والقانون, العدد الثاني ,المجلد 11, جوان 2019, ص 154.

2- تسجيل الأصوات: يتمثل في وضع الترتيبات التقنية وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية, واخفائها لتلقي أحاديث تفيد في تجلي الحقيقة وتسجيلها.[1]

3- التقاط الصور: يتمثل في وضع أجهزة التصوير المختلفة في أمكنة خاصة ودون موافقة المعنيين, من أجل التقاط صور لشخص أو عدة أشخاص تفيد في اجلاء الحقيقة وتسجيلها.[2]

وبالنظر لطبيعة اعتراض المراسلات وتسجيل الاصوات والتقاط الصور كإجراءات غير عادية, فان المشرع انطلاقا من أولوية رعاية المصلحة العامة على الحفاظ على أسرار الحياة الخاصة للأشخاص أقر العمل بها, ولكن وفق شروط موضوعية وشكلية دقيقة مما يحول معه دون التعسف في اللجوء على نطاق واسع وتعميمها على كل الجرائم.

ثانيا: التسرب

عرف المشرع الجزائري التسرب بموجب المادة 65 مكرر 12 من قانون الاجراءات الجزائية رقم 06/22 على أنه: " قيام ضابط او عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الاشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم انه فاعل معهم أو شريك أو خاف ".

من خلال هذا التعريف يمكن تصور عملية التسرب في نطاق جرائم الاعتداء على أنظمة المعالجة الالية في ولوج ضابط او عون الشرطة القضائية الى العالم الافتراضي(الانترنت) واشتراكه مثلا في محادثات غرف الدردشة او حلقات النقاش والاتصال المباشر في كيفية قيام احدهم باختراق شبكات أو بث الفيروسات, منتحلا في ذلك هوية مستعارة او باستخدام

[1] نجية الشيخ, أساليب البحث والتحري المستحدثة في القانون رقم 22/06 المعدل والمتمم لقانون الاجراءات الجزائية الجزائرية, المجلة النقدية, السند الرسمي, ص 294.

[2] نجية الشيخ, المرجع السابق, 294.

أسماء وصفات هيئات وهمية ظاهرا فيها بمظهر طبيعي كما لو كان فاعل مثلهم سعيا منه الى الكشف والاطاحة بالمجرمين.[1]

وقد بينت المادة 65 مكرر 15 الشروط الاجب توفرها في الاذن بالتسرب, وهي أن يكون مكتوبا ومسببا و ان يذكر فيه الجريمة التي تبرر اللجوء الى هذا الاجراء, وهوية ضابط الشرطة القضائية الذي تتم عملية التسرب تحت مسؤوليته.

كما يجب أن يحدد فيه أي الاذن _مدة عملية التسرب التي لايمكن أن تتجاوز أربعة أشهر كما أجازت المادة 65مكرر 15 كإجراء جديد في مكافحة الجريمة المعلوماتية اعتبار ضابط الشرطة القضائية الذي جرت عملية التسرب تحت مسؤوليته كشاهد عن العملية في اجراءات التحقيق فيها.[2]

الفرع الثاني: الاجراءات المنصوص عليها في القانون رقم 09/04

يتميز هذا القانون بأنه الاطار القانوني الأكثر ملائمة مع خصوصيات الجرائم المتعلقة بوسائل الاعلام والاتصال لا سيما الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت.

باستقراء فحوى هذا القانون يتبين لنا بأن المشرع استحدث تدابير جديدة غير مألوفة في القوانين السابقة للتصدي لجرائم المعلوماتية,[3] وتتمثل هذه التدابير الوقائية في مايلي :

أولا: مراقبة الاتصالات الالكترونية: لقد نصت المادة 04 من القانون 09/04 على أربع حالات التي يجوز فيها لسلطات الأمن القيام بمراقبة المراسلات والاتصالات الالكترونية, وذلك بالنظر الى خطورة التهديدات المحتملة وأهمية المصلحة المحمية وهي:[4]

---

[1] جمال ابراهيمي, مكافحة الجرائم الالكترونية في التشريع الجزائري, المجلة النقدية,ص142,143.

[2] نورة طرشي, المرجع السابق, ص 140.

[3] جمال ابراهيمي, المرجع السابق,151.

[4] اسمهان بوضياف, الجريمة الالكترونية والاجراءات التشريعية لمواجهتها في الجزائر, مجلة الاستاذ الباحث لدراسات القانونية والسياسية, العدد 11,سبتمبر 2018,ص366.

- للوقاية من الأفعال التي تحمل وصف جرائم الارهاب والتخريب وجرائم ضد أمن الدولة

- عندما تتوفر معلومات عن احتمال وقوع اعتداء على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو النظام العام.

- لضرورة التحقيقات والمعلومات القضائية حينما يصعب الوصول الى نتيجة تهم الأبحاث الجارية دون اللجوء الى المراقبة أو النظام العام.

- لضرورة التحقيقات والمعلومات القضائية حينما يصعب الوصول الى نتيجة تهم الأبحاث الجارية دون اللجوء الى المراقبة الالكترونية .

- في اطار تنفيذ طلبات المساعدات القضائية الدولية المتبادلة.

ثانيا: اقحام مزودي خدمات الاتصالات الالكترونية في مسار الوقاية من الجرائم المعلوماتية: وذلك من خلال فرض عليهم مجموعة من الالتزامات مذكورة في المواد 10,11و12 بالشكل التالي:[1]

- الالتزام بالتعاون مع مصالح الأمن المكلف بالتحقيق القضائي عن طريق جمع او تسجيل المعطيات المتعلقة بالاتصالات والمراسلات ووضعها تحت تصرفها مع مراعاة سرية هذه الاجراءات والتحقيق.

- الالتزام بحفظ المعطيات المتعلقة بحركة السير وكل المعلومات التي من شأنها أن تساهم في الكشف عن الجرائم ومرتكبيها, وهذين الالتزامين موجهين لكل مقدمي خدمات الاتصال الالكترونية دون استثناء.

- الالتزام بالتدخل الفوري لسحب المحتويات التي يسمح لهم الاطلاع عليها بمجر العلم طريقة مباشرة او غير مباشرة بمخالفتها للقانون, وتخزينها أو جعل الوصول اليها غير ممكن .

[1] جمال ابراهيمي, المرجع السابق, ص152,153.

- الالتزام بوضع ترتيبات تقنية للحد من امكانية الدخول الى الموزعات التي تحتوي على معلومات متنافية مع النظام العام والآداب العامة مع اخطار المشتركين لديهم بوجودها لديهم بوجودها, ونشير الى ان هذين الالتزامين يخصان فقط مقدمي الدخول الى الانترنت.

خاتمة

في الأخير نستخلص إن دراسة موضوع الجريمة المعلوماتية تكتسي أهمية بالغة كونها تساهم في التعريف بظاهرة إجرامية جديدة غير مألوفة بدأت في الظهور والانتشار في معظم الدول ومجتمعات العالم ونظرا لارتباطها بتكنولوجيا متطورة أدى إلى تميزها عن باقي الجرائم التقليدية من حيث تعريفها وطبيعتها القانونية وصولا إلى خصائصها المتميزة وكذا أنواعها التي تعددت وشملت الأشخاص والأموال ومؤسسات الدولة منها الأمنية والعسكرية وصولا إلى الملكية الفكرية والفنية و الأدبية بل تجاوزت ذلك إلى المساس بالأنظمة المعلوماتية والمكونات المادية والمنطقية وهذا ما أدى إلى ضرورة وجوب التصدي لذالك النوع من الجرائم ومواجهتها من خلال مجموعة من الآليات القانونية و إبرام اتفاقيات دولية للتصدي لهذا أنواع من الجرائم المعلوماتية ولا شك إن قانون 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتعديل قانون العقوبات الجزائري بموجب قانون 04/15 كانت لهما أهمية في تدارك الفراغ التشريعي الذي كان يملا القانون الجزائري وذلك من خلال حسم المشرع الجدل الفقهي القائم حول طبيعة المعلوماتية التي كانت تشوبها بعض العيوب والانتقادات وذلك من خلال استحداث القسم السابع مكرر في الفصل الثالث من المواد 394 مكرر 394 مكرر7 من قانون العقوبات كما إن هذا التعديل يعد قفزة في مجال التشريع كونه واكب التشريعات الأخرى بتجسيده معظم أحكام الاتفاقيات الدولية الخاصة بالجرائم المعلوماتية إلاَّ أنَّ المشرع الجزائري يبقى بعيد كل البعد عن التطور القانوني على المستوى العالمي من جهة وعن تطور أساليب ارتكاب هذا النوع من الجرائم من جهة أخرى مما يستلزم مراجعة وتطوير القوانين القائمة و إصدار المزيد من القوانين لتقوية الترسانة القانونية في هذا المجال

ولهذا فالجرائم المعلوماتية جعلت الخصوصية التي تتميز بها معظم الدول والهيئات والمنظمات الدولية و الإقليمية تدرك مدى خطورة هذه الظاهرة الإجرامية ومدى التحديات التي تفرضها عليها مما أدى بها إلى المسارعة من اجل وضعها في إطار قانوني يمكن من خلاله وضع طرق ناجعة وفعالة لمكافحتها ولقد تمثلت الجهود الدولية في تلك التي تبذلها منظمة الأمم المتحدة وذلك بعقد مؤتمرات وإبرام معاهدات واتفاقيات بين الدول و التحسيس بمخاطر هذه الظاهرة وتوجيه الدول وحثها على ضرورة مواكبة الركب من خلال سن قوانين داخلية في هذا المجال , أماً فيما يخص الجهود الإقليمية فتمثلت في جهود الاتحاد الأوروبي الذي يعتبر الإطار الأصلح و الانجح لمكافحة الجريمة المعلوماتية خاصة بعد اتفاقية بودابست سنة 2001 والتي وضعت الأسس والقواعد السليمة التي ينبغي تتبعها بالإضافة إلى الجهود العربية فبالرغم من قلتها وعدم بلوغها المستوي المطلوب إلاَّ إنَّها تبقي محاولات رائدة على مستوي الدول العربية , خاصة الجهود المبذولة على مستوي الجامعة العربية في انتظار المزيد من الجهود للحد من هذه الظاهرة ولحماية المكتسبات العربية , في ختام دراستنا المتواضعة والبسيطة يمكننا القول ان مكافحة الجرائم المعلوماتية يتطلب رسم سياسة وطنية صارمة تفرض عقوبات على مرتكبي هذا النوع من الجرائم ويستلزم أيضا أساليب وتقنيات متطورة لحماية المعلومات والتمكن من الكشف عن مرتكبي هذه الأعمال غير المشروعة بالإضافة إلى تكثيف التعاون الدولي من خلال تبادل الخبرات والمعلومات بخصوص الأساليب القانونية وكيفية صياغتها بالتصدي للجريمة المعلوماتية بشكل أكثر دقة ووضوح .

التوصيات:

خرجنا بعد دراسة بسيطة لموضوع الآليات القانونية لمكافحة الجريمة المعلوماتية في القانون الجزائري بجملة من المقترحات نذكر منها:

1- سن قانون إجرامي جزائي خاص وموحد تجمع وتحدد فيه مختلف الإجراءات بدقة ووضوح لمكافحة الجريمة المعلوماتية

2-إنشاء هياكل متخصصة في مكافحة هذا النوع من الجرائم , كالهيئة الوطنية لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال لكن هذا غير كاف ولا يزال يحتاج التفعيل حقيقي من خلال إعطائها الحرية الكاملة والاستقلالية في إنجاز مهامها .

3-التشجيع على خدمة تلقى الشكاوي والبلاغات إلكترونيا والعمل بها .

4-نشر ثقافة التبليغ من خلال عميلة تحسيس الأشخاص عامة والضحايا خاصة من اجل ضمان سهولة الكشف عن الجريمة المعلوماتية وسرعة اتخاذ الإجراءات المناسبة.

5-ضرورة استعانة الجزائر بخبير إلكتروني بجانب قاضي التحقيق إذا كان غير عارف التقنية أثناء التحقيق في تلك النوع من الجرائم .

6-تزويد الجهات الأمنية والقضائية بوسائل تعزز عملها لمواجهة الجرائم المعلوماتية .

7-تأهيل الجهات المختصة بمعالجة هذا النوع من الجرائم بدورات تكوينية وتدريبية لمواكبة تطور الجريمة المعلوماتية

8-رسم سياسة دولية تفرض عقوبات صارمة على مرتكبي الجرائم المعلوماتية

9-مراعاة التوازن بين البعد الأمني المعلوماتي وحق حرية التعبير عبر الوسائط الرقمية

10- ضرورة تعديل جميع التشريعات الخاصة بمكافحة الجريمة من خلال إضافة قوانين جديدة وهذا للاستفادة من تجارب الدول التي سبقتنا في مجال التشريع الخاص بتلك الجرائم شرط أن لا تكون مخالفة للنظام والآداب العامة

قائمة المصادر والمراجع

قائمة المراجع والمصادر

أولا: الكتب

1. أحمد خليفة الملط ،الجرائم المعلوماتية، دار الفكر الجامعي، الطبعة الثالثة،2006.
2. أمير فرج يوسف، الجرائم المعلوماتية على شبكة الانترنت، دار المطبوعات الجامعية، الاسكندرية، 2009.
3. جميل عبد الباقي صغير، المواجهة الجنائية لقرصنة البرامج التلفزيوني المدفوعة، دار النهضة العربية، القاهرة، 2001.
4. خالد عياد الحلمي، إجراءات التحري والتحقيق في جرائم الكمبيوتر والانترنت ،الطبعة الاولى ، دار الثقافة للنشر والتوزيع، عمان، 2011.
5. طارق ابراهيم الدسوقي عطية، الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، الطبعة الاولى ، دار الجامعة الجديدة ،2006.
6. طوني ميشال عيسى، التنظيم القانوني لشبكة الانترنت، طبعة 1، دار صابر للمنشورات، بيروت،2002.
7. عبد الله ماجد العكايلة، الوجيز في الضبطية القضائية ،الطبعة الاولى ،دار الثقافة للنشر والتوزيع ،عمان ،2010.
8. عفيفي كامل عفيفي، جرائم الكمبيوتر لحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشورات الحلبي الحقوقية، الطبعة الثانية، 2007.
9. علي القهوجي، قانون العقوبات القسم الخاص، دار النهضة العربية، القاهرة، 1993.
10. علي حسن محمد الطوالبة، التفتيش الجنائي عن نظم الحاسوب والانترنت، دار الجامعة الجديدة،2008.

11. الفتاح بيومي الحجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر الانترنت، الطبعة الأولى ، دار الفكر الجامعي، الاسكندرية،2006.
12. محمد حماد مرهج الهيتي، جرائم الحاسوب ،الطبعة الاولى ، دار المناهج للنشر والتوزيع ، الإسكندرية ،2012.
13. محمد زكي أبو عامر ـ قانون العقوبات –القسم الخاص دار النهضة العربية –القاهرة 1993
14. محمد سامي الشوا، ثورة المعلومات و انعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة،سنة1994.
15. نبيلة هبة هروال، الجوانب الاجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، الإسكندرية،2013.
16. هلال عبدلاه أحمد، التزام الشاهد بالإعلان الجرائم المعلوماتية، ط1، دار النهضة العربية،القاهرة،1997.

ثانيا: المقالات

1. ابراهيم ياما الشيخ، أساليب البحث والتحري المستحدثة في القانون رقم 22/06 المعدل والمتمم لقانون الإجراءات جزائية الجزائرية، المجلة النقدية، السند الرسمي.
2. أحمد السمدان، النظام القانوني لحماية برامج الكمبيوتر، مجلة الحقوقي، العدد 4، الكويت،1987.
3. اسماهان بوضياف، الجريمة الإلكترونية وإجراءات التشريعية لمواجهتها في الجزائر، الأستاذ الباحث للدراسات القانونية و السياسية، عدد 11، سبتمبر 2018.
4. جمال ابراهيمي ، مكافحة الجرائم الإلكترونية في التشريع الجزائري، المجلة النقدية.
5. شول بن شهرة، مراد مشوش، مجلة المستقبل للدراسات القانونية والسياسية، لعدد الأول، معهد الحقوق والعلوم السياسية آفلو الأغواط، جوان سنة2020.

6. صالحة العمري . جريمة غسيل الأموال وطرق مكافحتها ـ مجلة الاجتهاد القضائي ص 179 العدد 5 –جامعة محمد خيضر، بسكرة.

7. محمد هشام فريجه، النظام القانوني للجريمة المعلوماتية وصعوبات تحقيق الأمن الإلكتروني، كلية الحقوق والعلوم السياسية، جامعة المسيلة ، الجزائر ، تاريخ استقبال المقال 25/ 02/ 2018، تاريخ قبول نشر09/ 05/ 2018، المقال تاريخ نشر المقال 2018/07/10.

ثالثا: مداخلات وطنية و دولية:

1. ذكي ذكي أمين حسونة، جرائم الكمبيوتر والجرائم الاخرى في مجال التكتيك المعلوماتي، المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة،من25 الى 28 اكتوبر1993.

2.عبد الستار سالم الكبيسي، المسؤولية الجنائية الناشئة عن استعمال الحاسوب، سلسلة المائدة الحرة من ندوة القانون والحاسوب، بيت الحكمة، بغداد،1999.

رابعا: القوانين

1. دستور 1996، الجريدة الرسمية، رقم 76، المؤرخة في 8 ديسمبر1996، المعدل والمتمم بالقانون رقم 1/16 في 6مارس2016، ج ر، رقم 14 المؤرخة في 7 مارس2016.

2. دستور 2020،الصادر بموجب المرسوم الرئاسي 442/20 في 2020/12/30،ج ر 82 لسنة 2020، يتعلق بإصدار التعديل الدستوري المصادق عليه باستفتاء أول نوفمبر سنة 2020 للجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية .

3. قانون 09/04 المتعلقة بالقواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال ومكافحته، المؤرخ في 5 أوت 2006، الجريدة الرسمية العدد 47، الصادرة بتاريخ 16 أوت 2009.

خامسا: محاضرات

1. دليلة مباركي، محاضرات في قانون الإجراءات الجزائية، موجهة لطلبة سنة ثانية ليسانس حقوق، كلية الحقوق، باتنة،2022/2021.
2. سورية ديش، أنواع الجرائم الالكترونية واجراءات مكافحتها، جامعة جيلالي اليابس، سيدي بالعباس، الجزائر.
3. عيشة خلدون، محاضرات الجريمة المعلوماتية، السنة اولى ماستر، تخصص قانون جنائي والعلوم الجنائية، جامعة الجزائر، سنة 2021.
4. محمد بن أحمد علي المقصودي، الجرائم المعلوماتية خصائصها و كيفية مواجهته قانونيا، محاضرات بمعهد الإدارة العامة، الرياض، تاريخ النشر 5 أفريل 2016.

سادسا: الرسائل الجامعية:

اطروحات الدكتورة

1. عمر محمد بن يونس، الإجراءات الجنائية عبر الانترنت في القانون الأمريكي، رسالة دكتورة، كلية الحقوق، جامعة عين شمس، 2004.

مذكرات الماجستير

1. محمد بن عبد الله بن علي المنشاوي، جرائم الأنترنت في المجتمع السعودي، ماجيستير في العلوم الشرقية، أكاديمية نايف، العربية للعلوم الأمنية، الرياض ،2003.
2. نهلة عبد القادر المومني، الجرائم المعلوماتية، ماجيستير في القانون الجنائي المعلوماتي، دارالثقافة،عمان،ط2010.
3. نورة طرشي، مكافحة الجريمة المعلوماتية، مذكرات لنيل شهادة الماجستير في القانون الجنائي، جامعةالجزائر 1، كلية الحقوق 2011/ 2012.

4. يوسف صغير، الجريمة المرتكبة عبر الانترنت، ماجستير في قانون الأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزوو،2013.

مذكرات الماستر

1. ابتسام يغو، إجراءات المتابعة الجزائية في الجريمة المعلوماتية، مذكرة تكميلية لنيل شهادة ماستر في القانون، قانون جنائي، جامعة العربي بن مهيدي، أم البواقي،2016/2013

سابعا:الاتفاقيات الدولية

1. الاتفاقية المتعلقة بالجريمة الإلكترونية بودابست"، الصادرة عن مجلس اوربا_ مجموعة المعاهدات الاوروبية_رقم ١٨٥ بتاريخ 23 نوفمبر 2001

2. التقرير التفسيري لإتفاقية الجريمة الإلكترونية، مجلس اوربا، سلسلة المعاهدات الاوروبية، رقم 183، بودابست، في 23 نوفمبر/شيرين الثاني2001.

ثامنا: المواقع الالكترونية

1. http://eur-lex-europ a.eu/lexurisw/lex uni serv.do luri.cele x32002:fr.ht ml
2. www.convencions,coe,int 23 November 2001

المراجع باللغة الاجنبية

1. Champy essai de définition de la fraube informatiques. rs.c.i .1988.
2. Enquit fuding life insurence l'informatique nouvel le mai 1976.
3. Le monde informatique 21 fév. 1983 nous titre la de linquance rn.
4. LE report di conseil de l'Europe 15,18 nov, 1976 .
5. Luca, le droit de l’informatique, Thémis.

6. Tiedeman. Sraube et autres délits d’assure commis à l’aibe l’ordinateur elctrouniqe. R.d.p .c.1984.
7. Toty and hardCastle : computer related crine information technologie anbtchelaw u.k.1986.
8. Tre l de paris 12 eme ch corr jurement de 13jan 1982 Dalloz s 1982 ,p 502.

فهرس الموضوعات

فهرس الموضوعات

ملخص

تناولنا بالدراسة والتحليل في هذه المذكرة موضوع الآليات القانونية لمكافحة الجريمة المعلوماتية في القانون الجزائري أين حاولنا التعريف بهذه الظاهرة الإجرامية الجديدة التي بدأت في الانتشار عبر مختلف دول العالم مبرزين أهم خصائصها وطبيعتها القانونية و أنواعها ووجوب ضرورة التصدي لها من خلال آليات قانونية ردعية للحد من مخاطرها على الدول و الأشخاص , و أمام خطورة هذا النوع بالذات من الجريمة , يجب تكاثف التشريعات الدولية والداخلية للدول لمحاربة هذه الجرائم والقضاء عليها و إيجاد إطار خاص بها , يراعي خصوصية هذه الجريمة المستحدثة .

الكلمات المفتاحية:

الجريمة المعلوماتية. البرامج. النظام المعلوماتي. الكمبيوتر. الانترنت.

Summary :

We dealt with the study and analysais In This note the topic of legal mechanisonms to combat information crime in Algerian law where we tried to define this new criminal phenomenon that began to spread across various countries of the world ,highlighting its Most important characteristics, legal nature and types and the necessity of addressing it through deterrent legal mechanisms to limit among its dangers to states and people , and in view of the danger of this particular type of crime international and internal legislation of states must unite to combat and eliminate these crimes , and to find a frame work for them that takes into account the privacy of this newly created crime .

Key words :

Information crime. Software. Information. System. Computer. Internet.