جامعة العربي التبسي - تبسة -
كلية الحقوق والعلوم السياسية
قسم الحقوق

أطروحة مقدمة لنيل شهادة دكتوراه علوم في القانون الجنائي

بعنوان

الحماية الجنائية للمعطيات الرقمية

إعداد الطالبة/
عفاف خذيري

إشراف الأستاذ/
الطاهر دلول

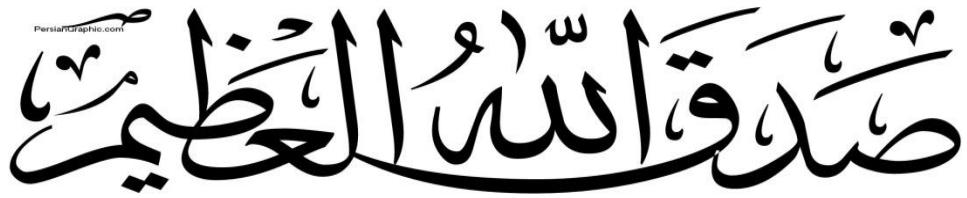
أعضاء لجنة المناقشة

الإسم واللقب	الرتبة العلمية	الجامعة	الصفة
بشير هادفي	أستاذ	جامعة العربي التبسي. تبسة.	رئيسا
الطاهر دلول	أستاذ	جامعة العربي التبسي. تبسة.	مشرفا ومقررا
عادل مستاري	أستاذ	جامعة محمد خيضر. بسكرة.	مناقشا
بدر الدين خلاف	أستاذ محاضر قسم. أ.	جامعة عباس لغرور. خنشلة.	مناقشا
كوسر عثمانية	أستاذ محاضر قسم. أ.	جامعة عباس لغرور. خنشلة.	مناقشا
هشام بخوش	أستاذ محاضر قسم. أ.	جامعة محمد الشريف مساعدية. سوق أهراس.	مناقشا

السنة الجامعية: 2018/2017

﴿ وَقُل رَّبِّ أَدْخِلْنِي مُدْخَلَ صِدْقٍ
وَأَخْرِجْنِي مُخْرَجَ صِدْقٍ وَاجْعَل لِّي مِن
لَّدُنكَ سُلْطَانًا نَّصِيرًا﴾

الآية رقم 80 من سورة الإسراء



إهداء

أهدي هذا العمل المتواضع إلى

أسرتي عائلة "خذيري"، وأسرة زوجي عائلة

"عثماني"،

وأخص بالإهداء إبنتي الحبيبة "أسيناث"

شكر وعرفان

إن الحمد و الشكر في المقام الأول لله الذي وفقني و ألهمني لإنجاز هذا العمل الذي ما كان ليكون لولا توفيق ومنة منه عز وجل.

أما بعد:

بكل فخرو اعتزاز ... و بكل شكر و عرفان، ووفاء و امتنان ... أتقدم بخالص شكري و عرفاني إلى أستاذي الفاضل الأستاذ الدكتور **الطاهر دلول** الذي تشرفت بمرافقته خلال طيلة مشواري الجامعي، وقد كان لي خير معين و خير ناصح و موجه في إنجاز هذه المذكرة.

كما يطيب لي أن أسجل كامل إمتناني و شكري للسادة أعضاء لجنة المناقشة، و أتوجه بالشكر الخاص للأساتذة الذين تحملوا مشقة التنقل من أجل مناقشة هذه المذكرة.

كما أتقدم بالشكر الجزيل إلى كل من ساعدني و أعانني على إنجاز هذه المذكرة من قريب أو بعيد.

مقدمة

لقد مهدت الثورة الصناعية التي تفجرت في منتصف القرن التاسع عشر، لبزوغ ثورة جديدة هي ثورة المعلومات، التي تقترن دائما بفكرة الحاسوب التي بدأها Charles Badbage الذي يعتبر أول من فكر في الحاسوب الرقمي من خلال سعيه الدؤوب لمكننة بعض العمليات الحسابية حيث إكتشف آلة الفروق ثم الآلة التحليلية ، وفي سنة 1943 قام جون فان نيومن J. W. Neumann عالم الرياضيات الأمريكي بوضع أسس الحاسوب كما هو معروف الآن ، والذي يتكون من خمسة مكونات أهمها إثنتان هما وحدة المعالجة المركزية ، التي يتم بواسطتها تنفيذ سلسلة العمليات الحسابية والمنطقية المطلوب تنفيذها، والذاكرة التي يتم فيها حفظ نتيجة كل عملية حيث يتم تنفيذ العملية طبقا لمجموعة من التعليمات أو البرامج المخزنة في الذاكرة ، فولد الحاسوب كجهاز رئيسي في الإعلام الآلي والمعلوميات ، وبفضل الحاسوب يعيش العالم الآن عصر المعلومات الذي يتسم بالتطور السريع لتكنولوجيا الحاسبات ، فقد أخذت المعلومات الآن ، في التزايد والتفاعل مع التقدم العلمي والتطور التكنولوجي كل دقيقة ، بل كل ثانية ، وبات تدفق المعلومات أساسا للرقي الحضاري للدول ، وبسبب تزايد المعلومات وكثرتها بدأت الدول تهتم بأساليب جمع هذه المعلومات وتبويبها وتصنيفها وتحليلها بغية الإستفادة منها ، في الوقت الذي تطورت فيه المستحدثات التكنولوجية ، والتي استهدفت التحكم في هذه المعلومات وتخزينها واسترجاعها ، وهو ما يعرف بتكنولوجيا المعلوماتية.

و قد كان لابد من استخدام الحاسبات في شتى مجالات الحياة ، ولكن في ظل بيئة المعلومات المخزنة آليا كان لابد أن "تضعف" قبضة الأمن والمراقبة والتحكم وأن تزدهر عمليات التجسس على المعلومات المعالجة إلكترونيا ، وقرصنتها وتخريبها وإتلافها ، حتى باتت تشكل تهديدا بالغا لسائر المنظمات الحكومية التي تعتمد أعمالها على الحاسبات والشبكات الإتصالية ، وترتفع مخاطر إساءة استخدام الحاسبات والتلاعب في البرامج وملفات المعلومات المخزنة آليا بقصد الحصول على أموال وأصول وخدمات غير مستحقة.

وتبرز أيضا كأهداف لعمليات التخريب والإرهاب منظومة معالجة المعلومات وقواعد البيانات وبرامج الحاسبات وشبكات الإتصال لاسيما المستخدم منها في الأغراض الدفاعية ، وبدأت الدول سواء المتقدمة منها أو السائرة في طريق النمو ومن بينها الجزائر تعاني من جرائم العبث والتخريب الموجه إلى الحاسبات ذاتها ، وسرقة المعلومات المخزنة فيها والإحتيال والغش المالي المرتبط بها والإستخدام غير المصرح به لخدمات الحاسبات وغيرها من الجرائم الفنية التي تحولت من مجرد إنتهاكات فردية لأمن النظم إلى ظاهرة تقنية تهدد الأمن القومي قبل أن تهدد الشركات والمؤسسات والأفراد لاسيما وأن شبكة الإنترنيت ، منذ أن توصل " فان سير" الباحث الأمريكي في جمعية لوس أنجلس سنة 1974

إلى هذا النظام الذي يسر ارتكاب جرائم معلوماتية عابرة للحدود ، بحيث أنه يمكن لشخص تتوافر لديه المهارة الفنية ويتسلح ببعض التجهيزات التقنية أن يمحو أو يعدل أو يخرب أو يستولي... على بيانات معالجة إلكترونيا في دولة أخرى خلال ثوان محدودة ، ويزداد الأمر خطورة عندما يتعلق الأمر بالإعتداء على البرامج الحساسة ذات الصلة بالجوانب العسكرية والأمنية والإستراتيجية للدول التي تتضمن خطط الحروب ، أو ضوابط الإنتاج إلى غير ذلك ، وبناء عليه فإن موضوع الجرائم المعلوماتية يكتسي أهمية قصوى من عدة نواح ، سواء العملية أو النظرية.

وإذا كان التطور المتجدد للمعلوميات يحجم صورة التجريم الحالية عن مواكبة ما يطرأ من صور إجرامية مستحدثة إلا أن وضع قواعد قانونية تنظم أوجه الحماية الجنائية أفضل بكثير من ترك ما يستجد على الساحة الجنائية دون حماية ، وهذا ما يقع على عاتق الفقه بداية بوضع نظرية عامة تسهم في صياغة المشرع للنصوص التشريعية وتساعد القضاء على تفسير النصوص وتكييف الوقائع.

ولقد أصبحت الجريمة في مجال المعطيات الرقمية بأبعادها و مظاهرها الحديثة ، تمثل تهديدا مباشرا للأمن و الإستقرار و السلام في العالم ، وعائقا يحول دون إتمام عمليات التطور و التنمية ، ولم تعد عواقبها قاصرة على بعض الأفراد أو الجماعات ، بل إمتدت آثارها لتهدد دولا برمتها ، بما يؤكد على الحاجة إلى التعاون و التنسيق بين أجهزة القضاء من أجل مجابهة شاملة لتلك الأبعاد الخطيرة.

ولقد أصبحت المعلوماتية قوة لا يستهان بها في أيدي الدول و الأفراد ، وكان هذا التطور الهائل الذي شهده قطاع تكنولوجيا المعلومات و الإتصالات و الإندماج المذهل الذي حدث بينهما فيما بعد هو المحور الأساسي الذي قامت عليه الثورة المعلوماتية ، و أدى هذا التطور في مجال المعلومات إلى ظهور الإنترنت التي جعلت من العالم قرية صغيرة ، وكذلك تطورت الجريمة و ظهر نوع جديد من الإجرام و هي جريمة المساس بالمعطيات الرقمية ، وهو ما جعل العديد من الدول تسعى إلى مكافحة هذه الجريمة من خلال إبرام العديد من الإتفاقيات كاتفاقية بودابست.

وتعد التكنولوجيات الرقمية الحديثة من أبرز سمات العصر الحديث ، و أصبح المجتمع الآن يقاس بمدى تطور وسائل تبادل المعلومات فيه عبر منظومة الإنترنت التي شاع استعمالها في مجتمعنا و التي ساهمت في تعزيز التواصل الحضاري و الثقافي و تعزيز التفاهم الإنساني و كسر الحواجز أمام التواصل بين الشعوب الذي أسهم بدوره إلى حد كبير في تغيير أنماط المعرفة.

ـ أهداف الموضوع:

نهدف من خلال دراستنا لموضوع الحماية الجنائية للمعطيات الرقمية إلى تحقيق جملة من الأهداف العلمية والعملية أهمها:

1ـ الأهداف العلمية:

ـ مع بداية إنتشار شبكة الإنترنت لم يكن هناك قلق تجاه الجرائم التي يمكن أن تنتهك على الشبكة ، وذلك نظرا لمحدودية مستخدميها حيث كانت قاصرة على أغراض البحث العلمي و مقتصرة على فئة معينة ، و بتوسع إستخدام هذه الشبكة و بدء إستخدامها في المعاملات التجارية ، والإقتصادية ... ودخول جميع فئات المجتمع إلى قائمة المستخدمين بدأت تظهر جرائم على الشبكة إزدادت مع الوقت و تعددت صورها و أشكالها.

ـ لم تغير التكنولوجيا في صور الجرائم من تقليدية إلى جرائم حديثة فقط بل غيرت أيضا في شكل المجرمين حيث أصبح هؤلاء يستهدفون إختراق أجهزة الحاسوب ، أو البريد الإلكتروني أو المواقع الإلكترونية على شبكة الإنترنت و خصوصا المواقع الإلكترونية التي تكون للشركات المعروفة و التي غالبا ما تكون مستهدفة من قبل شركات منافسة لها ، وقد تستهدف المواقع الإلكترونية للبنوك بهدف الدخول إلى حساب أحد العملاء فيها و بسرقة الأموال.

ـ يعتبر الحق في الخصوصية من بين الحقوق المكفولة دستوريا و المحمية في القوانين الوطنية و حتى القوانين الدولية ، و مع التطور العلمي و التكنولوجي الحديث تم اختراع وسائل الإتصال الحديثة كالهواتف الذكية و أجهزة الاعلام الآلي ، وأدى ذلك بدوره إلى اقتحام البريد الإلكتروني و كسر الشيفرات الخاصة به و العبث بالملفات الخاصة بالأفراد بتغيير البيانات ، و المعطيات الخاصة بهم ولم يتوقف الأمر عند هذا الحد بل وصل إلى سب و قذف و تشويه سمعة هؤلاء الأفراد.

ـ أيضا يلعب الأمن الوطني دورا مهما في حياة واستقرار الدولة ، و بدخول التكنولوجيا و بدواعي استخدامها داخل أجهزة الدولة ظهر نوع جديد من المجرمين أطلق عليه الإرهاب الإلكتروني لما يقوم به من قرصنة و تجسس إلكتروني وقد إعتبرته إتفاقية بودابست من أخطر أنواع الجرائم ترتكب عبر شبكة الإنترنت ، وهو بذلك يمس مبدأ السيادة من جهة و يزعزع مكافحتها في المجتمع الدولي من جهة أخرى.

2 ـ أهداف عملية: ومنها

ـ لقد أفرزت الجريمة المعلوماتية تحديات واضحة للقوانين التي وضعت لمكافحتها ، لذلك أظهرت ثورة الإتصلات الرقمية و المعلوماتية نوعا جديدا من الجرائم أطلق عليه بالجريمة الرقمية لم يتصور المشرع حدوثها أصلا فقد تغيرت الجريمة من صورتها التقليدية المتمثلة في صورتها المادية إلى أخرى معنوية ، ونتج من ذلك مشكلة تفسير النصوص القانونية ، و حظر القياس في المواد الجنائية و مبدأ الشرعية الجنائية ، وهذه العوامل تؤدي إلى إفلات الكثير من المجرمين من العقاب.

ـ بعد دراسة موضوع الحماية الجنائية للمعطيات الرقمية فإن ذلك يساعد على الفهم الأكاديمي لأنواع الجرائم الرقمية و الوقوف على وسائل مكافحة هذه الجرائم.

ـ بإعتبار أن الجرائم الرقمية تميزت بشيء من الخصوصية فكانت إجراءات متابعة هذه الجرائم لها هي الأخرى طابع آخر غير الإجراءات المعروفة في الجرائم التقليدية من تحقيق وإثبات هذه الجرائم ، وكذلك طريقة الإستعانة بالخبرة و الشهود باعتبار أن هذه الجرائم إلكترونية من جهة و حديثة من جهة أخرى.

ـ المنهج المتبع:

إعتمدنا للإجابة عن الإشكالية المطروحة في هذه الدراسة على المنهج التحليلي والمنهج الوصفي ، وهذا ما تتطلبه الدراسة في مثل هذه المواضيع:

ـ المنهج الوصفي : باعتبار أن الجرائم الرقمية تعتبر من الجرائم الحديثة تطرقنا إلى ماهية المعطيات الرقمية من خلال تعريفات قانونية و أخرى فقهية ، وبينا خصائص جرائم الإعتداء على المعطيات الرقمية ، وأهم صور هذه الإعتداءات ، مما يفرض معالجة بعض المعلومات و المعطيات.

ـ المنهج التحليلي: باعتباره المنهج المناسب لمعالجة مختلف العناصر الأساسية للبحث من تحليل و

شرح للنصوص القانونية محل الدراسة لبيان موطن الصواب ليحقق هذا البحث أهداف علمية ، كما أن

إتباع هذا المنهج سيكون ضروريا لتحليل بعض النصوص القانونية الخاصة بالتشريع الجزائري و مدى كفاية هذه النصوص في تحقيق حماية المعطيات الرقمية ، وتتخلل هذه الدراسة بعض التشريعات المقارنة و ذلك بسبب ندرة النصوص القانونية الجزائرية في هذه المادة من جهة أخرى.

ـ أهمية الموضوع:

تكمن أهمية دراسة موضوع الحماية الجنائية للمعطيات الرقمية ، في إعتبار أن الجرائم الماسة بالمعطيات الرقمية من الجرائم الحديثة ، وقد تنوعت أساليب إرتكابها و تزايدت مخاطرها و حجم الخسائر الناجمة عنها ، حتى باتت تشكل مصدرا من مصادر تهديد الأفراد في حرمة حياتهم الخاصة ، و تهديد أمن الدولة في جانبها الأمني و الإقتصادي خاصة تلك الدول التي تعتمد بشكل كبير على تقنية المعلوماتية في مرافقها العامة ، و قد تفاقم الأمر بإختراق المؤسسات المالية التي تعتمد على الحاسبات الآلية إعتمادا كليا لتسيير أعمالها و تنظيم حساباتهم و غيرها من الجرائم ، لذلك كان على المشرع الجزائري أن يكافح هذا النوع من الإجرام بسن القوانين و فرض العقوبات سواء عقوبة السجن أو الغرمات المالية أو كلاهما إذا تطلب الأمر ذلك.

ـ الدراسات السابقة:

يعتبر موضوع الحماية الجنائية للمعطيات الرقمية من بين الموضوعات الحديثة و التي لم يتم التطرق لدراستها سابقا إلا أن هناك بعض الدراسات التي تطرقت إلى جزئيات من الموضوع ومن بين هذه الدراسات:

ـ تركي بن عبد الرحمن الموشير ، بناء نموذج أمني لمكافحة الجرائم المعلوماتية و قياس فاعليته ، أطروحة دكتوراه ، كلية الدراسات العليا بجامعة نايف العربية للعلوم الأمنية ، الرياض ، سنة 2009

ـ عاقلي فضيلة ، الحماية القانونية للحق في حرمة الحياة الخاصة ، أطروحة دكتوراه ، جامعة قسنطينة ، الجزائر ، سنة 2012.

ـ محمد على سالم ، حسون عبيد ، هجيج الجريمة المعلوماتية ، مجلة جامعة بابل ، العلوم السياسية ، العدد 14، العراق ،سنة 2008.

– بوحليط يزيد ، السياسة الجنائية في مجال مكافحة الجرائم الالكترونية في الجزائر أطروحة دكتوراه ، كلية الحقوق ، قسم القانون الخاص ، جامعة باجي مختار عنابة ، 2016.

ـ سامي عبد الرحمان واصل، إرهاب الدولة في إطار القانون الدولي العام، رسالة لنيل درجة الدكتوراه في القانون، جامعة عين شمس، القاهرة، 2003.

ـ أسباب إختيار الموضوع:

ترجع أسباب إختياري لموضوع الحماية الجنائية للمعطيات الرقمية إلى مجموعة من الأسباب الموضوعية و الذاتية على النحو التالي:

أ/ الأسباب الموضوعية:

ـ بعد التطور الذي شهده العالم بشكل هائل و متسارع في تكنولوجيا عالم الإتصالات أصبحت وسائل الإتصال الحديثة وعلى رأسها الإنترنت وسيلة لا يمكن الإستغناء عنها ، فبعد أن كانت الإتصالات تعتمد على التليفون ثم الفاكس ظهرت الإنترنت ، و أصبحت الوسيلة المثلى في الإتصال و نقل المعلومات و تقديمها وعليه ظهرت مجموعة من الإعتداءات و الإختراقات مما أدى إلى ظهور جرائم السرقة و الإحتيال خصوصا مع كثرة المستخدمين و المتعاملين مع شبكة الإنترنت.

ـ ولقد أدى ظهور الحاسبات الآلية إلى تغيير شكل الحياة في العالم ، وقد أصبح الإعتماد على وسائل تقنية معلوماتية حديثة سواء في المؤسسات المالية أو المرافق العامة أو المجال التعليمي أمرا حتميا ، ولكن هذه الإستخدامات للتكنولوجيات أظهرت الوجه الأخر لها و ظهر ما يسمى بالإرهاب الإلكتروني و التجسس الإلكتروني الذي أصبح يهدد أمن و استقرار الدول و يهدد العالم بأسره لذلك إرتأينا دراسة هذا الموضوع من أجل تسليط الضوء على مختلف الجرائم التي ترتكب باستخدام الحواسيب الآلية.

ـ تعتبر الجرائم الماسة بالمعطيات الرقمية من الجرائم المستحدثة و ترتكب ضد الأفراد و الجماعات مع وجود دافع إجرامي لإلحاق الضرر عمدا بسمعة الضحية بكل الأشكال باستخدام شبكات الاتصال الحديثة مثل الانترنت و غرف الدردشة ، و البريد الالكتروني.

ـ شهد العالم في الفترة الأخيرة في شتى المجالات تطورا كبيرا خاصة في مجال تقنية المعلومات وكان الإلتجاء إلى حماية المعلومات وتخزينها وجمعها أمرا ليس سهلا ، كما أصبحت الوسيلة التقليدية شبه

عاجزة لذلك كان من الضروري وجود وسائل أكثر تطور لحماية هذه المعلومات خاصة بعد ظهور إمكانية إعتبار هذه المعلومات أموالا معنوية.

ب/ أسباب ذاتية:

ـ رغبتي الشخصية في البحث في مجال المعلوماتية و الرقمية وذلك بالإطلاع على أن هناك إختراقات و إعتداءات تقع عبر الشبكة المعلوماتية ـ الإنترنت ـ دون أن تسلم منها الدول سواء الدول المتقدمة أو السائرة في طريق التقدم ، كما تقع على الأفراد ودون حتى علم منهم.

ـ إثراء المكتبة القانونية بمراجع تخص التكنولوجيا الرقمية خاصة فيما يخص التشريع الجنائي الجزائري.

ـ صعوبات البحث:

تمثلت صعوبة البحث في ما يلي:

ـ رغم الترسانة القانونية التي سنها المشرع الجزائري في مجال المعلوماتية إلا أن هناك بعض الثغرات إما لم يعالجها المشرع أو أن هناك نقص في هذه القوانين.

ـ قلة الأبحاث و المراجع في موضوع المعطيات الرقمية خاصة في القانون الجزائري التي تساعد في إتمام هذا البحث.

ـ الإشكالية:

منذ عقد مضى لم نكن نتصور أن الحياة سوف تعتمد بصفة أساسية و مطلقة على جهاز الحاسب الآلي وملحقاته ، إلا أن ذلك أصبح واقعا و حقيقة خاصة بعد إعتماد مؤسسات الدولة و الأفراد على هذه التكنولوجيا ، غير أن هذه الأخيرة فتحت الباب على مصراعيه لظهور صور من السلوك الإجرامي التي لم يكن من الممكن وقوعها في الماضي ، و تخرج عن دائرة التجريم و العقاب القائمة ، لأن المشرع لم يتصور حدوثها أصلا ، فمن ناحية سمحت المعلوماتية بظهور صور جديدة من الجرائم لم تكن موجودة في الماضي ، كالإعتداءات الرقمية مثل سرقة المعلومات و الأسرار المودعة في قواعد البيانات ، وجرائم الغش و الإتلاف ، و إفساد المعلومات المخزنة في قواعد المعلومات ، و في ظل

خطورة هذا النوع من الجرائم يطرح التساؤل حول مدى كفاية الوسائل القانونية التي إعتمادها المشرع الجزائري في مواجهة الجرائم الماسة بالمعطيات الرقمية؟.

و في سبيل الإجابة على هذه الإشكالية تثور مجموعة من الإشكاليات الفرعية على النحو التالي:

ـ ما هي المعطيات الرقمية؟.

ـ و ما هي أهم صور الإعتداءات التي تقع على المعطيات الرقمية؟.

ـ و ما هي الإجراءات الواجب إتباعها لفرض حماية على المعطيات الرقمية؟.

ـ خطة البحث:

من أجل الإجابة على هذه الإشكالية و مجموعة الأسئلة الفرعية رأينا تقسيم موضوع الحماية الجنائية للمعطيات الرقمية إلى بابين:

ـ الباب الأول: بعنوان الأحكام الموضوعية للحماية الجنائية للمعطيات الرقمية ، وقد قسمنا هذا الباب إلى فصلين ، تناولنا في الفصل الأول: الإطار المفاهيمي حول المعطيات الرقمية ، و تحت هذا العنوان تناولنا مفهوم المعطيات الرقمية ، ثم أركان الجرائم الماسة بالمعطيات الرقمية ، و في الفصل الثاني: صور الإعتداء على المعطيات الرقمية ، تطرقنا أولا إلى الجرائم التي تقع على الأشخاص و الأموال ، ثم الجرائم التي تقع على الأمن الوطني ، أما في الباب الثاني فتناولنا الأحكام الإجرائية للمعطيات الرقمية ، وقد قسمنا هذا الباب إلى فصلين:

الفصل الأول: التحقيق في الجرائم الماسة بالمعطيات الرقمية و ذكرنا الأعوان المكلفون بمكافحة الجرائم الماسة بالمعطيات الرقمية ، كيفية التفتيش في هذه الجرائم ، وفي الفصل الثاني تطرقنا إلى إثبات الجرائم الماسة بالمعطيات الرقمية ثم الجزاءات المقررة للجرائم الماسة بالمعطيات الرقمية سواء للشخص الطبيعي أو المعنوي.

ـ الخاتمة: و فيها تم عرض أهم نتائج و التوصيات الخاصة بالموضوع.

البـــاب الأول: الأحكام الموضوعية للحماية الجنائية للمعطيات الرقمية

الباب الأول: الأحكام الموضوعية للحماية الجنائية للمعطيات الرقمية.

كانت أغلب الثورات مقتصرة على الأموال المادية دون غيرها لما كانت تحمله من أهمية ، إلا أنه وفي منتصف القرن العشرين إختلف الأمر بظهور الكمبيوتر ، الذي أصبح له دور رئيسي بل وفعال في شتى مجالات الحياة ، حيث كان له دور في الدفع بعجلة التطور و التقدم و إرساء دعائم الصناعة نظرا لما أصبحت تمتاز به من تطور و ازدهار ، لذلك أصبحت المعلومة الإلكترونية الركيزة الأساسية لتقدم الأمم على مختلف الأصعدة كما أصبحت اليوم وسيلة ضغط من طرف العالم المتقدم على العالم السائر في طريق النمو خاصة في المجال العلمي و الإقتصادي و السياسي حتى تفرض هذه الدول هيمنتها في كل مجالات الحياة ، ولا يخفي علينا أن المعلومة هي أحد ثمرات فكر الإنسان التي تتحول فيما بعد إلى رصيد معرفي تستسقي منه البشرية كل ما هي بحاجة إليه لتيسر سبل حياة البشر و هذه هي الخدمة التي يقدمها البشر لبعضهم البعض.

وبظهور شبكة المعلومات زادت أهمية الكمبيوتر الذي بدوره زاد من أهمية التطورات خاصة خلال سنوات السبعينات حيث تم الفصل بين المكونات المعنوية للبرامج و بين المكونات المادية ومن هنا بدأت صناعة البرامج في التطور بسرعة كبيرة و أصبحت هذه البرامج منتوجا في حد ذاته تمس بنظم المعالجة الآلية للمعطيات كيف لا وهي قد أصبحت المجال الخصب لاختراقات العديد من الأشخاص أو المجموعات ، كما أن مواقع التواصل الإجتماعي أصبحت المكان المناسب لنشر معطيات وخصوصيات الأشخاص سواء الطبيعيين أو المعنويين وهذا ما يعرف بالإعتداء على المعطيات الرقمية ، لذلك قسمنا هذا الباب إلى فصلين تناولنا في الفصل الأول: ماهية المعطيات الرقمية وفي الفصل الثاني صور الإعتداء على المعطيات الرقمية.

الفصل الأول: ماهية المعطيات الرقمية.

مع بداية إنتشار شبكة الإنترنت لم يكن هناك قلق تجاه الجرائم التي يمكن أن ترتكب على الشبكة ، وذلك نظرا لمحدودية إستخدامها حيث كانت قاصرة على أغراض البحث العلمي فقط وذلك لكونها مقتصرة على فئة معينة من المستخدمين وهم الباحثين والعلماء وطلبة الجامعات ومع ظهور الثورة المعلوماتية وتوسع إستخدام شبكة الإنترنت وبدء إستخدامها في المعاملات التجارية والإقتصادية والثقافية ودخول جميع فئات المجتمع إلى قائمة المستخدمين بدأت تظهر جرائم على الشبكة إزدادت مع الوقت وتعددت صورها وأشكالها ، وهذه الجرائم يطلق عليها بالجرائم المعلوماتية أي تلك الأعمال والأفعال المجرمة من إختراقات وتلاعب بالبيانات الرقمية لمستخدمي هذه الشبكة والتي عادة تتم عن طريق الإنترنت باعتبارها شبكة عالمية من جهة وأسرع طريق لنشر المعلومات وحذفها في أسرع وقت ممكن لذلك تعتبر من أهم وأخطر التحديات التي تواجه المعلومات الإلكترونية ، ونظرا لكثرة الإعتداءات على البيانات المتواجدة على الشبكة المعلوماتية ظهرت عدة تعريفات حول هذا الموضوع ، لذلك قسمنا هذا الفصل إلى مبحثين تناولنا في المبحث الأول مفهوم المعطيات الرقمية وفي المبحث الثاني أركان جريمة المساس بالمعطيات الرقمية.

المبحث الأول: مفهوم المعطيات الرقمية.

لقد مهدت الثورة الصناعية التي تفجرت في منتصف القرن التاسع عشر لبزوغ ثورة جديدة هي ثورة المعلومات التي تقترن دائما بفكرة الحاسوب ، و الذي بفضله يعيش العالم الآن عصر المعلومات الذي يتسم بالتطور السريع لتكنولوجيا الحاسبات ، فقد أخذت المعلومات الآن في التزايد و التفاعل مع التقدم العلمي و التطور التكنولوجي و بسبب كثرة المعلومات بدأت الدول تهتم بأساليب جمع هذه المعلومات و تبويبها و تصنيفها و تحليلها بغية الإستفادة منها في الوقت الذي تطورت فيه المستحدثات التكنولوجية التي استهدفت التحكم في هذه المعلومات و تخزينها واسترجاعها.

وهذا الكم الهائل من المعلومات كان لابد من إدراجه في الكمبيوتر ، ولكن في ظل بيئة المعلومات المخزنة آليا كان لابد من أن تضعف قبضة الأمن و المراقبة و التحكم و أن تزدهر عمليات التجسس على المعلومات المعالجة إلكترونيا و قرصنتها و تخريبها و إتلافها ، حتى باتت تشكل تهديدا بالغا لسائر المنظمات الحكومية التي تعتمد أعمالها على الحاسبات و الشبكات الإتصالية ، وترفع مخاطر إساءة إستخدام الحواسيب و التلاعب في البرامج و ملفات المعلومات المخزنة آليا بقصد الحصول على أموال وخدمات غير مستحقة هذا من جهة ، ومن جهة أخرى تثير المعلومات باعتبارها أهم عنصر في عالم المعالجة الآلية للمعطيات عدة مشاكل قانونية فقد ساء إستخدامها لارتكاب الجريمة عن بعد من ناحية أو كونها محلا للإعتداء عليها من ناحية أخرى مما يثير مسألة الإعتداء وما إذا كان يشكل جريمة أم لا ، لذلك قسمنا هذا المبحث إلى مطلبين تناولنا في المطلب الأول: تعريف المعطيات الرقمية و في المطلب الثاني: خصائص جرائم الإعتداء على المعطيات.

المطلب الأول : تعريف المعطيات الرقمية.

إن التطور التقني الحاصل في عالم تكنولوجيا المعلومات و ما يتطلبه من ضرورة القيام بمهام توفير و جمع و معالجة و تبادل المعلومات في نفس الوقت أدى إلى ارتكاب جرائم نظام المعالجة الآلية ، و الذي نشأ في الحقيقة بهدف و صف الحالة التي انبثقت عن إندماج تقنية نظام المعلومات و تقنية الإتصالات عن بعد ، وقد تم تعريفه على أنه عبارة عن آلية و إجراءات منظمة تسمح بتجميع و تصنيف و فرز البيانات و معالجتها و من ثم تحويلها إلى معلومات يستخرجها الإنسان عند الحاجة ليتمكن من إنجاز عمل و اتخاذ قرار أو القيام بأي وظيفة عن طريق المعرفة التي يحصل عليها من

المعلومات المسترجعة من النظام الذي يحتوى على ما يسمي بالمعطيات و عليه فإننا سنتطرق إلى تعريف المعطيات[1].

1- تعريف المعطيات:

لقد اجتهد فقهاء و دارسي القانون محاولين في ذلك إيجاد تعريف للمعطيات فعرفها البعض بأنها عبارة عن مجموعة من الأرقام و الكلمات و الرموز أو الحقائق أو الإحصاءات الخام التي لا علاقة بين بعضها البعض و لم تخضع بعد للتغير أو التجهيز للإستخدام ، أما المعلومات فهي المعنى الذي يستخلص من هذه المعطيات.

وقد عرفت الوكالة الفرنسية المعطيات les donnes بأنها كل حدث مفهوم أو تعليمة تقدم في شكل متفق عليه قابلة للتبادل عن طريق البشر أو بواسطة الحاسوب أو ينتجها الحاسوب[2] ، ولقد اعتمدت إتفاقية بودابست للجريمة المعلوماتية في تعريف المعطيات ذات التعريف الذي ذهبت إليه هيأة التوصيف العالمية الإيزو ، حيث نصت في مادتها الأولى على أن المعطيات هي كل تمثيل للوقائع أو المعلومات أو المفاهيم تحت أي شكل و تكون مهيأة للمعالجة بما في ذلك برنامج معد من ذات الطبيعة و يجعل الحاسوب يؤدي المهمة.

وقد أخذت التوصية الصادرة عن منظمة التعاون الإقتصادي و التنمية في 1992.11.26 الخاصة بحماية أنظمة الحاسبات الآلية و شبكات المعلومات بالتفرقة السابقة ، حيث عرفت المعطيات بأنها مجموعة من الحقائق أو المفاهيم أو التعليمات تتخذ شكلا محددا يجعلها قابلة للتداول و التغيير أو للمعالجة بواسطة الأفراد أو بوسائل إلكترونية ، أما المعلومات فهي المعنى المستخلص من هذه المعطيات[3].

و تأسيسا على هذا المعنى فإن المعطيات تعتبر المواد الخام التي تستخرج منها المعلومات باستخدام معالجة آلية في عملية الإستخراج ، إذ يتم تجميع وتشغيل المعطيات للحصول على المعلومات ثم تستخدم في إصدار قرارات تؤدي بدورها إلى مجموعة إضافية من المعطيات و التي يحصل تجميعها و معالجتها مرة أخرى للحصول على معلومات إضافية.

---

[1]- هشام محمد فريد رستم ، قانون العقوبات و محاضر تقنية المعلومات، مكتبة الآلات الحديثة 1992،ص26.

[2]- مفتاح محمد دباب، معجم المصطلحات و تكنولوجيات المعلومات و الاتصالات ، الدار الدولية للنشر ، القاهرة 1995،ص 42.

[3]- إنتصار عريب، أمن الكمبيوتر و القانون ، دار الراتب الجامعية ، بيروت ، ص81.

2- تعريف المعطيات في القانون الجزائري:

لقد أخذ المشرع الجزائري بما أخذت به باقي التشريعات فبالرجوع إلى قانون العقوبات القسم السابع مكرر03 بعنوان المساس بأنظمة المعالجة الآلية للمعطيات نجد أن المشرع لم يعرفها و قد أحسن بعدم تعريفه للمعطيات و ذلك نظرا للتطور التكنولوجي المستمر و التطورات السريعة و المتلاحقة على التقنيات الذي حال دون ذلك فما نراه اليوم من برامج أو بيانات خاضعة للحماية قد لا يكون غدا و العكس صحيح ، فكان مصطلح المعطيات مقصود به البيانات الرقمية و غير الرقمية و المعطيات ... الخ ، حيث يعتبر هذا المصطلح أشمل و أعم.

بينما جاء مصطلح المعطيات المعلوماتية في قانون القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال بأنها "أي عملية عرض للوقائع أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها"[1].

وبهذا التصور تكون المعطيات عبارة عن حقائق رقمية أو غير رقمية تتم بطريقة منهجية يمكن فهم دلالتها مباشرة دون الدخول في عمليات إستنتاجيه استقرائية لدلالاتها المعقدة من خلال أكثر من بيان[2]، لأن ذلك يعني أن التحول من كون الأمر مجرد معطيات إلى بيانات و معلومات لذلك وجب تعريف البيانات و المعلومات على أنها:

الفرع الأول: تعريف البيانات:

إن دراسة الطبيعة القانونية للبيانات أمر هام و ضروري إذ أن تطور و تنوع هذه البيانات غيّر تماما وسائل تحليل القوانين المعاصرة ، فليس من الغريب أن المسائل الخاصة بقواعد البيانات أصبحت محل جدل و يعود الأمر إلى سببين هما:

- التطور التكنولوجي في وسائل الإتصالات و عملية إدراج هذه البيانات على الأجهزة الإلكترونية.

[1]- أنظر المادة 02من القانون رقم 04.09المؤرخ في 05غشت 2009متضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها ، ج ر، العدد 47.

[2]- رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري و المقارن منشورات الحلبي الحقوقية ، الطبعة الأولى ، سنة 2012، ص67.

– عدم إدراك الأفراد للمعنى الحقيقي للبيانات و مدى خطورتها إستغلالها و هي مشاكل في تزايد مستمر لذلك سنتطرق في دراستنا لهذه الجزئية إلى تعريف البيانات لغة ثم اصطلاحا.

– تعريفها لغة: هي مجموعة المؤشرات و الأفكار المختلفة.

– أما اصطلاحا: فيقصد بها الحقائق أو المشاهدات أو القياسات التي تكون على صورة أرقام أو حروف أو رموز أو أية أشكال خاصة و تصنف فكرة أو موضوع أو حدث أو هدف أو أية حقائق أخرى كمواد خام غير مرئية أو مقومة أو مفسرة أو غير معدة للإستخدام إذا ما قومت و فسرت و نظمت و رتبت (أي عولجت و تم تشغيلها أو معالجتها) ، أصبح لها مضمون ذا معنى يؤثر في الإتجاه ورد الفعل و السلوك ...أي أنها في هذه الحالة تصبح معلومات و على سبيل المثال بيانات داخلية وأخرى خارجية.

– فالبيانات الداخلية: هي بيانات تتداول داخل المؤسسة حيث تسجل وتحلل العمليات الداخلية لها ، و تكون بصفة متكررة و دورية مثل بيانات عن حجم النشاط اليومي.

أما البيانات الخارجية: فهي بيانات تنتشر خارج المؤسسة مثل المتعاملين ، حيث تقوم بوصف منتجات و خدمات المؤسسة و تأخذ أشكال نشر عديدة مثل المجلات ، تقارير مالية ...
و قد تعدت التعريفات حول البيانات منها العربية و الغربية[1].

وقد نص المشرع الجزائري للبيانات في معرض تعريفه للمعطيات ذات الطابع الشخصي وذلك في القانون المتعلق بحماية الأشخاص الطبيعيين في مجال معاجة المعطيات ذات الطابع الشخصي[2] ،

---

[1] أ– التعريفات العربية:

لقد عرف المشرع المصري البيانات: بأنها أي تجميع متميز للبيانات يتوفر فيه عنصر الابتكار أو الترتيب أو أي مجهود شخصي يستحق الحماية و بأية لغة أو رمز و بأي شكل من الأشكال و يكون مخزنا بواسطة حاسب و يمكن استرجاعه بواسطته أيضا.

أما المشرع اللبناني: فقد عرف البيانات و يعتبرها مجموعة أعمال مجموعات معلومات سواء كانت في شكل مقروء أو آلي أو أي شكل أخر تكون منجزة من طرف صاحب حق المؤلف.

ب– التعريفات الغربية:

عرف المشرع الأمريكي البيانات: بأنها تجميع و يعرف التجميع بأنه مصنف يقوم بتجميع أو حشد لبيانات أو مواد موجودة سلفا تم اختبار المناسب منها و تنسيقها و ترتيبها بطريقة تجعل من العمل الناتج عن ذلك عملا مبتكرا من أعمال التأليف.

أما المشرع الياباني فعرفها: بأنها مجموعة من المعلومات مثل المقالات ، الأرقام حيث أن هيكلها و تصنيفها يسمح بأن يتم البحث عنها بواسطة الكمبيوتر.

[2]- القانون رقم 18-07 المؤرخ في 25 رمضان عام 1439 الموافق لـ 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الصادر بالجريدة الرسمية رقم 34 لسنة 2018.

حيث جاء في نص المادة الثالثة من هذا القانون أن المعطيات ذات الطابع الشخصي هي كل معلومة بغض النظر عن دعامتها تكون متعلقة بشخص طبيعي معين تكون المعطيات ذات الطابع الشخصي المتعلقة به موضوع معالجة آلية ، وتتمثل هذه البايانات على وجه الخصوص في رقم التعريف ، أو أحد عناصر الهوية البدنية أو الفيزيولوجية أو الجينية أو البيوميترية أو النفسية أو الإقتصادية أو الثقافية أو الإجتماعية[1].

الفرع الثاني: تعريف المعلومات.

هي من المصطلحات التي تكاد تفقد وزنها الدلالي من كثرة الإستعمال حيث أن جميع التعريفات التي ذكرت في المعلومات تعبر بشكل كبير عن آراء ووجهات نظر أصحابها ، و هذه التعريفات قد تكون مقبولة عند بعض التخصصات و مرفوضة عند البعض الآخر، و قبل التطرق إلى تعريف المعلومات سنتطرق إلى تعريفها لغة ثم اصطلاحا:

– تعريفها لغة: المعلومات من حيث المدلول اللغوي مشتقة من المادة اللغوية "علم" و هي مادة غنية بالكثير من المعاني كالعلم و الإحاطة ببواطن الأمور و الوعي ، و الإدراك واليقين ، الإرشاد ، الإعلام ، الشهرة ، المعرفة ، التعليم ، الدراية ....آخره من المعاني المتصلة بوظائف العقل، information هي المقابل الانجليزي لكلمة معلومات و هذه الكلمة الإنجليزية مشتقة من اللاتينية information التي تعني في الأصل عملية الإتصال أو ما يتم إيصاله أو تلقيه[2].

– أما تعريفها اصطلاحا: فقد عرفت المعلومات بأنها مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح لأن تكون محلا للتبادل و الإتصال أو التفسير و التأويل أو المعالجة و تجزئتها و جمعها أو نقلها بوسائل أو أشكال مختلفة[3].

و قد عرف الأستاذ calte المعلومات بأنها رسالة ما معبر عنها في شكل يجعلها قابلة للنقل أو الإبلاغ للغير[4].

و عرفت أيضا بأنها النقل المجرد لوقائع معينة ثم الحصول عليها من مصادر متعددة.

---

[1]- المادة 03 من القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي ، القانون السابق.

[2]- حتمت قاسم ، مدخل لدراسة المكتبات و علم المعلومات ، القاهرة ، دار غريب ، سنة1990،ص15.

[3]- نائلة محمد فريد فورة ، جرائم الحاسب الآلي الاقتصادية ، منشورات الحلبي ، الطبعة 01، سنة 2005، ص97.

[4]- رشيدة بوكر ، المرجع السابق ، ص 65.

ورغم اجتهاد فقهاء القانون و محاولاتهم لوضع تعريف شامل يتكفل بوضع تعريف محدد للمعلومات إلا أنهم لم يتمكنوا بعد من ذلك[1] ، فقد حاولت بعض التشريعات و ضع تعريف للمعلومات و تعددت فمنها العربية و الغربية[2].

إذا فالمعلومات وفقا لذلك هي النتيجة المبدئية أو الذهنية المترتبة على تشغيل المعطيات و تعليلها أو استقراء دلالتها و استنتاج ما يمكن استنتاجه منها وحدها أو مترافقة مع غيرها أو تفسيرها على نحو يعتري معرفة مستخدمي القرار و يساعدهم في الحكم السديد على الظواهر و المشاهدات أو يسهم في تطوير المعارف النظرية أو التطبيقية[3].

- فالمعلومات تكون قابلة للدمج حيث تضاف معلومة إلى معلومة أخرى ليكونا معا معلومة جديدة تختلف في قيمتها و أهميتها و بالتالي تثار مسألة مقدار الحماية اللازمة لها ، وهو ما يطلق عليه بالنظرية التكاملية للمعلومات.

و هنا يطرح السؤال نفسه ما هو الفرق بين البيانات و المعلومات ؟

الفرع الثالث: الفرق بين البيانات و المعلومات

عادة ما يخلط الباحثين و الدارسين بين البيانات و المعلومات و قد جرت العادة على استخدام كل منهما مكان الآخر ، إلا أنه يوجد فرق بين المصطلحين و يكمن في:

---

[1] - خالد ممدوح ابراهيم ، أمن الجريمة الالكترونية ، الدار الجامعية ، الاسكندرية ،سنة 2008، ص27.

[2] أ- التعريفات العربية:

لقد اجتهدت التشريعات العربية محاولة في ذلك إيجاد تعريف للمعلومات منها: عرف القانون الأردني المعلومات بأنها: البيانات أو النصوص أو الصور أو الأشكال أو الأصوات أو الرموز أو برامج الحاسوب أو قواعد المعلومات التي أنشأت أو أرسلت أو استلمت أو خزنت بوسائل إلكترونية.

في حين عرف قانون البحرين المعلومات بأنها: البيانات و الصور و النصوص و الأصوات و الرموز و برامج الحاسوب و البرمجيات و يمكن أن تكون قواعد البيانات و الكلام.

أيضا عرف قانون الإمارات العربية المتحدة في قانون المعاملات التجارية الالكترونية المعلومات على أنها: بيانات و معلومات الكترونية في شكل نصوص أو رموز أو أصوات أو رسوم أو صور أو برامج الحاسب الآلي أو غيرها.

ب- التعريفات الغربية:

أشار المشرع الفرنسي في قانون الاتصالات السمعية و البصرية إلى المعلومات على أنها صور الوثائق و البيانات و الرسائل من أي نوع.

أما المشرع الأمريكي فقد عرف المعلومات في قانون المعاملات التجارية الالكترونية بأنها: تشمل البيانات و الكلمات و الصور و الأصوات و الرسائل و برامج الكمبيوتر و البرامج الموضوعة في الأقراص المرنة و قواعد البيانات أو ما شابه ذلك.

[3]- محمد محمد شتا ، فكرة الحماية الجنائية لبرنامج الحاسب الآلي ، دار الجامعة الجديدة للنشر 2002 ، ص61.

1- يبدأ أي نظام للمعلومات بالبيانات data و ينتهي بالمعلومات information.

2-البيانات هي حقائق تم تسجيلها ، أو سيتم تسجيلها مستقبلا بشأن أحداث معينة ، وقد تكون هذه الحقائق مستقلة و غير مرتبطة ببعضها و غير محددة العدد ، و تعرف أيضا بالمداخلات أو المادة الخام للمعلومات ، و بمعنى آخر هي مجموعة من الحقائق و المشاهدات التي يتم جمعها من مجتمع إحصائي معين ، و يتم إدخالها إلى الحاسوب لمعالجتها و إخراج النتائج ، ومن أمثلة البيانات الإسم ، السن ، المهنة ....الخ.

3-المعلومات هي ناتج تشغيل البيانات ، أو مجموع النتائج التي تم التحصل عليها من الحاسوب و

بمعنى آخر هي مجموعة البيانات التي جمعت و أعدت بطريقة ما جعلتها قابلة للاستخدام أي مفيدة بالنسبة لمستقبلها أي مستخدمها ، و هي تمثل المخرجات في نظام المعلومات و لها تأثير في اتخاذ القرارات المختلفة.

4-يقوم المستخدم بإدخال البيانات للحاسب ثم بتشغيلها و ترتيبها ، ثم تجري عليها بعض العمليات لتحصل على معلومة ذات قيمة و فائدة ، وكل مجموعة من المعلومات تشكل معرفة ما و هذه هي وظيفتها النهائية ، وتستخدم في تأكيد معلومات سابقة ، أو في إضافة حقائق أو أفكار جديدة لمستقبل أو مستخدم المعلومات.

5- عادة ما تكون البيانات على شكل أرقام و جداول و أشكال بيانية بينما تكون المعلومات على شكل نصوص و عبارات أو صور توضيحية ، و يمكن أن تكون البيانات نصوصا أو أرقام أو صور أو أي شكل آخر.

6-يرى الباحثون أنه من الصعب أن نضع حدا فاصلا بين البيانات و المعلومات ، فما يعتبر معلومات في بعض المراحل ، تعتبر بيانات في المرحلة التي تليها ، و أن المعلومات قد لا تكون في صورة كمية أي يعبر عنها بالأرقام ، وإنما قد تكون معلومة عبر كلمة أي وصفية[1].

* و هنا يمكن القول بأن البيانات و المعلومات مكملات لبعضها البعض ، فلولا البيانات لما تشكلت المعلومات ، فالمعرفة لا تأتي من فراغ ، و إنما من بيانات تم بذل الجهد عليها لتوفيرها و من ثم يبذل

[1]-Word.acc.net / vb/shothread K php ?t 7187

جهدا آخر لمعالجتها ، و تحقيق معلومة تصنع منها قرارات ، و تحقق عرضا منشودا ، و بعبارة أخرى يتضح جليا أن المعلومات هي عبارة عن بيانات و معلومات في حالة سكون و أن البيانات و المعلومات هي المعطيات في حالة معالجة.

المطلب الثاني: خصائص الجرائم الواقعة على المعطيات الرقمية

من البديهي أننا أصبحنا في عصر بات كل شيء فيه خاضعا للعلم والخبرة و المعرفة ، ويبرز ذلك خاصة في المعاهد و الكليات... بوصفها عنصرا أساسيا في الجانب الأمني ، وتوفير مقومات السلام و الإستقرار في البلاد ، لذلك فإن عالم الجريمة ليس معزولا عن التحولات الهامة خاصة الإلكترونية منها التي يشهدها العالم ، بل يمكن القول أن جماعات الجريمة المنظمة تكون السباقة أحيانا في إحداث مثل هذه التحولات من خلال ابتكار أنماط إجرامية تستدعي جهدا كبيرا وتقنيات متقدمة لمواجهتها و درء أخطارها على الإنسانية.

كما تعاني المجتمعات الإلكترونية في الآونة الأخيرة من انتهاكات للحقوق و الخصوصيات الإلكترونية ، وذلك في ظل انتشار الجريمة الإلكترونية أو جريمة التعدي على المعطيات و هذا النوع من التقنيات و التكنولوجيا ، الأمر الذي دفع الدول إلى العمل مليا للحد من هذه الجرائم التي تلحق الضرر بالأفراد من خلال التوعية و الرسائل الوقائية و الأمنية ، ومن خلال ما تقدم يتبين لنا أن الجريمة الماسة بالمعطيات لها عدة خصائص سواء الخاصة بالحاسب الآلي كجهاز أو الأشخاص الذين يقومون بهذه الجرائم لذلك قسمنا هذا المطلب إلى فرعين تناولنا في الفرع الأول سمات و خصائص الجرائم التي تمس المعطيات أما في الفرع الثاني فتناولنا تصنيف مجرمي التعدي على المعطيات.

الفرع الأول: سمات الجرائم الماسة بالمعطيات الرقمية.

إن الجرائم التي تمس المعطيات تعد من الجرائم المعلوماتية فهي ترتبط بها و تقوم عليها و قد أدى اتساع هذه الجرائم إلى إلحاق ضرر بالمجتمع ، كما أن ازدياد وازدهار حجم تقنية المعلومات في القطاعات المختلفة أدى إلى إعطاء الجرائم المعلوماتية لونا أو طابعا قانونيا خاصا يتميز عن غيرها من الجرائم سواء التقليدية منها أو المستحدثة بمجموعة من الخصائص و لعل أبرز خصائص الجرائم التي تمس المعطيات الإلكترونية ما يلي:

1- جريمة تمس معطيات الحاسب الآلي:

أ- الحاسب الآلي أداة لارتكاب هذه الجرائم: تتميز الجرائم الماسة بالمعطيات أو المعلومات بخاصية منفردة تميزها عن الجرائم التقليدية ، و باعتبار أن الحاسب الآلي هو الوسيلة الرئيسية الأكثر استخداما في الجريمة[1] و من جهة أخرى يتم الإعتداء على الحواسب الأخرى و الدخول إلى البرامج و سرقتها أو العبث ببيانات الحاسوب أو إتلافها و الإطلاع على المعلومات المخزنة[2] ، لذلك اشترط الفقهاء وجود شبكة الإنترنت حتى يتم الربط بين هذه الحواسيب ، وقد شهد العالم وسائل إلكترونية غير الحاسب الآلي كالهواتف النقالة الذكية التي استطاع البعض استغلالها في التعدي على المعلومات الخاصة.

ب- أن يقع الإعتداء على الحاسب الآلي أو ملحقاته: وهنا يكون الهدف من ارتكاب تلك الأفعال عبر شبكة الإنترنت هو الإعتداء على معطيات الحاسب الآلي ، كالمعلومات و البيانات المخزنة في الذاكرة و هذه المعطيات ليست ذات طبيعة مادية منقولة ملموسة ، حتى نجزم بخضوعها لنصوص قانون العقوبات التقليدي، و هي أقرب إلى الكيانات الذهنية أو المعنوية التي تم إدخالها إلى الحاسب الآلي[3] ، فالغالب يكون الهدف هو تخزين تلك الأجهزة نهائيا أو على الأقل تعطيلها لأطول فترة ممكنة ومعظم تلك الجرائم تتم بواسطة استخدام الفيروسات[4].

2- جرائم ترتكب على شبكة الإنترنت:

لم يكن هناك قلق مع بدايات شبكة الإنترنت من جرائم يمكن أن ترتكب عليها أو بواسطتها ليس لأنها آمنة في تصميمها و بناءها ، بل لمحدودية مستخدميها ، و لكون الإنترنت عبارة عن شبكة كبيرة تربط بين شبكات منفردة متواجدة عبر مختلف دول العالم للملايين من أجهزة الكمبيوتر التي يمكنها الإتصال بنفس المواقع في اللحظة ذاتها و سرعة فائقة لكم هائل من المعلومات والخدمات ، لذلك لجأ إليها البعض لتحقيق أهداف و صارت شبكة الإنترنت مجالا للإعتداءات الإجرامية و التي تتصور

---

[1]- منير محمد الجنبهي ، ممدوح الجنبيهي ، جرائم الانترنت و الحاسب الآلي ووسائل مكافحتها ، دار الفكر الجامعي ، الإسكندرية ، دون طبعة ، 2006، ص25.

[2]-محمود أحمد عبابنة ، جرائم الحاسوب و أبعادها الدولية ، دار الثقافة للنشر و التوزيع الأردن ، 2009، ص36.

[3]-محمود أحمد عبابنة ، المرجع نفسه ، ص39.

[4]- أمير فرج يوسف الجريمة الالكترونية و المعلوماتية و الجهود الدولية و المحلية للمكافحة ، الطبعة 01مكتبة الوفاء القانونية ، الإسكندرية ، سنة 2011،ص 20.

فيها أغلب صور جرائم الأموال[1] ، كالإعتداء على البنوك الشركات ....الخ.

3-جرائم عابرة للحدود:

مع التطور الذي شهدته تكنولوجيا الإتصالات ظهرت شبكة الإنترنت التي ألغت كل الحدود الجغرافية ما جعلها تكتسب طبيعة دولية كاختراق الشيفرات البنكية ، تبييض الأموال و سرقتها ، تزوير وإتلاف المعلومات و البيانات ، تخريب أجهزة الحاسب الآلي عند الضرورة ، وهنا يطرح الإشكال حول تحديد الدولة صاحبة الإختصاص القضائي وماهية القوانين الواجبة التطبيق.

4-جريمة يصعب إكتشافها و إثباتها:

و من بين هذه الخصائص صعوبة إكتشافها و صعوبة إثباتها و السبب في ذلك أنها لا تترك أثرا

خارجيا ، و إذا اكتشفت يكون ذلك بمحض الصدفة ، ومما يزيد الأمر تعقيدا أن هؤلاء القراصنة لا يهاجمون من أجهزة الحاسوب الخاصة بهم، و إنما يدخلون إلى شبكات بعيدة عنهم و يهاجمون من خلالها[2]، فالجاني يتمتع بقدرات فنية تمكنه من جريمة بدقة، ومثال ذلك إرسال الفيروسات المدمرة و سرقة الأموال و البيانات الخاصة أو إتلافها و التجسس و سرقة المكالمات و غير ذلك من الجرائم[3]، كما له القدرة على أن يمنع الوصول للدليل بشتى الوسائل فيقوم بإدخال برنامج أو وضع كلمات سرية ورموز تعوق الوصول إلى الدليل و يلجأ لتشفير التعليمات لمنع إيجاد أي دليل يدينه.

وقد يكون سبب صعوبة إكتشافها و إثباتها راجع إلى:

أ- خفاء الجريمة: تتسم الجرائم الماسة بالمعطيات و البيانات بميزة الخفاء على عكس الجرائم التقليدية و التي عادة تكون علنية ، فالمجني عليه لا يلاحظها رغم أنها قد تقع أثناء و جوده على الشبكة لأن الجاني يتمتع بقدرات فنية تمكنه من الجريمة و بدقة عالية[4]، كإرسال الفيروسات المدمرة و سرقة الأموال و البيانات الخاصة أو إتلافها و التجسس و سرقة المكالمات و غيرها من الجرائم.

---

[1]-محمد أمين الشوابكة ، جرائم الحاسوب و الانترنت ، الجريمة المعلوماتية ، دار الثقافة للنشر و التوزيع ، عمان ، الطبعة 01، سنة 2007، ص26.

[2]- محمد عبيد الكعبي ، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الأنترنت ، دار النهضة العربية ، القاهرة ، ص32.

[3]- محمود أحمد عبانية ، المجرع السابق ،ص37.

[4]- محمد عبيد الكعبي ، المرجع نفسه ، ص32.

ب-سرعة محو الآثار و الأدلة: فجريمة المعطيات تقع خارج إطار الواقع المادي الملموس في بيئة إلكترونية يتم فيها نقل المعلومات و تداولها بطريقة غير مرئية علاوة على صعوبة الإحتفاظ الفني بآثارها إن وجدت[1] ، فهي معلومات و بيانات وأرقام تتغير بسرعة فائقة و لا تترك أي أثر أو دليل

على ذلك و هنا تأتي صعوبة الكشف عن هذه الجريمة.

5-جريمة ناعمة:

من المتعارف عليه في الجرائم التقليدية أنه يستعمل فيها أدوات وسبل لتحقيق النتيجة الإجرامية، كجريمة السرقة مثلا فإن الأمر يتطلب كسر، و خلع، أو حتى الحرق ....الخ و كذلك جرائم الإرهاب أو جرائم المخدرات ...بينما في الجرائم الماسة بالمعطيات فالأمر مختلف تماما و هذا ما يميز هذا النوع من الجرائم و يجعلها من الجرائم الناعمة، لأنها لا تتطلب عنفا لسرقة المعلومات و البيانات أو نقلها من حاسب لآخر أو معرفة الشيفرات الخاصة بالبنوك و السطو على أرصدتها، فرغم غياب العنف إلا أن النتيجة المراد تحقيقها تحققت و هذا سبب تسميتها بالجريمة الناعمة.

6- نقص الخبرة لدى الأجهزة الأمنية و القضائية:

تحتاج جرائم المعطيات أو المعلومات إلى خبرة فنية عالية يصعب على المحقق التقليدي التعامل معها ، و نظرا لما تتطلبه هذه الجرائم من تقنية لارتكابها فهي تتطلب لاكتشافها و البحث عنها كفاءات عالية ، لذلك يجد ضباط الشرطة القضائية أنفسهم غير قادرين على التعامل بالوسائل الإستدلالية و الإجراءات التقليدية مع هذه النوعية من الجرائم فضلا عن صعوبة إجراء التحريات السرية ، و تتبع مسار العمليات الإلكترونية العابرة للحدود[2]، كما أن رجال الشرطة قد لا يتعاملون بمهارة و احترافية مع الدليل الإلكتروني المستمد من الجريمة و إن وجد فقد يتلفونه من غير قصد.

لذلك وجب عقد دورات تدريبية مشتركة بين رجال القضاء من النيابة العامة و رجال الشرطة و خبراء فنيين مجتمعين معا ، و ذلك بغرض معرفة أكبر قدر ممكن من المعلومات حول الإختراقات و قرصنة المعلومات و البيانات ...الخ حتى يتم الوصول إلى أنسب الطرق القانونية لمكافحة هذا النوع من الجرائم مع تعزيز التعاون بين الجهات القضائية الوطنية و الدولية.

[1]- خالد ممدوح ابراهيم ، المرجع السابق ، ص 45،46.
[2]- خالد ممدوح ابراهيم ، المرجع نفسه ، ص 45،46.

7- مرتكب الجريمة هو شخص ذو خبرة فائقة:

لاستخدام الحاسب الآلي و لإرتكاب جريمة على شبكة الإنترنت لابد أن يكون مستخدم هذا الحاسوب الآلي على دراية و خبرة كبيرة في مجال استخدامه و التي تمكنه من تنفيذ جريمته و العمل على عدم اكتشافها ، فهذا الشخص يتمتع بذكاء ، إذ يمكنه التغلب على كثير من العقابات التي تواجهه أثناء ارتكابه الجريمة ، حيث يمتلك هذا المجرم من المهارات ما يؤهله للقيام بتعديل و تطوير في الأنظمة الأمنية حتى لا يستطيع أحد أن يلاحقه و يتبع أعماله الإجرامية من خلال الشبكات أو داخل أجهزة الحواسيب فالمجرم المعلوماتي هو مجرم يعتمد على الذكاء[1]، فهو شخص ذو مهارات فنية عالية متخصص في الإجرام المعلوماتي و يستغل مداركه و مهاراته في إختراق الشبكات و كسر كلمات المرور أو الشيفرات و يسبح في عالم الشبكات ليحصل على كل غالي و ثمين من البيانات و المعلومات الموجودة في أجهزة الحواسيب و من خلال الشبكات يستطيع استخدام خبراته في الإختراقات و تغيير المعلومات و له القدرة على تغيير البرامج أو تحويل الأموال، لذلك نجد أن معظم من يرتكبون تلك الجرائم هم الخبراء في مجال الحاسب الآلي أو المعلوماتي و أن الشرطة تبحث أولا عن خبراء الكمبيوتر عند ارتكاب الجرائم المعلوماتية.

8- توفر وسائل تقنية تعرقل الوصول للدليل:

فالمجرم المعلوماتي عادة ما يتميز بذكاء خارق على إختراق المواقع و قد يرتكب عدة جرائم كسرقة بيانات أو تغييرها أو اختلاسات فهناك أدلة الكترونية و هي على الغالب الأعم هي أدلة دقيقة جدا، و حتى لا يتمكن شخص آخر من الوصول إلى هذه الأدلة التي قد تبين المجرم ، فيقوم هذا الأخير بدوره بمنع الوصول للدليل بشتى الوسائل فيقوم بإرسال برامج أو وضع كلمات سرية و رموز أو يلجأ لتشفير التعليمات لمنع الوصول إلى أي دليل يدينه.

الفرع الثاني: تصنيف المجرمين المتعديين على المعطيات الرقمية.

ظهرت و منذ زمن طويل العصابات في الطرق و المدن و كانت تهدف هذه الأخير إلى جرائم تقليدية كالسرقة ، و الإختطاف و التخريب ....الخ ، وكانت الشرطة تتصدى لهذا النوع من الإجرام إلى أن ظهر الكمبيوتر و الإنترنت، و بدأت هذه الوسائل تستغل في شقها السلبي و ارتكبت بواسطتها عدة

[1]- أمير فرج يوسف ، الجرائم المعلوماتية على شبكة الإنترنت ، دار المطبوعات الجامعية ، الإسكندرية ، سنة2008، ص32.

جرائم و التي تتزايد كلما زاد استخدام الأشخاص لأجهزة الحاسب الآلي، ومن بين هذه الجرائم السرقة ،الإبتزاز...الخ.

فهؤلاء يستهدفون اختراق أجهزة الحاسوب أو البريد الإلكتروني أو المواقع الإلكترونية على شبكة الإنترنت و خصوصا المواقع الإلكترونية التي تكون للشركات المعروفة مثل شركة مايكروسوفت و غيرها من الشركات العالمية و التي غالبا ما تكون مستهدفة من قبل شركات منافسة لها، و التي قد تتسبب في خسارة الكثير من الأموال، وقد تستهدف المواقع الإلكترونية للبنوك بهدف الدخول إلى حساب أحد العملاء فيه و سرقة الأموال.

فهذه الجرائم ليس بالضرورة أن يقوم بها المجرم و الضحية داخل بلد واحد فقد يكون هناك بعدا جغرافيا في هذا النوع من الإجرام ، فيكون الفاعل في بلد و النتيجة في بلد آخر أو قارة أخرى هذا ما يطلق عليه بالمجرم التقني أو بالمجرم المعلوماتي لذلك عرف البعض **المجرم المعلوماتي** بأنه كل شخص يأتي أفعالا إرادية تشكل سلوكا إيجابيا أو سلبيا باستخدام تقنية المعلوماتية لإحداث نموذج إجرامي بالإعتداء على حق أو مصلحة ، وسمات المجرم المعلوماتي تشبه في كثير من الأحيان سمات المجرمين ذوي الياقات البيضاء[1].

و عرف البعض الآخر المجرم المعلوماتي في الجريمة المعلوماتية بأنه عندما لا نكون بصدد مجرم عادي بل أمام مجرم ذي مهارات تقنية و ذو علم بالتكنيك المستخدم في نظام الحسابات الآلية ، فشخصية المجرم المعلوماتي سواء أكان طبيعيا أو معنويا و آلية ارتكاب الجريمة تجعل منه شخصا يتسم بسيمات خاصة تضاف إلى الصفات الأخرى التي يجب أن تتوافر في المجرم العادي[2].

ومن خلال ما تقدم فقد أطلق البعض على هؤلاء بالهاكرز أو الكراكرز لذلك سنتطرق إلى تعريف الهاكرز:

1-تعريف الهاكرز: تسمى باللغة الانجليزية hacking و تسمى باللغة العربية عملية التجسس أو إختراق أو قرصنة ، حيث يقوم أحد الأشخاص غير المصرح لهم بالدخول إلى نظام التشغيل في جهاز الحاسوب بطريقة غير شرعية و لأغراض غير سوية مثل التجسس أو السرقة أو التخريب حيث يتاح

[1] عبد الفتاح يومي حجازي ، التزوير في جرائم الكمبيوتر و الأنترنت ، دار الكتب القانونية ، مصر ، سنة 2008، ص105.
www.miishawi.com- و قد تم الاطلاع على الموقع بتاريخ 13.05.2016
[2]- محمد على سالم، حسون عبيد، هجيج الجريمة المعلوماتية ، مجلة جامعة بابل ، العلوم السياسية ، العدد 14، العراق ،سنة 2008، ص88

للشخص المتجسس الهاكر أن ينتقل أو يسمح أو يضيف ملفات أو برامج كما أنه بإمكانه أن يتحكم في نظام التشغيل فيقوم بإصدار أمر بالطباعة أو التصوير أو التخريب[1].

و صنف هؤلاء المجرمون إلى فئات مختلفة نذكر منها:

أ-فئة الهاكرز المخترقون أو المتطفلون:

و يقصد بهم الشباب البالغ و هم المفتونون بالمعلومات و الحاسبات الآلية و بعضهم يطلق عليهم نوابغ المعلوماتية[2]، وأغلب هذه الطائفة هم من الطلبة و الشباب حاصلين على معرفة في مجال التقنية المعلوماتية ، و غالبا ما يتقيد هؤلاء بقواعد السلوك و الشرف دون أن تكون لهم نية الإضرار بالمجني عليهم[3]، و الباعث الأساسي لهذه الطائفة هو الإستمتاع و المزاح بإستخدام هذه التقنية لإثبات مهاراتهم و قدراتهم على إختراق شبكات الحاسب الآلي و بجهدهم الذاتي و بدون الإستعانة بأية تعليمات من أية مصادر أخرى ، بالإضافة إلى اثبات قدراتهم في اكتشاف و إظهار مواطن الضعف في الأنظمة المعلوماتية دون إلحاق ضرر بها ، و قد تكون لديهم الرغبة في المغامرة و التحري و الرغبة في الإكتشاف[4].

2- الكراكرز أو المحترفون:

فهؤلاء يعملون على اكتشاف الثغرات من أجل إختراق الأنظمة و التطبيقات[5]و هذه الفئة تتراوح أعمارهم بين 25-45 سنة و يكونوا ممن يحملون درجات جامعية عليا تخصص كمبيوتر و معلوماتية و يعملون محللي نظم و مبرمجين و هم على دراية عالية ببرامج التشغيل و معرفة عميقة بالخبايا و الثغرات الموجودة بها ، و غالبا ما تنتشر هذه الفئة بأمريكا و أوروبا ، وقد بدأت تنتشر كذلك في المنطقة العربية[6].

---

[1]- ياسر رجب التهامي ، خدع الهاكرز ، دون طبعة ، سنة2008، 03.

[2]- عبد الفتاح بيومي حجازي ، مبادي الإجراءات الجنائية في جرائم الكمبيوتر ، و الأنترنت ، دار الفكر الجامعي ، الإسكندرية ، الطبعة 01، سنة 2006، ص46.

[3]- أنيس المومني ، قانون العقوبات في مواجهة مخاطر الأنترنت ، رسالة ماجستير في القانون الجنائي ، جامعة عنابة ، الجزائر ، سنة 2003، ص13.

[4]- محمد دباس الحميد، ماركو ابراهيم نينو ، حماية أنظمة المعلوماتية ، دار حامد للنشر و التوزيع ،عمان، الطبعة 01، سنة 2007، ص37.

[5]- خالد بن نواف الحربي ، الأمن و الحماية في الأنترنت ، المملكة العربية السعودية ، ص04.

[6]- ياسر رجب التهامي ، المرجع نفسه ، ص04

تعتبر هذه الفئة الخطيرة من بين مجرمي التقنية حيث تهدف إلى تحقيق الكسب لهم و للجهات التي كلفتهم بالأساس إلى تحقيق الكسب المادي لهم أو الجهات التي كلفتهم وسخرتهم لارتكاب جرائم التعدي على المعطيات[1] ، كما تهدف إعتداءات بعضهم إلى تحقيق أغراض سياسية و التعبير عن موقف فكري أو نظري أو فلسفي و تعد هذه الفئة أخطر من الفئة الأولى فهذه الأخيرة يمكن أن نلمس لهم حسن النية على عكس الفئة الثانية التي أثبت اعتداءاتها ميولها إلى التخريب و الإجرام.

3- فئة الحاقدون:

تعتبر هذه الفئة الأخطر على الإطلاق فعادة التأثر و الإنتقام هو الطابع الغالب على تصرفاتهم ، كما أن أعضاء هذه الفئة لا تتسم بالمعرفة التقنية الإحترافية ، ويغلب على أنشطتهم من الناحية التقنية إستخدام الفيروسات و البرامج وتعطيل النظام أو الموقع المستهدف و إتلاف كل أو بعض معطيات الأنظمة الخاصة بالحاسب الآلي إن كان من مواقع الإنترنت.

و ليس هناك ضوابط محددة بشأن أعمارهم ، كما لا تتوفر عناصر التفاعل بين أعضاء هذه الطائفة و لا يتفاخرون بأنشطتهم بل يعمدون إلى إخفائها ، وهم الطائفة الأسهل من حيث كشف الأنشطة التي قاموا بارتكابها لتوفر ظروف و عوامل تساعد على ذلك[2]، و من جهة ثانية فإن هذه الفئة لا يسعون إلى إثبات قدراتهم التقنية و الفنية و لا يبغون تحقيق مكاسب مادية أو سياسية و لا يفاخرون أو يجاهرون بأنشطتهم بل يعملون إلى إخفاء و إنكار أفعالهم[3].

وبعد دراسة تصنيف المجرمين المتعدين على المعطيات إرتأينا دراسة الدوافع التي أدت إلى اختراق وقرصنة المعطيات المتواجدة في الحاسب الآلي:

دوافع المجرمين المتعدين على المعطيات:

مما لا شك فيه أن السلوك الإنساني أيا كان له ما يفسره ، و ما الذي بعث على ارتكابه ، وهو الذي يطلق عله الدوافع إلا أن صورة الدوافع فكرة تشوبها بعض الغموض و عدم إتفاق من جانب الفقه و لذلك تعددت الإتجاهات و اختلفت فمنهم من أطلق عليه الغاية و منهم النية ، ومنهم الغرض و منهم الباعث.

[1]- جعفر حسن جاسم الطائفي ،جرائم تكنولوجيا المعلومات ، درا البداية ، عمان ، سنة 2007، ص162.
[2]- نسرين عبد الحميد نبيه ، المرجع السابق ،ص42
[3]- أيمن عبد الحفيظ ، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية ، سنة 2005، ص34.

ومهما يكن الأمر ، فإن دراسة دوافع هذا النمط من الإجرام قد تكون لها فائدة مزدوجة فهي:

* أولا قد تساعدنا في إيجاد الحلول المناسبة لمقاومتها و التغلب عليها.

* و ثانيا المساهمة في تحديد التكييف القانوني الذي قد تضفيه عليها، لذلك قد تكون هذه الدوافع شخصية و دوافع خارجية.

أ/الدوافع الشخصية:

بعد دراسات عديدة توصل العلماء و الباحثون إلى أن هناك العديد من الدوافع الشخصية التي يرى فيها مرتكبوا الجريمة أسبابا منطقية لتبرير أفعالهم و أنها هي التي تقوم بتحفيزهم على إرتكاب مثل تلك الأفعال و الإعتداءات غير المشروعة في الفضاء السيبراني[1]، و يمكن رد الدوافع الشخصية لدى المجرم المعلوماتي إلى عدة دوافع منها المالية و أخرى ذهنية:

1-الدوافع المالية:

يعتبر السعي إلى تحقيق الربح في المرتبة الأولى ويمثل في الحقيقة غاية الفاعل ومن بين أكثر الدوافع تحريكا للجناة للتعدي على المعطيات المتواجدة في الحاسوب حيث يقوم مرتكبوا هذه الجريمة ذوي الكفاءة الفنية العليا ، بما لديهم من خبرة في المجال التكنولوجي بتوجيه هذه الإمكانات نحو المؤسسات المالية لمحاولة تحقيق المكاسب المالية إما بسرقة تلك الأموال أو بتحويلها لحسابه الشخصي داخل البنك ، فيستطيع المجرمون بمجرد دخولهم إلى أنظمة البنوك معرفة أرقام الحاسب وسرقتها أو تحويلها ، ويكون المكسب المادي أيضا هدفا لمن هم أقل في المعرفة التقنية و قد يكونون غير مؤهلين على الإطلاق في المجال المعلوماتي و لا يمكنهم الدخول إلى أنظمة تلك الحواسب و يكون أسلوب ارتكابهم للجرائم أسلوب محدد في مجال معين لا يحتاج إلى خبرة و مهارة[2].

و وفقا للدراسات فإن القطاع المالي يعد أكثر القطاعات استهدافا من قبل الجناة و يرجع ذلك إلى أن

[1]- لقد عرف الفضاء السيبراني بأنه: مجال شامل يتكون من شبكة محبكة تضم المنشآت التكنولوجية للإعلام ، بما فيها الانترنت ، شبكات الاتصال السلكي و اللاسلكي ، أنظمة افعلام الآلي ، دارات مدمجة و معالجات دقيقة و يضم المعلومة الرقمية المنقولة و كذا متعملي الخدمات على الخط . وهناك من اعتبره مجال شامل على مستوى البيئة الرقمية يتشكل من شبكات مرتبطة بينيا بالمنشآت و تكنزلوجيا الإعلام بما فيها الانترنت ، شبكة الإتصال ، أنظمة الحواسيب و الدارات المدمجة و كذا وسائل الرقابة .و لمزيد من التفصيل أنظر : بلفريد لطفي لمين ، الفضاء السبراني : هندسة و فواعل مقال منشور بالمجلة الجزئرية للدراسات السياسية ، العدد 05، سنة 2016 ، ص 148.

[2]-أيمن عبد الحفيظ ، المرجع السابق ، ص18.

هذه البنوك تعتمد و بشكل أساسي على أنظمة التمويل الإلكتروني المستخدمة في الأيدي الخاطئة وبالتالي فإن ملايين الدولارات يمكن أن تنقل في ثواني معدودة إلى الجاني دون أن يترك أي دليل ضده[1].

وعلى سبيل المثال شركات التأمين التي تعد من القطاعات المستهدفة بعمليات النصب و الإحتيال ، كما أنها تقوم بدور الجاني في بعض الأحيان كشركة تأمين (اكوتيى فندنغ) بمدينة لوس أنجلس الأمريكية التي تمكن مستخدموها و بمساعدة نظامها المعلوماتي من خلق عملاء وهمين مؤمن عليهم ، حيث تمكنت هذه الشركة من بيع 46 تأشيرة تأمين إلى شركات مناظرة في إطار اتفاقيات تقنية التأمين[2].

فيعمد الجاني رغبة منه في تحقيق الثراء و الكسب المادي إلى التلاعب بأنظمة المعالجة الآلية للمؤسسات المالية و خاصة إذا كان أحد موظفيها ، أو اخترق نظم المعالجة الآلية لها من خلال اكتشافه لفجواتها الأمنية فيعمل على استغلالها و برمجتها لتحويل مبالغ مالية لحسابه أو لحساب شركائه أو لحساب من يعمل لحسابهم إن كان خارج المؤسسة ، و يمكن الحصول على المكاسب المالية من خلال المساومة على البرامج أو المعلومات المتحصل عليها عن طريق الإختلاس من جهاز الحاسوب[3].

و تجدر الإشارة إلى أنه في حال نجاح المجرم في ارتكاب جريمته عبر الإنترنت فإن ذلك قد يدر عليه أرباحا هائلة في زمن قياسي ، و يمكن أن نوضح مدى الأرباح المادية التي يحققها المجرم نتيجة لإقترافه هذا النوع من الإجرام من خلال ما يردده أحد هؤلاء المجرمين المحترفين في سجن كاليفورنيا بقوله : "لقد سرقت أكثر من نصف مليار دولار بفضل أجهزة حاسوب جهاز الضرائب في الولايات المتحدة الأمريكية و بإمكاني أن أكرر ذلك في أي وقت لقد كان شيئا سهلا ، فأنا أعرف أسلوب عمل جهاز الحاسوب للضرائب ، وقد وجدت ثغرات كثيرة في نظامه يمكن أن تمدني بمبالغ طائلة لو لم يكن سو الحظ قد صادفني"[4].

وكذلك ما حدث في فرنسا سنة 1986 حيث كان العائد من ارتكاب جريمة سرقة مع حمل السلاح هو

---

[1]-محمود أحمد عبابنة ، المرجع السابق ، 24.

[2]- محمود أحمد عبابنة ، المرجع نفسه ، ص 25.

[3]- نهلا عبد القادر المومني ، الجرائم المعلوماتية ، دار الثقافة للنشر و التوزيع ، الطبعة 01، عمان ، سنة 2008، ص90.

[4]- نهلا عبد القادر المومني ، المرجع نفسه، ص91.

70000 فرنك فرنسي في حين أن جريمة الغش في مجال المعالجة الآلية للمعلومات حصل منها الجاني على 670.000 فرنك فرنسي[1].

2-الدوافع الذهنية:

تعد الصورة الذهنية لمرتكبي الجرائم الماسة بالمعطيات أو جرائم الحاسوب و الإنترنت هي صورة البطل و الذكي لذي يستحق الإعجاب لا صورة المجرم الذي تستوجب محاكمته فمرتكبوا هذه الجرائم يسعون إلى إظهار تفوقهم و مستوى ثقتهم ببراعتهم لدرجة أنه إزاء أي ظهور لأي تقنية مستحدثة فإن مرتكبي هذه الجرائم لديهم شغف الآلة فيحاولون إيجاد وسيلة إلى تحطيمها أو التفوق عليها[2] ، لذلك يرى قراصنة الكمبوتر أن الحصول على المعطيات يجب أن لا يكون عليه قيد ، فالجاني يكرس كل جهده في تعلم كيفية إختراق المواقع الممنوعة ، وغالبا مايكون القراصنة مجموعات يكون الهدف منها التعاون و تبادل المعلومات و تقاسم البرامج و الأخبار و يفضل هؤلاء القراصنة أن يكونوا مجهولين حتى يتمكنوا من الإستمرار في التواجد لأطول فترة ممكنة[3]، في الوقت الذي يزداد فيه الاهتمام بأمن الحاسب الآلي ، عن طريق تطوير طرق جديدة و صعبة لإختراقه ، كبرمجيات التشفير التي تمكن مستقبلها وحده من فهمها ، و كمثال على ذلك وزارة الدفاع الامريكية البنتاغون التي تقوم يتغيير أنظمة الترميز للبيانات المستخدمة يوميا ، حتى أن بعض المعلومات الحساسة تغير كل ساعة أنظمة ترميزها ، و هذا مما لا شك فيه يدل على قدر عال من التقنية و النظام لذلك نرى أصحاب الشغف الإلكتروني يتسابقون لخرق هذه الأنظمة و إظهار تفوقهم عليها و الدليل على ذلك قيام أحد الهواة في أوروبا بحل شفرة أحد مراكز المعلومات في البناتاغون و تمكنه من العبث ببيانات هذا المركز[4].

وقد ذهب البعض إلى أنه قد تكون الدوافع لارتكاب الجريمة الماسة بالمعطيات الرغبة في تحدي و قهر النظام و التفوق على تعقيد وسائل التقنية ، فإختراق الأنظمة الإكترونية و كسر الحواجز الأمنية المحيطة بهذه الأنظمة قد يشكل متعة كبيرة لمرتكبها و تسلية تغطي أوقات فراغه ، إذ يميل المجرم هنا إلى إظهار تفوقه على وسائل التكنولوجيا ويعتبر ذلك من دوافع التحدي و إثبات المقدرة[5].

---

[1]-Rosephillppe les criminalities information que sais-je ? les édition .PUF.1988.P 490.

[2]- نسرين عبد الحميد نبيه ، المرجع السابق ، ص44.

[3]- محمد أمين الرومي ، جرائم الكمبيوتر و الانترنت ، دار المطبوعات الجامعية ، الاسكندرية ، سنة 2003 ، ص24.

[4]- محمد أحمد عبابنة ، المرجع السابق ، ص25.

[5]- رشيدة بوكر، المرجع السابق، ص95.

ب/الدوافع الخارجية:

لإرتكاب بعض الجرائم الماسة بالمعطيات فإن الإنسان يتأثر بمؤثرات خارجية ، نتيجة لوجوده في بيئة المعالجة الآلية للمعطيات ، أو المعلومات هذا و تعد المؤثرات التي تدفع بالفرد إلى اقتراف مثل هذا السلوك سواء دوافع سياسية ، أو دوافع الإنتقام.

1- دوافع سياسية:

تعد الدوافع السياسية من أبرز بواعث المحاولات الدولية لاختراق شبكات حكومية في مختلف دول العالم ، كما أن الأفراد قد يتمكنون من إختراق الأجهزة الأمنية الحكومية لذلك أصبحت شبكة الإنترنت مجالا خصبا لنشر أفكار العديد من الأفراد و المجتمعات ووسيلة لترويج الأخبار و أمور أخرى قد تحمل في طياتها مساسا بأمن الدولة أو نظام الحكم أو بالرموز الدولية والإساءة لهم بالذم و التشهير....[1].

وقد انتشرت الكثير من المواقع غير المرغوب فيها على شبكة الإنترنت لعدة دوافع و من بين هذه الدوافع ما يكون موجها ضد سياسة دولة محددة أو ضد عقيدة أو مذهب معين ، وهي تهدف في المقام الأول إلى تشويه صورة الدولة أو المعتقد المستهدف و يتم غالبا في المواقع السياسية المعادية تلفيق الأخبار و المعلومات و لو زورا أو حتى الإستناد إلى جزء بسيط جدا من الحقيقة و من ثم نسج الأخبار الملفقة حولها ، و غالبا مايعمد أصحاب تلك المواقع إلى إنشاء قاعدة بيانات بعناوين أشخاص يحصلون عليها من الشركات التي تتبع قواعد البيانات تلك ، أو بطرق أخرى ومن ثم يضيفون تلك العناوين إلى قائمتهم البريدية و يبدؤون في إغراق تلك العناوين بمنشوراتهم ، وهم عادة يلجؤون إلى هذه الطريقة رغبة في تجاوز الحجب الذي قد يتعرضون له و لإيصال أصواتهم إلى أكبر قدر ممكن[2].

و من أوجه الصراع الإلكتروني بدوافع سياسية ، ما جرى بعد حوالي أسبوعين من انطلاق الإنتفاضة في نهاية سنة 2000م ، و بعد أن تمكن حزب الله اللبناني من إختطاف أربعة من جنود قوات

[1]- تركي بن عبد الرحمن الموشير ، بناء نموذج أمني لمكافحة الجرائم المعلوماتية و قياس فاعليته ، أطروحة دكتوراه ، كلية الدراسات العليا بجامعة نايف العربية للعلوم الأمنية ، الرياض ، سنة 2009، ص39.

[2]- أيمن عبد الحفيظ، المرجع السابق، ص20.

الإحتلال في جنوب لبنان بادر الإسرائيليون إلى مهاجمة موقع حزب الله على الإنترنت التالي:http:/www.hizbaallah.org و نجحوا في تعطيله ، وتم لهم ذلك بإستخدام برنامج ICQ الإسرائيلي ، و برنامج آخر صمم خصيصا لهذا ، ويعد هذا الهجوم من أصعبها لأنه يعتمد على توجيه طلبات إلى الموقع بكميات هائلة ، بحيث لا يتمكن معها من التلبية ، فيتوفق تلقائيا عن العمل ، و لكن حزب كان جاهزا لمثل هذا الهجوم ، فأقاموا موقعا جديدا على العنوان الآتي:HTTP:/WWW.HIZA ALLAH.ORQ.

وأعلنت رسالة نشرت بالإنجليزية في موقع خاص بجمعيات الهاكر في 12 تشرين الأول من عام 2000 الطريقة التي بها العملية ، وتضمنت الرسالة إعلانا يشير إلى نجاحهم في إيقاف الموقع عن العمل بعد تمرير رسالة عبر البرنامج ICQ تحمل الكلمات : " يمكنك مساعدة أصدقائك الإسرائليين من منزلك لتعطيل موقع حزب الله و بالنقر على أمر RUN من قائمة START و إدخال الأمر التالي 2600 T.W 000.000.000 PING مع وضع عنوان IP لموقع حزب الله بدل الأصفار فإذا نفذه عدد كبير من الأشخاص ، ستتمكن من تعطيل الموقع".

كذلك شهدت الصراعات السياسية اليوم و خاصة في السنوات القليلة الماضية محاولات دولية لاختراق شبكات حكومية في مختلف دول العلم ، فالتجسس عبر الإنترنت يتم يوميا من قبل أجهزة المخابرات حتى الأفراد العاديين قد يتمكنوا من اختراق الأجهزة الأمنية الحكومية و خير مثال على ذلك عندما استطاع ثلاثة إخوة من قرية كفر قاسم الفلسطينية إختراق شبكة المخابرات الإسرائيلية (الموساد) و جهاز الأمن الاسرائيلي (شين بت) و استطاعوا أن يتنصتوا على عدد من المكالمات و الحصول على بعض المعلومات و تقديمها إلى السلطات الفلسطينية علما أن الأشقاء الثلاثة من فاقدي نعمة البصر[1].

2-دوافع الإنتقام:

يعد هذا الدافع من أخطر الدوافع التي يمكن أن تدفع الشخص إلى ارتكاب الجريمة ذلك أنه غالبا ما يصدر عن شخص يملك معلومات كبيرة عن المؤسسة أو الشركة التي يعمل بها و غالبا ما يكون هذا الدافع لأسباب تتعلق بالحياة المهنية ، ومن ذلك الشعور بالحرمان من بعض الحقوق المهنية أو الطرد

[1]- محمود أحمد عبابنة ، المرجع السابق ، ص26و لمزيد من التفصيل أنظر فادي سالم ، الوجه الإلكتروني في الصراع العربي الاسرائلي / مجلة إنترنت العالم العربي، السنة الرابعة ، العدد الثاني، سنة 2000، ص 48.

من الوظيفة ، فيتولد لدى المجرم المعلوماتي الرغبة في الإنتقام من رب العمل[1]، فكثيرا من الأفراد يفصلون تعسفا أو بغير وجه حق من الشركة أو منظمة حكومية ، وهم يملكون المعلومات و التدريب اللازم و المعرفة الكافية بخفايا هذه الجهة و في حالات كثيرة مثلت قوة محركة لبعض العاملين لإرتكاب جرائم الحاسوب.

لذا يرتكب الجاني الجريمة رغبة منه في الإنتقام ليجعل الشركة أو المؤسسة تتكبد خسائر مالية كبيرة

من جراء ما يسببه لها من ضرر يحتاج إصلاحه إلى وقت لا باس به[2]، فعلى سبيل المثال دفع الإنتقام بمحاسب شاب إلى التلاعب بالبرامج المعلوماتية الخاصة بالشركة التي يعمل بها ، حيث برمجها على أن تخفي كل البيانات الخاصة بالشركة بعد مضى ستة أشهر من تاريخ تركه للعمل وحدث ما أراد بالفعل فبعد أن ترك العمل ومرت ستة أشهر اختفت البيانات الخاصة بتلك الشركة نهائيا عن جهاز الكمبيوتر[3].

كما تشير التقديرات إلى أن نسبة كبيرة من الجرائم المرتكبة عبر الإنترنت ترتكب من قبل موظفي الجهة نفسها ، و من الوقائع التي حدثت في الولايات المتحدة الأمريكية أنه حكم على أحد الموظفين في إحدى شركات التأمين بالسجن لمدة سبع سنوات و غرامة قدرها 150 ألف دولار لأنه أدخل فيروسا في أجهزة الشركة التي كان يعمل فيها مما أدى إلى ضياع 160 سجلا من سجلات العملاء ، و ذلك إنتقاما من الشركة لأنها قامت بفصله عن العمل[4]، وقد يكون الهدف ليس تعطيل الموقع فقط و إنما الإستيلاء على البيانات الخاصة بالموقع و استعمالها كما حصل أخيرا لشركة **سوني** العملاقة حينما قام هاكرز بإختراق موقعها الألكتروني الخاص بلعبة – البلاي ستيشن– وسرقة بيانات خاصة بنحو 77مليون عميل و كان من ضمن هذه البيانات معلومات خاصة ببطاقات عملاء **سوني** الإئتمانية.

3- الأشخاص أو الجهات:

هناك بعض الجرائم التي ترتكب عبر شبكة الأنترنت يكون الدافع من وراء ارتكابها إلحاق الأذى

[1]- محمد سامي الشوا، ثورة المعلومات و إنعكاساتها على قانون العقوبات ، دار النهضة العربية ، سنة 2003، ص52.
[2]- نسرين عبد الحميد نبيه ، المرجع السابق ، ص52.
[3]- إيهاب فوزي السقا ، الحماية الجنائية و الأمنية لبطاقات الإئتمان ، دار الجامعة الجديدة ، الإسكندرية ، سنة 2007، ص138.
[4]- صالح بن محمد المسند ، جرائم الحاسب الآلي الخطر الحقيقي في عصر المعلومات مقال بالجلة العربية للدراسات الأمنية و التدريب ، المجلد 15، العدد 29، الرياض ، ص182.

بالأشخاص أو جهات بعينها و غالبا ما تكون تلك الجرائم مباشرة ترتكب في صورة إبتزاز أو تهديد أو تشهير مثل ما حصل بإماراة دبي بدولة الإمارات العربية المتحدة عندما قام أحد الأشخاص بقرصنة صور الفتيات و السطو على البريد الإكتروني الخاص بمجموعة من فتيات تلك الدولة و سرقة صورهن الشخصية و نشرها على موقع خاص بشبكة الإنترنت مع مجموعة صور إباحية ، أيضا ما حصل في المملكة العربية السعودية حينما قام أحد الأشخاص باختراق البريد الإكتروني الخاص بإحدى الفتيات بالسعودية و الحصول على بعض الصور الشخصية الخاصة بها و إبتزازها فيمابعد ، و قد تكون غير مباشرة تتمثل في الحصول على البيانات و المعلومات الخاصة بتلك الجهات أو الأشخاص لاستتخدامها فيما بعد في ارتكاب جرائم مباشرة.

4- دوافع تجارية و إقتصادية:

تعد شبكة الإنترنت مجالا جديدا تماما للعمل التجاري ، إذ سمحت للشركات بالعمل بسرعة و دون استخدام قنوات الإتصال التقليدية عالية التكاليف ، و وفرت إمكانيات متساوية للجميع في كل أنحاء العالم ، وفرضت حدود إقتصادية ، ووفرت فرصا للأمن في عملية تبادل المعلومات داخل المؤسسة الواحدة أو بين مختلف المؤسسات و الشركات و المنظمات البعيدة جغرافيا عن بعضها البعض مما وسع من دائرة المستهلكين ، بالإضافة للحركية التي وفرتها الشبكة وسمحت من جديد بالنظر في الأشكال الجديدة من الخدمات و البضائع ومن أمثلة ذلك إمكانية القيام من خلال الشبكة بحجوزات في الكثير من دول العالم من ذلك حجز التذاكر لحضور الألعاب الرياضية و النشاطات الترفيهية و السفر بالطائرات و السفن و القطارات ، و يعمل بنجاح في روسيا نظام للحجز المسبق لبطاقات خطوط السكك الحديدية للسفر على خطوط دول رابطة الدول المستقلة ، ووفر ظهور التسويق عبر شبكات الإنترنت إمكانيات جديدة و رخيصة ، وسريعة و عملية من خلال الشبكات ، لأنه يمكن تحديث صفحات ال web خلال ثوان لا أكثر ، و تعتبر بعض صفحات ال web أنه كلما وصلت المعلومات بسرعة للمشترين ، كان إتخاد القرار بالشراء أسرع في هذا المجال.

و أظهرت الدراسات أن الكثير من المستخدمين يزورون الصفحات في البداية من أجل التعرف على المنتجات الجديدة و سرعان ما يتخدون قرارات من خلال المعلومات التي يحصلون عليها[1] ، وينتظر

[1]- محمد البخاري ، الإنترنت و مبادئ الأمن المعلوماتي الدولي : الدورة المعلوماتية فجرت الحواجز القائمة بين الشعوب ، شبكة الضياء للمؤتمرات و الدراسات أنظر الموقع www.diae.net تاريخ الإطلاع على الموقع في 04-06-2016.

الخبراء حدوث تطورات كبيرة في مجال التجارة الإكترونية.

رغم الإيجابيات التي حصلت عليها الإنسانية من تطور تكنولوجيا المعلوماتية كشبكة الأنترنت و المعلومات الرقمية ، إلا أن العالم اليوم يواجه مشلكة نتيجة زيادة نسبة الجرائم المرتكبة عن طريق الحاسبات الإكترونية ، وخاصة في المجالات الإقتصادية و الإقراض المالي ، ومن المعلومات التي نشرتها وزارة الداخلية الروسية عام 1997 أن حصة الجرائم المرتكبة عن طريق الحاسبات الإكترونية بلغت نسبة 0.02 % من عدد الجرائم في المجال المالي و أن الخسائر المادية بلغت أكثر من 20 مليار روبل ، ووفر إنفتاح الشبكات إمكانيات أكبر للمقتحمين الذين استطاعوا من خلالها الوصول لإمكانية معرفة كلمة السر ، و عناوين الصفحات الإكترونية و غيرها وحتى الدخول إلى الشبكات بأسماء مسجلة لمستخدمين آخرين ، ونتيجة لتلك التصرفات تضررت شركات معروفة بشكل كبير ، وتضررت قدرتها التنافسية و عرضتها لفقدان ثقة الزبائن[1].

5- الدوافع الأمنية و العسكرية:

هناك العديد من الجرائم التي ترتكب بواسطة شبكة الأنترنت ويكون الهدف أو الدافع من وراء ارتكابها سياسيا يتمثل في تهديد الأمن القومي و العسكري و ظهور ما يعرف بحرب المعلومات والتجسس الإلكتروني و الإرهاب الإلكتروني ، هذا وقد وقعت في الفترة الأخيرة العديد من الحوادث التي تؤكد ذلك ، مثل ماحصل في الفترة ما بين عامي 1990-1991 عندما استطاع خمسة متسللين من هولندا التسلل إلى 34 نظاما من أنظمة الحاسب الآلي في مواقع الجيش الأمريكي على شبكة الأنترنت ، بما في ذلك المواقع التي كانت موجهة مباشرة لعملية عاصفة الصحراء حيث استطاعوا الحصول على معلومات في غاية الأهمية من مواقع دقيقة للقوات الأمريكية و أنواع الأسلحة التي تملكها تلك القوات و قدرة الصواريخ و حركة السفن الحربية الأمريكية في منطقة الخليج.

و مثال آخر يتمثل في سرقة معلومات عسكرية تتعلق بالسفن التي تستعملها القوات العسكرية التابعة للدول الأعضاء من حلف شمال الأطلنطي من أنظمة الحاسبات الآلية الخاصة بسلاح البحرية الفرنسية خلال صيف 1994 ، و مثل ما حصل في إيطاليا عام 1998م عندما تعرضت عدة وزارات و جهات حكومية و مؤسسات مالية لهجوم من جماعات الأيدي الحمراء عن طريق تدمير مراكز المعلومات الخاصة بها.

[1]- محمد البخاري ، الأنترنت و مبادئ الأمن المعلوماتي الدولي ، الموقع السابق.

وكذالك ما حصل عندما قامت مراهقة في الخامسة عشرة من عمرها بمحاولة تسلل إلى موقع خاص بإحدى القواعد العسكرية للغواصات الحربية بسنغافورة ، وفي عام 1999 تمكن مراهق أمريكي عمره 16 عاما من إختراق حاسبات وكالة الفضاء الأمريكية (ناسا) ووزارة الدفاع الأمريكية (البينتاجون) و تمكن من نسخ برامج من إدارة الطيران و الفضاء قيمتها حوالي 7.1مليون دولار ، و في عام 2001 إخترق متسللون حاسبات شبكة كهرباء كاليفورنيا بالولايات المتحدة الأمريكية و خلال شهر ماي 2008 تعرضت العديد من المواقع الإكترونية البلجيكية إلى عمليات قرصنة ، كما أن موقع الأمم المتحدة أيضا تعرض لعملية قرصنة من قبل أحد القراصنة و ذلك في بداية شهر أغسطس 2007 الذي طالب طالب اسرائيل و أمريكا بالتوقف عن شن الحروب و قتل الأطفال ، كذلك موقع الكهرباء السورية الذي تعرض لعملية قرصنة في منتصف عام 2007 و ذلك على خلفية الإنقطاعات الدائمة و المتكررة للتيار الكهربائي في معظم المدن السورية و التي تجاوزت أحيانا السبع ساعات.

المبحث الثاني: أركان الجرائم الماسة بالمعطيات.

إستقر الفقه على ضرورة وجود نصوص قانونية تجريمية خاصة لمواجهة الجريمة عبر الوسائط الإلكترونية ، خاصة بعد ظهور شبكة الإنترنت التي ساهمت بشكل كبير في تفشي الجريمة ووعيا بخطورة الوضع أصدر المجلس الأوروبي سنة 1989 توصية لتشجيع الدول الأعضاء على تبني نصوص تشريعية عقابية خاصة بالجريمة المعلوماتية[1]، ومنذ ذلك الحين و الدول في سعى حثيث لإرساء قواعد قانونية تجريمية تتفق و هذه الظاهرة المستحدثة ، وقد سعى المشرع الجزائري في تعديله في قانون العقوبات بإضافته القسم السابع بعنوان "المساس بأنظمة المعالجة الآلية للمعطيات" وقد أرسى هذا القسم حماية فعالة لأنظمة المعالجة الآلية للمعطيات ، و ذلك رغبة منه في وضع حد للإعتداءات الواقعة على المعطيات من جهة و مواكبة العصرنة و السير قدما نحو تطوير منظومته التشريعية تأسيا بذلك بغيره من التشريعات من جهة أخرى ، ومن ثمة نص على مجموعة من الجرائم ، وأوجب لها عقوبات قاسية للحد من اقترافها ، وكما هو معلوم فإن المشرع يتطلب لقيام جريمة ما توافر على أركان الجريمة لذلك قسمنا هذا المبحث إلى مطلبين تناولنا في المطلب الأول الركن المادي و الركن المعنوي في المطلب الثاني.

المطلب الأول: الركن المادي للجرائم الماسة بالمعطيات الرقمية.

يعد الركن المادي للجريمة الجانب المادي الذي يدخل في تكوينها ، و يبرز هذا الجانب إلى العالم الخارجي بمظهر مادي يعبر عن سلوك و نتيجة[2]، ويتكون الركن المادي من ثلاث عناصر هي السلوك الإجرامي و النتيجة التي تحققت و العلاقة السببية التي تربط بين السلوك و النتيجة ، وقد لا يتوفر الركن المادي دائما على هذه العناصر في جميع الجرائم ، فقد يكتفي المشرع بالسلوك وحده للقول بقيام الركن المادي للجريمة دون اشتراطه أن تتحقق النتيجة وصور ذلك ما يسمى بالجرائم الشكلية[3].

وفي الحقيقة يصعب الفصل بين العمل التحضيري و البدء في النشاط الإجرامي في الجرائم الماسة

[1] ـ قارة أمال ، الجريمة المعلوماتية ، رسالة ماجستير ، جامعة الجزائر ، سنة 2002،ص37

[2] ـ عبود السيراج، قانون العقوبات ، القسم العام ، الطبعة الرابعة، مطبوعات جامعة دمشق ، سنة 1990، ص143.

[3] ـ عبد الله سليمان، شرح قانون العقوبات الجزائري القسم العام، الجزء الأول، ديوان المطبوعات الجامعية، الجزائر، سنة 1998، ص145.

بالمعطيات ، فحتى لو كان القانون لا يعاقب على الأعمال التحضيرية في الجرائم العادية إلا أن الأمر يختلف بعض الشيء في جرائم تكنولوجيا المعلومات ، فشراء برنامج الإختراق أو تصميمه أو شراء معدات لفك الشفرات و كلمات المرور ، وحيازة صور مخلة بالحياء لأطفال صغار في السن كلها أشياء تشكل جريمة في حد ذاتها ، لذلك نجد أن المشرع الفرنسي قد وسع من مفهوم الشروع في الجرائم المعلوماتية باعتبار هذه الأفعال هي مقدمة الفعل غير المشروع و بالتالي فإن الجزء الأكبر من الأعمال التحضيرية يدخل في نطاق الشروع في السلوك المجرم و يعاقب عليه بنفس عقوبة الجريمة التامة[1].

لذلك تحديد الركن المادي في الجرائم الماسة بالمعطيات أو الجرائم المرتكبة عبر الإنترنت يثير جملة من الصعوبات التي تفرضها طبيعة الوسط الذي تتم فيه الجريمة والمتمثل في الجانب التقني ، وهذا ما يميز ركنها المادي الذي يجب أن يتم باستخدام أجهزة الحاسب الآلي أو الشبكة العالمية للإنترنت و تبدأ التساؤلات التي تتعلق ببداية النشاط التقني أو الشروع فيه ، ومكان البداية و اكتمال الركن المادي ، و أجهزة السلوك الإجرامي المرتكب في العالم المادي ، أو العالم الإفتراضي و غيرها من التساؤلات التي تتعلق بطبيعة الجريمة[2] ، و قد قسمنا هذا المطلب الى أربع فروع تناولنا في الفرع الأول : جريمة الدخول غير المصرح به ، وفي الفرع الثاني : جريمة البقاء الإحتيالي ، وفي الفرع الثالث : جريمة الغش المعلوماتي ، وفي الفرع الرابع : جريمة الإتلاف المعلوماتي.

الفرع الأول: الركن المادي في جريمة الدخول غير المصرح به و جريمة البقاء الإحتيالي.

أولا- في جريمة الدخول غير المصرح به: بالرجوع إلى قانون العقوبات الجزائري نجده أنه يعاقب كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك[3].

ومن خلال ذلك نجد أن المشرع نص على فعل مادي وهو الدخول عن طريق الغش ، إلا أنه لم يقدم تعريفا له ، وبالرجوع إلى بعض التشريعات العربية نجدها تعرف هذا الفعل على أنه دخول

[1] - أحمد حسام طه تمام ، الجرائم الناشئة عن استخدام الحاسب الآلي (الحماية الجنائية للحاسب الآلي ، دراسة مقارنة)، دار النهضة العربية ، القاهرة ، الطبعة الأولى ، 2000، ص596.

[2] - منصور بن صالح السلمي ، المسؤولية المدنية لانتهاك الخصوصية في نطاق مكافحة جرائم المعلوماتية ، السعودية ، جامعة نايف العربية للعلوم الأمنية ، كلية الدراسات العليا سنة2010،ص 76.

[3] - أنظر المادة 394 مكرر من الأمر رقم 66 . 150 المؤرخ في 8 جوان1966 المتضمن قانون العقوبات الجزائري المعدل و المتمم.

شخص بطريقة معقدة إلى حاسب آلي ، أو موقع إلكتروني أو نظام معلوماتي ، أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها[1]، لذلك يعد فعل الدخول غير المصرح به أو المخول به من الأنشطة الجرمية الأكثر انتشارا من بين جرائم الكمبيوتر أو المعطيات ، ويقوم التوصل غير المصرح به بالأساس على الدخول إلى نظام الحاسوب أو شبكة المعلومات ، ويكون ذلك عادة من خلال استخدام وسيلة إتصال عن بعد كالمديم و من خلال التواصل عبر نقاط الإتصال و الموجات الموجودة على الشبكة إلى نظام كمبيوتر معين بغرض الوصول إلى البيانات أو البرامج المخزنة في النظام و يتطلب هذا النشاط غالبا تجاوز أو كسر إجراءات الحماية التقنية للنظام كتجاوز كلمة السر و إجراءات التعريف و الجدران النارية و غيرها أو التوصل لنقطة ضعف في نظام حماية البرامج و النفاذ منها[2].

يتبين لنا أن المشرع الجزائري إكتفى بذكر فعل الدخول فنص على ذلك" ... كل من يدخل أو يبقى عن طريق الغش " ولم يذكر الأفعال المادية لفعل الدخول و لم يحدد الوسيلة أو الطريقة التي يتم بها الدخول إلى النظام ، لذلك جرم أي وسيلة أو طريقة سوى تم الدخول بطريقة مباشرة أو غير مباشرة على عكس بعض التشريعات الأخرى التي وسعت من دائرة التجريم و ذكرت مجموعة كبيرة من الأفعال التي قد تحدث نتيجة فعل الدخول[3] ، وقد تم تجريم تلك الأفعال لعدم وجود حماية قانونية صريحة للبيانات و المعلومات الإلكترونية في التشريعات العقابية إضافة إلى لزوم معاملتها معاملة المال و الوثائق و الحقوق الأخرى التي يحظر القانون المساس بها ، فالمعلومات و البيانات الإلكترونية لها قيمة مادية و معنوية لا تقل عن قيمة الوثائق و الأموال و الحقوق الأخرى المحمية بموجب التشريعات النافذة ، و لا إمكانية لتصور وقوع إتلاف إلكتروني لا يكون محله مال إلكتروني معنوي وهو أمر لا يتوفر إلا في بيئة إلكترونية قوامها تقنين نظم المعلومات ، كما قد تحتوي هذه البيانات على دراسات و معلومات خاصة أو أنها برامج تتحكم بأنظمة أو مؤسسات و تسيرها مما يترتب على ما تقدم أن أي من تلك الأفعال قد ينجم عنها تعطيل خدمات مثل الكهرباء ...إلخ ، وقد ينجم عنها تعطيل الأجهزة ووقوع خسائر مادية أخرى ، مما يتطلب وجود حماية تشريعية خاصة

[1] ـ أنظر المادة الأولى من المرسوم الملكي السعودي المتعلق بنظام مكافحة الجرائم المعلوماتية السعودية، الصادر في 27،4 ، 2008.

[2] -http// www- assakina. com ./book .59149 تاريخ الاطلاع على الموقع بتاريخ 11،6،2016.

[3] ـ وقد حاولت بعض التشريعات معالجة فعل الدخول غير المصرح به ، ومن بين هذه التشريعات ما نص عليه القانون الأردني : كل من دخل قصدا إلى موقع إلكتروني أو نظام معلومات بأي وسيلة دون تصريح أو بما يخالف أو يجاوز التصريح يعاقب بالحبس ...وإذا كان الدخول بهدف إلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو توقيف أو تعطيل عمل نظام معلومات أو تغيير موقع إلكتروني أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو إنتحال صفته أو إنتحال شخصية مالك فيعاقب الفاعل....

للمعلومات و البيانات المخزنة في نظام معلومات أو شبكة معلومات لسهولة الوصول إليها و إلغاءها و حذفها و إضافتها و تدميرها و إتلافها[1].

ويرى الفقه الفرنسي أن الدخول مدلول معنوي ، حيث يعتبر الدخول إلى نظام معالجة البيانات أو النظام المعلوماتي أو النظام الإلكتروني يشبه الدخول إلى ذاكرة الإنسان ، كما أن له مدلولا ماديا يتمثل في أن الشخص يكون متى دخل الجاني إلى النظام كله أو جزء منه و كذلك يتحقق الدخول غير المشروع متى كان مسموحا للجاني بالدخول لجزء معين في النظام و تجاوز ذلك إلى جزء آخر غير مسموح له بالدخول ، و حتى نكون بصدد جريمة الدخول غير المصرح به يجب أن يكون النظام مفتوحا أمام الجمهور، لأنه لو كان كذلك لما اعتبر جريمة و معظم الذين يدخلون بطريقة غير مشروعة عن طريق التوصل إلى الأرقام و الكلمات أو الشفرات أو الحروف أو المعلومات السرية التي تكون بمثابة النظام الأمني لجهاز الحاسب الآلي أو البرامج و النظم المعلوماتية[2].

وقد لا يكون هدفهم في الغالب الإضرار بالبيانات و الملفات أو تدميرها ، وقد يسعى مقترفو هذه الأنشطة إلى الإطلاع على المعلومات المحمية ، غير أن حماية المعلومات من أخطار هذه الأنشطة أو احتمال تطور هذه الأنشطة من مجرد هدف للإطلاع إلى أهداف أكثر خطورة كالتلاعب بالمعطيات أو إتلافها أو ارتكاب غير ذلك من جرائم الحاسوب أو استخدام الدخول لارتكاب جرائم أخرى بواسطة الكمبيوتر ، دفعت غالبية دول العالم إلى تجريم هذه الأنشطة كما هو الشأن في قوانين كل الدول الأوربية ، و حتى أمريكا ، واليابان إذ تقع الجريمة من كل إنسان أيا كانت صفته ، سواء كان يستطيع أن يستفيد من الدخول أولا فيكفي أن يكون الجاني ليس ممن لهم الحق في الدخول إلى النظام أو من الذين ليس لهم الحق في الدخول بالطريقة التي دخلوا بها ، حيث تتوافر الجريمة في كل حالة يكون فيها الدخول مخالفا لشروط الدخول التي نص عليها القانون أو الاتفاقيات ، كما هو الحال إذا كان القانون يفرض سرية معينة بالنسبة لبعض الأنظمة مثل أسرار الدولة أو السرية المتعلقة بالمعلومات الذاتية أو الإسمية أو أسرار الأشخاص مثل أسرار الحياة الخاصة المهنية أو أي معلومات[3] يجمعها الإنسان في نظام و لا يترك أمر الإطلاع عليها لأي إنسان ، ويكون الدخول غير مشروع إذا كان من له حق السيطرة على النظام قد وضع بعض القيود للدخول إليه ولم يحترم الجاني

[1] ـ بهاء فهمي الكبيجي ، مدى توافق أحكام جرائم أنظم المعلومات في القانون الأردني ، رسالة ماجستير في القانون العام ، جامعة الشرق الأوسط ، 2013، ص26.

[2] ـ بهاء فهمي الكبيجي ،المرجع نفسه، ص29.

[3] ـ قارة أمال ، الجريمة المعلوماتية ، المرجع السابق ، ص42 .

تلك القيود ، و إذا كان يتطلب ضرورة دفع مبلغ من النقود ، وتم الدخول دون دفع ذلك المبلغ و ترتكب الجريمة من من يعمل على الحاسب و لكن بنظام معين ، فيدخل في نظام آخر كما تقع الجريمة سواء تم الدخول إلى النظام كله أو إلى جزء منه فقط ، أي يكفي لتوافر الجريمة أن يتم الدخول على بعض عناصر النظام ، أو على عنصر واحد منه ، أو منطقة منه بشرط أن يكون العنصر الذي تم الدخول إليه فقط يدخل في برنامج متكامل قابل للتشغيل[1].

كما أن عملية الدخول إلى نظام المعلوماتي بإعتبارها مسألة تقنية بحتة قد تتم بعدة طرق هي:

ـ الإتصال المادي المباشر بالنظام المعلوماتي: ويقصد به الدخول في النظام دون الحاجة إلى شبكة إتصال معلوماتي أو إلكتروني لتحقيق الجريمة أي الجاني موجود في نفس المكان الذي يوجد فيه النظام محل الجريمة و ماعليه في هذه الحالة إلا إجراء عمليات سواء مادية مثلا إدخال دعامة مادية كالقرص المضغوط تحتوى على برنامج فك الرموز للدخول في النظام المعلوماتي المحمي تقنيا أو إزالة أو حذف عنصر مادي من الكمبيوتر محل الجريمة لتسهيل عملية الدخول في النظام ، كما قد يتم الدخول في النظام بإجراء عمليات إلكترونية كالتلاعب في عين المكان بنظام معطيات أو برامجه أو إجراء تعديلات فيها بهدف تسهيل عملية الدخول.

ـ الإتصال المعنوي عن بعد بالنظام المعلوماتي: و يقصد به الدخول في النظام المعلوماتي محل الجريمة بإستعمال وسائل الإتصال عن بعد المستحدثة (الشبكات المعلوماتية أو الإلكترونية السلكية أو اللاسلكية) ، وفي هذه الحالة لا يشترط حتى تقوم الجريمة أن يكون الجاني موجود في نفس مكان وجود الكمبيوتر محل الجريمة.

وتهدف كل من حالتي الإتصال بالنظام محل الجريمة القيام بتصرفات غير مشروعة من بينها حالة إستعمال أو مناداة برنامج عن بعد أو داخل النظام دون أي ترخيص أو من دون أي صلاحية.
ـ حالة إستجواب أو الإطلاع على محتوى معطيات معلومات موجودة في النظام من دون أي ترخيص أو صلاحية[2].

[1] ـ قارة أمال، المرجع السابق، ص43.
[2] ـ دردور وسيم ، جرائم المعلوماتية على ضوء القانون الجزائري و المقارن ، رسالة ماجستير ، جامعة قسنطينة ، 2013، ص30، 31.

و في النهاية فإن الجريمة تقوم بمجرد فعل الدخول إلى النظام دون ضرورة حدوث أية نتيجة أخرى ، فلا يشترط لقيامها إلتقاط المتدخل للمعلومات التي يحتويها النظام أو بعضها أو استعمالها تلك المعلومات ، بل أن الجريمة تتوافر حتى و لو لم تكن لدى الجاني القدرة الفنية على تنفيذ العمليات على النظام[1].

ثانيا ـ في جريمة البقاء الإحتيالي.

إعتبر المشرع أن البقاء الإحتيالي جريمة نص عليها في قانون العقوبات بقوله ، كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات ...[2] لذلك عرف البقاء الاحتيالي بأنه كل تواجد غير عادي كالإتصال بواسطة الشبكة المعلوماتية بالنظام المعلوماتي أي الدخول و النظر فيه ، أي في المعطيات التي يتضمنها و غيرها من التصرفات الغير مسموح بها و التي تشكل بدورها بقاء إحتيالي[3]، فيتحقق الركن المادي في جريمة البقاء الإحتيالي إذا اتخذ صورة البقاء داخل النظام و يقصد بفعل البقاء " التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام[4] ".

وقد يجتمع الدخول غير المشروع و البقاء غير المشروع معا و ذلك في الفرض الذي لا يكون فيه الجاني له الحق في الدخول إلى النظام و يدخل إليه فعلا ضد إرادة من له الحق في السيطرة عليه ، ثم يبقى داخل النظام بعد ذلك و يتحقق في هذا الفرض في الإجتماع المادي لجريمتي الدخول و البقاء غير المشروع في النظام[5].

لذلك تعد هذه الجريمة من الجرائم المستمرة ، فالجريمة تستمر كلما زادت مدة البقاء الغير مشروع داخل النظام المعلوماتي[6] ، كما أن جريمة البقاء الإحتيالي لم يشترط فيها القضاء الفرنسي أن تتوافر لدى المجرم نية الإضرار بالنظام المعلوماتي بل يكفي أن يقوم بمجرد البقاء فقط إذا كان غير مشروع ، و قد يتسبب المجرم زيادة عن بقائه الغير مشروع في النظام إلى الإضرار بهذا الأخير[1].

---

[1] ـ قارة أمال ، المرجع السابق ،ص 43.

[2] ـ أنظر المادة 394 مكرر فقرة الأولى من قانون العقوبات الجزائري ، المرجع السابق.

[3] - Bensoussan Alain (sous la direction de) , Internet :aspect Juridique , édition Hèmes ,Juin 1996 (France) ,page 109

[4] ـ علي عبد القادر قهوجي ، الحماية الجنائية لبرامج الكمبيوتر ، المكتبة القانونية ، القاهرة ، 1999، ص133.

[5] ـ علي عبد القادر قهوجي ، المرجع نفسه، ص133.

[6] ـ أحسن بوسقيعة ، الوجيز في القانون الجزائي العام ، الطبعة الأولى ، الديوان الوطني للأشغال التربوية ، الجزائر ، 2002، ص 85، 68.

وقد نص قانون العقوبات على أنه ، تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة ...[2].

يتبين أن المادة نصت على ظرفي تشديد لعقوبة الدخول أو البقاء داخل النظام ، ويتمثل هذان الظرفان في حالة ما إذا نتج عن الدخول أو البقاء غير المشروع محو أو تعديل البيانات التي يحتويها النظام ، أو عدم قدرة النظام على تأدية وضيفته ، و يكفي لتوافر هذا الظرف المشدد أن تكون هناك علاقة سببية بين الدخول أو البقاء غير المشروع و بين النتيجة التي تحققت ، وهي محو النظام أو عدم قدرته على أداء وظيفته ، أو تعديل البيانات.

الفرع الثاني: الركن المادي في جريمتي الغش المعلوماتي و الإتلاف المعلوماتي.

أولا ـ في جريمة الغش المعلومتي: تعد جريمة الغش المعلوماتي في مجال المعالجة الآلية للمعطيات من أخطر طرق الغش التي تقع في هذا المجال و لاسيما بعد تراجع المحررات و المستندات و الوثائق و الصكوك الورقية في حين غزت المحررات الإلكترونية كل المجالات مما زاد صعوبة اكتشاف و إثبات الغش في هذا المجال ، أو هو تغيير الحقيقة في مستند رسمي و لكن المستند هنا ليس مستندا عاديا بل هي عبارة عن تسجيلات إلكترونية أو محررات إلكترونية.

وقد أشار المشرع بخصوص الغش بقوله : ... عن طريق الغش ....خاصة مع تزايد حجم الإعتداءات الواقعة عل المعطيات المخزنة داخل الحاسب الآلي التي تمس الأفراد في حقوقهم و أموالهم و حياتهم الخاصة و أمام تزايد فرص الأشخاص للعبث و التلاعب في معطيات الحاسب بتبديلها و تحويرها بالشكل الذي يفقد الثقة بالتقنية و يمس مراكز الأفراد بات من الواجب بسط الحماية لهذه المعلومات و ضمان أمنها و سلامتها من كل تبديل وغش[3].

و يتمثل الركن المادي لجريمة الغش المعلوماتي في تغيير الحقيقة في محرر معلوماتي بإحدى الطرق التي نص عليها القانون وهو تغيير من شأنه أن يسبب ضررا ومن هنا و لقيام هاته الجريمة لا بد من توافر ثلاثة عناصر أساسية:

---

[1]-André Lucas ,jean Devréze jean Frayssinent , Droit de L'informatique et de l'internet edition Dallas ,collection thémis (Droit Privé) November 2001 (France) de la page 683 à684

[2] ـ أنظر المادة 394 مكرر 2ـ 3 قانون العقوبات الجزائري ، القانون السابق.

[3] ـ محمود أحمد عبابنة، المرجع السابق، ص107.

- وجود محرر.

- تغيير الحقيقة بإحدى الطرق المنصوص عليها قانونا.

- أن يترتب على ذلك ضررا.

1- وجود محرر:

لعل من أهم العقبات التي واجهت تطبيق النص الخاص بالغش المعلوماتي هي وجود محرر ، فمستند المعلومات ينتج عن إصدار أمر من مشغل الجهاز إلى الطابعة وذلك بطبع المعلومات التي تم معالجتها آليا داخل جهاز الكمبيوتر ، حيث أن البيانات بإدخالها تتم معالجتها و تتحول إلى معلومات مفيدة ، ويشترط أن يظهر مستند المعلومات لحيز الوجود ، فلا يشترط أن يتم الغش على المستندات المطبوعة على أوراق بواسطة طباعة ، فيمكن أن يتم التزوير على المعلومات المعالجة آليا داخل جهاز الكمبيوتر و المسجلة على قرص صلب أو قرص مرن و من هنا يمكن القول بتطبيق ذلك على برنامج الكمبيوتر ، عندما يكون هذا البرنامج قد دون على أسطوانة أو شريط ممغنط محررا ، ومن ثم فإن تغيير الحقيقة فيه يعد غشا أو تزوير لانتقال المعطيات المخزنة إلى جسم مادي ، يأخذ صفات المحرر المكتوب ، الذي يمكن قراءته بالعين عن طريق الكمبيوتر و الكشف عن مضمونه من قبل الغير[1].

2- تغيير الحقيقة:

يقصد بتغيير الحقيقة هو إبدالها بما يغايرها ، وبالتالي فلا يعتبر تغييرا للحقيقة أي إضافة لمضمون المحرر طالما ظل مضمون المحرر على حالته قبل الإضافة أو الحذف ، و يقوم ذلك بصدد المستندات المعلوماتية في حالة حذفها أو إضافتها أو التلاعب فيها بأي صورة سواء كانت البيانات مخزنة في ذاكرة الآلة أم كانت تمثل جزءا من برنامج التشغيل أو برنامج التطبيق و يجب في هذه الحالة أن تكون محلا للتجريم.

3 - الضرر:

وهو عنصر أساسي في جريمة الغش المعلوماتي ، فإذا تخلف الضرر إنتفى التزوير و لو توافرت كل أركانه ، فالضرر عنصر جوهري في جريمة الغش المعلوماتي ، و لا يشترط القانون وقوع ضرر

[1] - خثيرمسعود ، الحماية الجنائية لبرامج الكومبيوتر أساليب و ثغرات، دار الهدى ،الجزائر طبعة 2010 ،ص134 ،135.

بالفعل بل يكفي إحتمال وقوعه ، و يكفي لقيام التزوير أن يكون الضرر ماديا أو أدبيا أو فرديا أو إجتماعيا ، و البحث في توافر الضرر من عدمه مسألة تتعلق بالوقائع يفصل فيها قاضي الموضوع ، ونظرا لعدم كفاية النصوص المتعلقة بالغش في المحررات لمواجهة الغش المعلوماتي الذي يقع في مجال المعالجة الآلية للمعطيات ، فقد عاقب المشرع الفرنسي على الغش المعلوماتي الذي يقع في المستندات المعالجة آليا ، سواء كانت داخل الجهاز أو خارجه[1].

يرتكب الشخص جريمة الغش المعلوماتي إذا قام بمايلي:

1 ـ يدخل أو يسبب الدخول في الحاسب الآلي أو أي جزء منه ، أو إلى برنامج أو بيانات الحاسب بقصد ابتكار أو تنفيذ أي مشروع ، و يضع حيلة للغش أو جزء من مخادعة.

2 ـ يحصل على الإستعمال أو يتلف ، أو يحطم حاسب آلي أو أي جزء منه أو يعدل أو يمحو أو يسحب أي برنامج أو بيانات موجودة في الحاسب الآلي بأي مشروع ، عن طريق صلة أو غش أو جزء من مخادعة.

3 ـ يدخل أو يسبب الدخول في حاسب آلي أو جزء منه ، أو برنامج بيانات و يحصل على مال أو يسيطر على مال ، أو ممتلكات ، أو خدمات ذات صلة بأي مشروع.

ثانيا ـ الركن المادي في جريمة الإتلاف المعلوماتي.

قد يتخذ الركن المادي لجريمة إتلاف المعلومات إما صورة إجراء تعديلات غير مشروعة لها ، أو تدميرها أو الإدخال غير المشروع للمعلومات داخل أنظمة الحاسبات الآلية:

1 ـ التعديل غير المشروع للمعلومات: يشكل التعديل غير المشروع للمعلومات المبرمجة آليا واحد من أكثر صور إتلاف المعلومات شيوعا ، و يمكن تعريفه بأنه كل تغيير غير مشروع للمعلومات و البرامج يتم عن طريق إستخدام إحدى وظائف الحاسب الآلي.

وقد فرقت التوصية الصادرة عن المجلس الأوروبي المتعلق بجرائم المعلوماتية بين التعديلات التي تؤدي إلى نتائج سلبية تتعلق بحالة المعلومات و البرامج وبين التعديلات غير المصرح بها و التي لا

[1] ـ خثير مسعود، المرجع السابق ، ص137.

تؤدي إلى إحداث هذه النتائج بل قد تساعد على تحسين أي من المكونات المنطقية للحاسب الآلي و نظامه[1].

2 ـ تدمير المعلومات: يعد تدمير المعلومات بدوره صورة من صور الإتلاف و إن كان أبعد أثرا من مجرد إجراء بعض التعديلات للمعلومات ، وقد أوصى التقرير الصادر عن المجلس الأوروبي بخصوص جرائم المعلوماتية بتجريم الأفعال التي تؤدي إلى تدمير المعلومات ، ولقد ميزت التوصية الصادرة عن المجلس الأوروبي بين شكلين من أشكال التدمير الذي يلحق بالمعلومات ، الأول يتعلق بمحو المعلومات تماما ، والثاني بإخفاء المعلومات بحيث لا يمكن الوصول إليها دون أن يترتب على ذلك محو تماما ، ويذهب البعض إلى أن إخفاء المعلومات دون محوها لا يمكن أن يشكل تدميرا لها ، ومؤدى ذلك أن إخفاء أحد الملفات على سبيل المثال لا يترتب عليه محو المعلومات التي يحتوى عليها من ذاكرة الكمبيوتر و إنما يؤدي فقط إلى تعديل في قائمة الملفات وهو ما يعني أن إخفاء المعلومات في هذه الحالة لا يعدو أن يكون تعديلا و ليس تدميرا [2].

المطلب الثاني : الركن المعنوي في الجرائم الماسة بالمعطيات الرقمية.

لا يكفي للقول بوجود جريمة ما مجرد قيام الواقعة المادية التي تخضع بنص الجريمة و لا تخضع لسبب من أسباب الإباحة ، بل لا بد من أن تصدر هذه الواقعة عن إرادة فاعلها و ترتبط بها إرتباطا معنويا وهو ما يعبر عنه بالركن المعنوي للجريمة بمعني وجود رابطة معنوية أو صلة نفسية تربط بين ماديات الجريمة و نفسية فاعلها بحيث يمكن القول بأن الفعل هو نتيجة لإرادة الفاعل ، فالركن المعنوي هو المسلك الذهني و النفسي للجاني باعتباره محور القانون الجنائي ، ذلك لأنه في إطار هذا الركن تتحقق كافة مقومات المسؤولية الجنائية من إسناد و إذناب مع إقرار حق الدولة في العقاب الذي يبنى على هذه المقومات[3].

لذلك يتكون الركن المعنوي لجرائم المعطيات الرقمية من عنصريها أي العلم و الإرادة ، فالعلم هو إدراك الفاعل للأمور ، أما الإرادة فهي اتجاه السلوك الإجرامي لتحقيق النتيجة طبقا للمبادئ العامة المعروفة في قانون العقوبات ، وقد يكون القصد عاما أو خاصا ، فالقصد الجنائي العام هو الهدف

[1] ـ خالد ممدوح إبراهيم ، فن التحقيق الجنائي في الجرائم الالكترونية ، دار الفكر الجامعي، الإسكندرية ،2010،ص418.
[2] ـ خالد ممدوح إبراهيم ، المرجع نفسه ، ص419.
[3] ـ خمايسية حفيظة ، التعاون الدولي في مكافحة جرائم الانترنت ، رسالة ماجستير ، المركز الجامعي خنشلة ،2012 ص 24

المباشر للسلوك الإجرامي و ينحصر في حدود في ارتكاب الفعل ، أما القصد الخاص فهو الغاية من تحقيق النتيجة مثلا في جريمة القتل لا يكتفي الجاني بالفعل بل يتأكد من إزهاق روح المجني عليه.

و الأصل أن الفاعل في جريمة المعطيات الرقمية يوجد سلوك إجرامي نحو ارتكاب فعل غير مشروع أو غير مسموح به مع علمه و قاصدا ذلك و مهما يكن لا يستطيع إثبات إنتفاء علمه كركن للقصد العام ، إذن فالقصد الجنائي العام متوافر في جميع الجرائم المعلوماتية أو الإلكترونية دون أي استثناء و لكن هذا لا يمنع أن بعض الجرائم الإلكترونية تتوافر فيها القصد الجنائي الخاص مثلا جرائم تشويه السمعة عبر الإنترنت ، جرائم نشر الفيروسات عبر الشبكة[1] ، حيث قسمنا هذا المطلب إلى خمس فروع تناولنا في الفرع الأول : جريمة الدخول و البقاء غير المشروع داخل نظام المعالجة الآلية للمعطيات ، وفي الفرع الثاني: جريمة الاعتداء على سير نظام المعالجة الآلية للمعطيات ، وفي الفرع الثالث : إستخدام المعطيات كوسيلة في إرتكاب الجريمة الماسة بأنظمة المعلوماتية ، وفي الفرع الرابع: جريمة إتلاف المعلومات ، وفي الفرع الخامس: جريمة السرقة في الجرائم في نظام المعالجة الآلية للمعطيات

الفرع الأول: الركن المعنوي في جريمة الدخول و البقاء غير المشروع داخل نظام المعالجة الآلية للمعطيات:

بالرجوع إلى قانون العقوبات نجده قد نص على:" كل من يدخل أو يبقى عن طريق الغش[2]" ، حيث للركن المعنوي أهمية في قيام جريمة الدخول غير المصرح به إلى نظام الكمبيوتر ، فالأفعال التي تقوم عليها هذه الجريمة يقوم بها كل مستخدمو الكمبيوتر ، ومن بين كل هذه الأفعال لا يمكن تجريم سوى تلك التي يتحقق بشأنها القصد الجنائي ، فالركن المعنوي في جريمة الدخول و البقاء غير المشروع يتطلب دراسة القصد العام و الخاص لذلك سنتطرق إلى:

ـ القصد العام: يتطلب القصد العام أن يحيط علم الجاني بكل واقعة ذات أهمية قانونية في تكوين الجريمة ، فكل ما يتطلبه القانون من وقائع لبناء أركان الجريمة و استكمال عناصرها يتعين أن يشمله علم الجاني ، ولكن علم الجاني لا يقتصر نطاقه على الوقائع التي تدخل في تكوين الجريمة ، وإنما يتعين أن يحيط أيضا بالتكييف الذي تتصف به بعض هذه الوقائع و تكتسب به أهميتها في نظر القانون ، حيث أن عددا من الوقائع التي تقوم بها الجريمة لا تمثل أهمية في نظر القانون ، إلا إذا

[1] ـ فضيلة عاقلي ، الجريمة الالكترونية و إجراءات مواجهتها من خلال التشريع الجزائري ، مقال منشور على الموقع الآتي : . www . jilrc . com. بتاريخ 2017.04.10 و تم الاطلاع على الموقع بتاريخ 2017.10.21 .

[2] ـ أنظر المادة 394، مكرر من قانون العقوبات الجزائري.القانون السابق

اكتسبت وصفا معينا ، فإن تجردت من هذا الوصف فقد تجردت من الأهمية القانونية و لم تعد صالحة لتقوم بها الجريمة[1].

ـ أما القصد الخاص: فهو أن يتوقع الجاني حين يأتي فعله النتيجة الإجرامية التي سوف تترتب على الفعل ، فتوقع النتيجة هو الأساس النفسي الذي تقوم عليه إرادتها ، فحيث لا يكون التوقع لا نتصور وجود الإرادة ، والنتيجة التي يجب أن يتجه إليها توقع الفاعل هي النتيجة التي يحددها القانون ، وهي الدخول غير المصرح به إلى النظام و لا يشترط أن يتجه التوقع إلى الآثار غير المباشرة التي لا يدخلها القانون في تحديد النتيجة ، فالقصد الجنائي يتوافر و لو لم يتوقع الجاني هذه الآثار ، فيتعين إذن أن يتوقع الجاني أنه سوف يدخل إلى نظام غير مصرح له بالدخول إليه و لا يشترط أن يتوقع الضرر الذي سوف يلحق النظام من جراء هذا الدخول.

كذلك من الدخول غير المصرح به ، أن يكون مالك النظام قد وضع قيودا للدخول إلى النظام ولم يلتزم الجاني بهذه القيود ، أو كان الأمر يتطلب سداد مبلغ نقدي لم يسدده الجاني و قام بالدخول غير المشروع إلى النظام ، ويلاحظ في هذا الصدد أن المشرع الجزائري يعاقب على الدخول المجرد إلى النظام المعلوماتي ، فمجرد الدخول تقوم به الجريمة حتى ولو لم يترتب على دخوله ضرر أو يتحقق له من وراء الدخول نفع أو فائدة طالما أن الدخول غير مشروع.

و يتحقق فعل الدخول كذلك ، كلما دخل الجاني إلى النظام كله أو جزء منه كالدخول إلى شبكة الإتصال أو البرامج ، ويتحقق الدخول غير المشروع كذلك متى كان مسموحا للجاني بالدخول لجزء معين في البرامج فيتجاوزه إلى جزء آخر غير مسموح له بالدخول فيه فمثلا أو أن الجاني دخل على موقع www.amazon.com وهو موقع للبيع الإلكتروني معد للجمهور ، ولكنه تجاوز الموقع إلى البيانات الخاصة بإعداد الموقع و تنظيمه ، في حين أن هذه البيانات أو المعلومات لا يجوز للجمهور الدخول عليها ، فهنا يكون فعل الجاني مكونا لجريمة الدخول غير المشروع رغم أن الموقع مفتوح للجمهور[2].

[1] ـ خالد ممدوح الجريمة المعلوماتية ، المرجع السابق ، ص 260
[2] ـ خالد ممدوح الجريمة المعلوماتية ، المرجع نفسه ، ص 269

الفرع الثاني: الركن المعنوي في جريمة الإعتداء على سير نظام المعالجة الآلية للمعطيات وإتلاف المعلومات.

أولا ـ في جريمة الإعتداء على سير نظام المعالجة الآلية للمعطيات: نص قانون العقوبات على "كل من شارك في مجموعة أو إتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم و كان التحضير مجسدا بفعل أو عدة أفعال مادية ..."[1] لذلك تعتبر جريمة الإعتداء على سير نظام المعالجة الآلية للمعطيات هي جريمة عمدية لأن أفعال الإعتداء المتمثلة في أفعال العرقلة و التعطيل تعد من الأفعال العمدية ، و هذا ما يميزه عن الإعتداء غير العمدي لسير النظام الذي يعتبره ظرف مشددا لجريمة الدخول و البقاء غير المشروع داخل النظام ، وعليه فالقصد الجنائي المفروض ينتج من طبيعة الأفعال المجرمة[2].

و جريمة الإعتداءات العمدية على المعطيات يتخذ فيها القصد الجنائي بعنصريه العلم و الإرادة ، فيجب أن تتجه إدراة الجاني إلى فعل الإدخال أو المحو أو التعديل ، كما يجب أن يعلم الجاني بأن نشاطه الإجرامي يترتب عليه التلاعب في المعطيات ، ويعلم أيضا أنه ليس له الحق في القيام بذلك ، وأنه يعتدي على صاحب الحق في السيطرة على تلك المعطيات بدون موافقته ، ويشترط لتوافر الركن المعنوي بالإضافة إلى القصد الجنائي نية الإعتداء ، لكن هذا لا يعني ضرورة توافر قصد الإضرار بالغير بل تتوافر الجريمة و يتحقق ركنها بمجرد فعل الإدخال أو المحو أو التعديل مع العلم بذلك و اتجاه الإرادة إليه ، وإن كان الضرر قد يتحقق في الواقع نتيجة للنشاط الإجرامي إلا أنه ليس عنصرا في الجريمة.

ثانيا ـ في جريمة إتلاف المعلومات:

يشترط لقيام هذه الجريمة توافر القصد العام فيكفي هذا القصد لثبوت علم الجاني بأن الأموال التي يتعدى عليها بالإتلاف هي ملك للغير و أن فعله من شأنه أن يتلف الشيء أو يجعله معطل أو يجعله غير صالح للإستعمال أو ينقص قيمته ، و يجب أيضا أن تتجه إرادة الجاني إلى إحداث الإتلاف أو التخريب أو التعطيل و ينتج عن فعله تحقق الضرر المترتب على جريمته مع علمه أن فعله غير شرعي.

[1] ـ أنظر المادة 394 مكرر 5 من قانون العقوبات الجزائري.القانون السابق

[2] ـ قارة أمال ، الحماية الجزائية للمعلوماتية في التشريع الجزائري ، دار هومة ، الجزائر ، الطبعة 02 ، 2007،ص125

وفعل الإتلاف يتطلب وجود القصد الجنائي و يكفي قيام القصد العام في اتجاه نية الجاني إلى إتلاف الأموال الثابتة أو المنقولة و يتطلب علم الجاني بأن فعله يؤدي إلى إتلاف أموال مملوكة للغير ، فإن عدم العلم هنا ينفي القصد الجنائي ، و يجب أيضا إتجاه الإرادة للفعل الذي يؤدي إلى الإتلاف ، لأن الجريمة عمدية ففي الجريمة المتعلقة بإعاقة سير نظام معلوماتي أو الجريمة المتعلقة بالإعتداء على المعلومات الموجودة داخل الجهاز تتجه إرادة الجاني إلى إتلاف المال وذلك بالقيام بوضع برنامج من شأنه أن يغير المعلومات أو يقوم بمحو البيانات[1] ، فمن يعمل هذا العمل الإجرامي فهو على درجة عالية من الناحية التقنية في مجال المعلوماتية ، وبناء على ذلك فهو يعلم بالفعل بأن هذه الأموال المعلوماتية التي تتجه إرادته إلى إتلافها مملوكة للغير فإن القصد الجنائي يكون متوافرا و تقوم الجريمة المنصوص عليها باكتمال أركانها أما لو كان الإتلاف ناتج عن حادث غير مقصود ، كما لو وقع شيء من العامل أو الموظف على الجهاز أدى إلى إتلاف جزء منه فلا تقوم جريمة الإتلاف العمدي التي تسبب عنها إعاقة النظام المعلوماتي[2].

الفرع الثالث: الركن المعنوي في جريمة السرقة في نظام المعالجة الآلية للمعطيات.

كما سبق فإن جانب من الفقه الجنائي يسلم بأن المعلومات تصبح لأن تكون محلا للسرقة بالإعتداء عليها و اغتصابها من حوزة صاحبها فالمعلومات لها قيمة تقدر بثروات طائلة ، و المعلومات من الأموال المعنوية و لذلك فهي تصلح محلا للسرقة و يتم الحصول على هذه المعلومات عن طريق الحصول على كلمة السر و السرقة المعلوماتية يترتب عليها ضرر للغير فقد تكون السرقة بهدف إفشاء سر و يكون ذلك بدخول الجاني إلى نظام معلوماتي خاص و يلتقط المعلومة أو يسرقها بطريقة نسخ شريط أو بطباعتها و نقلها و الإستيلاء عليها[3] ، وفي كل الأحوال فإن السرقة المعلوماتية لا يترتب عليها خروج المعلومات من حيازة صاحبها أو الحائز القانوني لها ولكن تخرج فقط نسخة من هذه المعلومات.

فالقصد العام: إن الخطأ الذي ينصب على رضى المجنى عليه ينفي فعل العلم و ينفي القصد الجنائي كمن يأخذ برنامجا معتقدا أن صاحبه راض عن ذلك فينتفي هنا عنصر العلم ومن يستولي

[1] ـ خالد ممدوح إبراهيم ، فن التحقيق الجنائي في الجريمة الالكترونية ،المرجع السابق، ص420
[2] ـ خالد ممدوح إبراهيم ، فن التحقيق الجنائي في الجريمة الالكترونية ، المرجع نفسه ، ص421
[3] ـ خالد ممدوح إبراهيم ، الجرائم المعلوماتية ، المرجع السابق ، ص 304

على دعائم بها معلومات أو من دخل خطأ على برنامج بالرقم السري فإنه لا يعد مرتكبا لجريمة السرقة.

القصد الخاص: تعد السرقة جريمة عمدية يفترض لإثباتها توافر قصد جنائي خاص و هو الذي يعبر عن نية التملك ، لأنها هي التي تكشف عن نية الجاني في حيازة الشيء المعلوماتي و يستدل على توافر القصد من القرائن و الظروف ، ونية التملك التي تتجه إليها إرادة الجاني هو عنصر يضاف إلى عنصر القصد العام (العلم والإرادة) فبالإضافة إلى ضرورة إتجاه الإرادة إلى سرقة الشيء المعلوماتي مع علم الجاني أنه يسرق شيء مملوك للغير يضاف إليهما عنصر نية الإستحواذ على الشيء المسروق[1].

[1] ـ خالد ممدوح إبراهيم ، الجرائم المعلوماتية ، المرج السابق ، ص306

الفصل الثاني : تصنيف الجرائم الواقعة على المعطيات الرقمية.

تعتبر الجرائم الماسة بالمعطيات الرقمية من الجرائم التي ترتكب ضد أفراد أو مجموعات مع وجود دافع إجرامي لإلحاق الضرر عمدا بسمعة الضحية بشكل مباشر أو غير مباشر، بإستخدام شبكات الإتصال الحديثة مثل الإنترنت (غرف الدردشة ، البريد الإلكتروني و الهواتف الجوالة ، الرسائل النصية القصيرة ورسائل الوسائط المتعددة...) و تشمل صور الإعتداء على المعطيات أي فعل إجرامي يتم من خلال الحواسيب أو الشبكات كعمليات الإختراق و القرصنة ، كما تضم أيضا الجرائم التقليدية التي يتم تنفيذها عبر الإنترنت ومثل تلك الجرائم قد تهدد أمن الدولة و سلامتها المالية و القضايا المحيطة بهذا النوع من الجرائم كثيرة وأبرزها الإختراق أو القرصنة ، نشر الصور الإباحية للأطفال ، ومحاولات إستمالتهم لاستغلالهم جنسيا ، و التجارة غير القانونية كتجارة المخدرات ، طالما تضم انتهاك خصوصية الآخرين عندما يتم استخدام معلومات سرية بشكل غير قانوني.

ولا تقتصر الجرائم الإلكترونية على الأفراد أو مجموعات ، وإنما قد تمتد إلى الصعيد الدولي لتشمل التجسس الإلكتروني و السرقة المالية و غيرها من الجرائم العابرة للحدود و أحيانا توصف الأنشطة التي تتعلق بدولة تستهدف فيها دولة أخرى واحدة على الأقل بأنها تقع في إطار حرب إلكترونية ، و النظام القانوني الدولي يحاول تحميل الفاعلين المسؤولية عن أفعالهم في مثل هذا النوع من الجرائم لذلك قسمنا هذا الفصل إلى مبحثين تناولنا في المبحث الأول الجرائم التي تقع على الأشخاص و الأموال وفي المبحث الثاني: الجرائم الواقعة على الأمن الوطني.

المبحث الأول:الجرائم التي تقع على الأشخاص و الأموال.

يعتبر الحق في الخصوصية شيء متلازم مع الإنسان و الذي يرتبط بصورة مباشرة ، و لا تكاد تتبين في مراجع العصور القديمة أية مكانة لحق الإنسان في حياته العامة أو الخاصة ، فقد خلق الإنسان قبل آلاف السنين في بيئة قاسية لا تعرف الحقوق و لا الواجبات و لا تعترف بهما و مع مرور الزمن بدأت الصراعات القبلية ما دفع بالمجتمعات إلى أن تبحث عن حلول مناسبة لمواجهة هذه الصراعات و الإعتداءات المتتالية فبدأت تظهر معالم الحقوق كالحق في الحياة ، الحق في الأمن، و الإستقرار الأسري ....الخ ، وهكذا إلى أن ظهرت فكرة الحق في حرمة الحياة في القانون الوضعي في الربع الأخير في القرن التاسع عشر، ولازمت التطور التاريخي لهذه الفكرة إتجاهات فقهية و تشريعية و قضائية متباينة حول مضمون هذا الحق و طبيعته القانونية و العناصر المكونة له.

و أدى التطور العلمي و التكنولوجي الحديث إلى اختراع وسائل الإتصال كالهواتف الذكية و أجهزة الإعلام الآلي ووسائل التنصت على المحادثات التليفونية ما أدى إلى اقتحام البريد الإلكتروني وكسر الشيفرات الخاصة به و العبث بالملفات الخاصة بالأفراد ما زاد من احتمال تهديد حرمة الحياة الخاصة ، بالتطفل على أسرارها و إنتهاك حرمتها دون وجه حق لذلك أبرمت عدة إتفاقيات و أصدرت العديد من القوانين حماية لحرمة الحياة الخاصة.

لذلك قسمنا هذا المبحث إلى مطلبين تناولنا في المطلب الأول الجرائم الواقعة على الأشخاص عبر المعطيات الرقمية و في المطلب الثاني الجرائم الواقعة على الأموال عبر المعطيات الرقمية.

المطلب الأول : الجرائم التي تقع على الأشخاص عبر المعطيات الرقمية.

رغم أهمية تحديد مفهوم شامل للحياة الخاصة إلا أنه لم يرد تعريف قانوني لفكرة الحياة ، سواء كان ذلك في الدساتير أو التشريعات العربية كانت منها أو الغربية و ترجع صعوبة عدم إيجاد تعريف إلى أن الفكرة تتسم بالمرونة و تختلف من مجتمع إلى آخر باختلاف القيم الأخلاقية و الدينية و النظام السياسي و الإجتماعي السائد ، لذلك اكتفت النصوص القانونية بفرض حماية لحرمة الحياة الخاصة تاركة أمر التعريف إلى الفقه ، لذلك قسمنا هذا المطلب إلى فرعين تناولنا في الفرع الأول: تعريف الحق في الحياة الخاصة ، والإعتداء على الأشخاص عبر المعطيات الرقمية في الفرع الثاني.

الفرع الأول: تعريف الحق في الحياة الخاصة.

إذا كانت الحياة الخاصة موضوع إهتمام منذ القديم ، فإن هذا الإهتمام قد تزايد في المجتمعات الحديثة ، إذ يشغل موضوع الحياة الخاصة حيزا على الصعيد القانوني فانشغل به الفقه و القضاء الحديث بغية الفصل بين الحياة المهنية للإنسان عن حياته الخاصة و توفير الحماية اللازمة لها لذلك سنتطرق في هذا الفرع إلى التعريف الفقهي للحياة الخاصة ، التعريف الواسع و التعريف الضيق.

أولا- التعريف الواسع:

لقد تعددت التعريفات الفقهية الموسعة حول تعريف الحياة الخاصة و من بينها:

- عرفت الحياة الخاصة بأنها حق الأفراد أو المجتمعات أو المؤسسات في أن يقرروا بأنفسهم زمن و كيفية نقل المعلومات عن أنفسهم إلى الآخرين ، و الخصوصية منظور إليها من علاقة الفرد بالمشاركة الإجتماعية ، وهي إنسحاب الفرد الطوعي و المؤقت من المجتمع العام عبر وسائل مادية أو نفسية[1].

في حين عرف البعض الآخر بأنه الحق في أن يكون الفرد حرا في أن يترك ليعيش كما يريد مع أدنى حد للتدخل الخارجي[2].

ومن أشهر التعريفات للحق في الخصوصية التعريف الذي وضعه معهد القانون الأمريكي و الذي يعرف الخصوصية عن طريق المساس بها ، كل شخص ينتهك بصورة جدية و دون وجه حق ، حق شخص آخر في أن لا تصل أموره و أحواله إلى علم الغير، وأن لا تكون صورته عرضة لأنظار الجمهور يعد مسؤولا أمام المعتدى عليه.

كذلك عرف الفقه المصري الحياة الخاصة بأنها : قطعة غالية من كيان الإنسان لا يمكن إنتزاعها منه و إلا تحول إلى أداة صماء عاجزة عن القدرة على الإبداع الإنساني، فالإنسان بحكم طبيعته له أسراره الشخصية و مشاعره الذاتية و خصائصه المتميزة و لا يمكن للإنسان أن يتمتع بهذه الملامح إلا في مناخ يحفضها و يهيئ لها سبيل البقاء[1].

[1]- صالح جواد كاظم ، مباحث في القانون الدولي، التكنولوجيا الحدسثة و السرية الشخصية ، الطبعة 1،دار الشؤون الثقافية العامة ، بغداد ، سنة 1991، ص136

[2]- أسامة عبد الله قايد ، الحماية الجنائية للحياة الخاصة و بنوك المعلومات ، دون طبعة ، دار النهضة العربية ، مصر ، سنة 1994، ص13

في حين عرف الفقيه **آلان ويستن** الحياة الخاصة قائلا ، تعتبر الحياة الخاصة إنسحابا إراديا و مؤقتا للفرد من المجتمع إلى حالة من العزلة أو الإقتصار على مجموعة صغيرة يألف إليها ، أو حتى وسط مجموعات أكبر لكن يكون في حالة لاتعرف فيها شخصيته و لا يلتزم بالتحفظ[2].

وعرفها الفقيه **مارتن** بأنها ، الحق في الحياة الأسرية و الشخصية و الداخلية و الروحية للشخص عندما يعيش وراء بابه المغلق[3].

أما الهيئة الإستشارية للمجلس الأوروبي نجدها عرفت الحياة الخاصة بأنها القدرة على أن يعيش الإنسان حياته كما يريد مع أقل حد ممكن من التدخل ، ثم تعددت صور تطبيقات الحياة الخاصة و اعتبرتها:

*الحياة العائلية.

*الحياة داخل المنزل الأسرة.

*الكشف عن وقائع غير مفيدة ومن شأنها أن تسبب الحرج.

*إعطاء صورة غير صحيحة عن الفرد.

*ما يتعلق بسلامة الجسم و الشرف و الإعتبار.

*نشر الصور الفوتوغرافية دون إذن الشخص.

*الحماية ضد التجسس.

*الحماية ضد الكشف عن المعلومات الخاصة التي يعلمها أحد الأشخاص.

*الفضولية غير المقبولة و التي تكون دون مبرر.

*الحماية ضد إساءة إستعمال الإتصالات الخاصة.[4]

رغم تعدد التعريفات الفقهية حول مفهوم الحياة الخاصة إلا أن إتجاه آخر من الفقه عرف الحياة الخاصة بشكل ضيق لذلك سنتطرق إلى التعريف الضيق.

2-التعريف الضيق:

حيث عرف بعض الفقهاء الحياة الخاصة بأنها عكس الحياة العامة ، ومن ثمة فالحياة الخاصة هي

---

[1]- عاقلي فضيلة ، الحماية القانونية للحق في حرمة الحياة الخاصة، أطروحة دكتوراه ، جامعة قسنطينة ، الجزائر ، سنة 2012، ص89

[2]- علي أحمد ، حق الخصوصية في القانون الجنائي ، دراسة مقارنة ، المؤسسو الحديثة للكتاب ، طرابلس، سنة 2006، ص119

[3]- مارتن لوسيان، سر الحياة الخاصة ، المجلة الفصلية ، القانون المدني الفرنسي ،سنة1959،ص230.

[4]- أنظر المادتين 3،2من التوصية الصادرة عن الهيئة الإستثمارية للمجلس الأوروبي ، المرقمة 428، الصادرة بتاريخ 23 جانفي 1970.

كل ما ليس له علاقة بالحياة العامة أو هي الحياة العملية التي تجري وقائعها دون خفاء أمام الناس[1].

ومن بين التعريفات الضيقة لمفهوم الحياة الخاصة ما عرفه الفقه الفرنسي بأنه ، ليس لأحد أن يقتحم غيره عالم أسراره و أن يدعه في سكينة ينعم بالألفة دون تطفل عليه[2].

ومن خلال التعريفات السالفة الذكر من تعريفات موسعة و أخرى ضيقة ، فإننا نميل إلى التعريف الذي وضعته كلية الحقوق بجامعة الإسكندرية ، الذي حاول تعريف الحياة الخاصة بأنها ، حق الشخص في أن يحترم الغير كل ما يعد من خصوصياته مادية كانت أو معنوية أو تعلقت بحرياته على أن يتحدد ذلك بمعيار الشخص العادي وفقا للعادات و التقاليد و النظام القانوني القائم في المجتمع و مبادئ الشريعة الإسلامية[3].

وقد أقر الدستور الجزائري كغيره من الدساتير الغربية و العربية حماية الخصوصية للأفراد لذلك نص في:

دستور1963 على بعض الصور دون استعمال مصطلح الحياة الخاصة كحق مستقل و اكتفى بحصر الخصوصية في حرمة السكن و التي نصت على أنه لا يجوز الإعتداء على حرمة المسكن[4].

ثم جاء دستور 1976 وقد نص صراحة على حرمة المواطن الخاصة بحيث لا يجوز انتهاك حرمة حياة المواطن الخاصة ، ولا شرفه ، والقانون يصونها ، ونص على بعض الصور بقوله سرية المراسلات و المواصلات الخاصة بكل أشكالها مضمونة[5].

أما في دستور 1980 فقد نص على أنه لا يجوز انتهاك حرمة حياة المواطن الخاصة و حرمة شرفه و أكد على أن القانون يحميها ، كذلك سرية المراسلات و الإتصالات الخاصة بكل أشكالها مضمونة ، و تضمن الدولة عدم انتهاك حرمة المسكن و تأكيد للحماية و السرية التي يتميز بها الحق في الحياة الخاصة ، إذ نص على أنه يمارس كل واحد جميع حرياته في إطار إحترام الحقوق المعترف بها للغير في الدستور و لاسيما احترام الحق في الشرف و ستر الحياة الخاصة و حرمة الأسرة ...[6].

---

[1]- بن سعيد صبرينة ، حماية الحق في حرمة الحياة الخاصة في عهد التكنولوجيا ، أطروحة دكتوراة ، جامعة باتنة ، الجزائر، 2015،ص18

[2]- ممدوح خليل بحر، حماية الحياة الخاصة في القانون الجنائي المقارن أطروحة دكتوراه ، جامعة القاهرة مكتبة دار الثقافة للنشر و التوزيع، الأردن ،سنة 1996،ص159.

[3]- أنظر المادة الألى من التوصيات الصادرة عن المؤتمربكلية الحقوق المنعقد بجامعة الأسكندرية في 4-5-6يونيو 1987

[4]- أنظر المادة 14من الدستور الجزائري الصادر في 1963.

[5]- أنظر المادة 49من الدستور الجزائري الصادر في 1976.

[6]- أنظر المواد 37-38-60 من الدستور الجزائري الصادر في 1989.

دستور 1996 نص على أنه لا يجوز انتهاك حرمة حياة المواطن الخاصة وهي بكل أشكالها مضمونة ، و تضمن الدولة عدم انتهاك حرمة المسكن بحيث يمارس كل واحد جميع حرياته ، في إطار إحترام الحقوق المعترف بها للغير في الدستور ، لاسيما إحترام الحق في الشرف ، وستر الحياة الخاصة و حماية الأسرة[1].

ومن نفس الدستور تكلفت الدولة بحماية حرمة الحياة الخاصة لمواطنيها واعتبر أن هذه الحرمة بمثابة الحريات الأساسية و حقوق الإنسان مضمونة ، وتكون تراث مشتركا بين الجزائريين الجزائريات ، وواجباتهم أن ينقلوه من جيل إلى جيل كي يحافظوا على سلامته و عدم إنتهاك حرمته و حماية لهذه الحقوق نصت على أنه تضمن الدولة عدم إنتهاك حرمة الإنسان و يحظر أي عنف بدني أو معنوي أو أي مساس بالكرامة.

و أكد المشرع على أنه يعاقب القانون على المخالفات المرتكبة ضد الحقوق والحريات و على كل ما يمس سلامة الإنسان البدنية و المعنوية[2].

كذلك دستور 2008 نص في ديباجة الدستور على الحقوق و الحريات و قد أشار إلى ذلك بأن الحريات الأساسية و حقوق الإنسان و المواطن مضمونة ، و تكون تراثا مشتركا بين جميع الجزائريين و الجزائريات واجبهم أن ينقلوه من جيل إلى جيل كي يحافظوا على سلامته وعدم انتهاك حرمته ، ولضمان هذه الحماية للحقوق و الحريات نص على حق الدفاع الفردي أو عن طريق الجمعية عن الحقوق الأساسية للإنسان و عن الحريات الفردية والجماعية المضمونة ، و نفس الدستور عاقب على إنتهاك تلك الحقوق و الحريات الفردية فالقانون يعاقب على تلك المخالفات المرتكبة ضد الحقوق و الحريات وعلى كل ما يمس سلامة الإنسان البدنية و المعنوية[3].

وهي إشارة إلى الحماية الدستورية التي أولتها الدولة ضد من يتعدى على حريات و حقوق الأفراد سواء كانت ذات طابع بدني أو معنوي ، كما نص الدستور على تلك الحقوق و الحريات المرتبطة بحرمة المسكن و حرمة الحياة الخاصة و حرمة المراسلات و الإتصالات الخاصة و حرية الرأي و التعبير و الحرية السياسية ، وكلها جاءت لتؤكد ضمان الحماية الدستورية لتلك الحقوق و الحريات[4].

---

[1]- أنظر المواد 39-40-63من الدستور الجزائري الصادر في 1996.

[2]- أنظر المواد 32-35 من دستور 1996.

[3]- أنظر المواد 32-33-35من الدستور الجزائري الصادر في 2008.

[4]- أنظر المواد 39 وما بعدها من دستور 2008.

لقد أقر المشرع الجزائري في جل دساتيره بوجوب حماية حرمة الحياة الخاصة فقد اقترنت تلك الحماية بنصوص عقابية عند التعدي على تلك الحرمة ، فمثلا بالرجوع إلى قانون العقوبات نجده نص على الحياة الخاصة في القسم الخامس تحت عنوان الإعتداءات على شرف و اعتبار الأشخاص و على حياتهم الخاصة و إفشاء الأسرار ، فنص على أنه يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات و بغرامة مالية من 50.000 دج إلى 300.000 دج من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأية تقنية كانت و ذلك:

1-بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية ، بغير إذن صاحبها أو رضاه

2-بالتقاط أو تسجيل أو نقل صورة في مكان خاص ، بغير إذن صاحبها أو رضاه.

ونظرا لخطورة الجريمة على حياة الأفراد الخاصة فقد وسع المشرع من دائرة العقاب فأشار إلى الشروع في هذا النوع من الإجرام بنصه على أنه يعاقب على الشروع في ارتكاب الجنحة المشار إليها في هذه المادة بالعقوبات ذاتها المقررة للجريمة التامة[1].

كما يعاقب بنفس العقوبات كل من احتفظ أو وضع أو سمح بأن توضع في متناول الجمهور أو الغير ، أو إستخدم بأية وسيلة كانت التسجيلات أو الصور أو الوثائق المتحصل عليها بواسطة أحد الأفعال السابقة الذكر ، و في نفس السياق إعتبر المشرع بأن الشخص المعنوي هو الآخر يعد مسؤولا إذا ارتكب هذا الجرم وفقا للشروط المنصوص عليها في المادة 51مكرر و تطبق عليه الغرامة حسب الكيفيات المنصوص عليها في المادة 18مكرر[2].

و في القانون المدني إن كان المبدأ المستقر عليه قانونا أن العمل الشخصي المسبب ضررا للغير يرتب المسؤولية ، ويلزم صاحبه بالتعويض حيث نص على أنه كل فعل أيا كان يرتكبه الشخص

بخطئه ، و يسبب ضررا للغير يلزم من كان سببا في حدوثه بالتعويض[3].

فإن المشرع الجزائري رغم عدم نصه صراحة على حرمة الحياة الخاصة في القانون المدني، إلا أنه يمكن إقرار هذا الحق من خلال ما نص عليه لكل من وقع عليه اعتداء غير مشروع في حق من

[1]- أنظر المادة 303 من قانون العقوبات.القانون السابق

[2]- أنظر المادة 303 مكرر 01 من قانون العقوبات.القانون السابق

[3]- أنظر المادة 124من القانون رقم 75-58المؤرخ في 26-09-1975و المتضمن القانون المدني المعدل و المتمم.

الحقوق الملازمة لشخصيته أن يطلب وفق هذا الإعتداء التعويض عما يكون قد لحقه من ضرر[1]، وقد عالج المشرع الخصوصية بصورة مباشرة و هو الحق في الإسم حيث نص على ذلك بقوله لكل من نازعه الغير في إستعمال اسمه دون مبرر ، ومن إنتحل الغير اسمه أن يطلب وفق هذا الإعتداء التعويض عما يكون لحقه من ضرر.

ولقد كفلت القوانين حرمة الحياة الخاصة و أقرت جل الدساتير بخصوصيتها و حرمتها ووضعت عقوبات لمن يقترف إنتهاكا للحرمات ، و نصت على عقوبات جزائية و غرامات مالية و ما يهمنا في موضوع دراستنا هو حماية المراسلات الشخصية خاصة منها المراسلات الإلكترونية و البريدية و البرقية و حتى الهاتفية ...و الحفاظ على سريتها وهو مبدأ دستوري منصوص عليه ، ولاشك أن تعرض الشخص لتهديد في ماله و عرضه و خصوصيته سواء بالمخاطبات المكتوبة أو المنشورة أو المراسلات الإلكترونية يشكل بدوره جريمة إعتداء على الحرية الشخصية.

الفرع الثاني: صور الإعتداء على الأشخاص عبر المعطيات الرقمية.

يعد الحق في الحياة الخاصة من الحقوق الدستورية الملازمة للشخص الطبيعي بصفته الإنسانية كأصل عام ، وهو أساس بنيان كل مجتمع سليم ، ويعد من الحقوق السابقة على وجود الدولة ذاتها لذلك حضت الحياة الخاصة للأفراد بحماية دستورية و قانونية كبيرة في كل دول العالم ، وقد شهدت السنوات الأخيرة استجابة تشريعية على مستويات مختلفة لدواعي هذه الحماية و سايرها القضاء بتجاوب ملحوظ مؤيدا الفقه لما للحياة الخاصة للأفراد من أهمية قصوى على كيان الفرد و المجتمع معا.

وقد شهد العالم اليوم ميلاد تلك الوسائل التكنولوجية الحديثة و التقنيات المتطورة ، مما دفع هذا الإنسان نفسه الذي كان سببا في ظهورها إلى الإنتهاك و الإعتداء على الحياة الخاصة ، بواسطة تلك الأجهزة التي أبدعها عقله و ابتكرتها عبقريته المتفوقة ، فكان لانتشار وسائل الإعلام و الإنترنت و الحسابات الآلية و آلات التصوير الرقمية الأعلى جودة وتقنيات تسجيل ونقل الصورة و الصوت و القنوات الفضائية سببا مباشرا في الإعتداء على الحياة الخاصة ، وخاصة أن المستخدم لم يدرك تدفق المعلومات و الإتصالات عبر الحدود دون أي اعتبار لحدود جغرافية أو سياسية ، فالأفراد يعطون

[1]- أنظر المادة 47من القانون المدني الجزائري القانون السابق.

معلومات لجهات مختلفة قد تكون داخلية أو خارجية وربما جهات ليس لها مكان معروف وهو ما يثير مخاطر إساءة استخدام هذه البيانات خاصة في دول لا تتوفر فيها مستويات الحماية القانونية للبيانات الشخصية ، مما جعلها تشكل خطرا جسيما على سمعة و شرف الأشخاص و انتهاكا صارخا لأسرار الأفراد و حياتهم الداخلية ، مما أدى إلى نشوء أزمة حقيقية في تعريض أسرار الأفراد وخصوصياتهم إلى الإعلان و النشر أو التهديد أو الإبتزاز و الضغط ، كما صارت تلك الأسرار في ظل الإنتشار السريع للوسائل المتطورة للإتصال بضاعة أو سلعة متداولة لدى العامة ، بحيث يستطيع الغير الحصول عليها دون الحصول على إذن مسبق ، مما أثر على الحقوق و الحريات الفردية للإنسان فكان من البديهي أن يتفطن المشرع إلى تجريم تلك الأفعال الماسة بهذا الحق نتيجة للإنتهاكات التي مست بكيان الفرد في ذاته وجوهره ، حيث صار اليوم نقل صورة الشخص حتى ولو في منزله أو تسجيل أحاديثه الخاصة أو السرية في مكالماته الهاتفية من أبرز الأفعال الماسة بهذا الحق ، خصوصا مع تطور وسائل نقل الصورة و الصوت و الرسائل...إلخ.

أولا: جرائم تمس الأشخاص

يشهد عالمنا تحولات جذرية في إطار العلاقات التقليدية السائدة بين الأفراد و انتقالها في إطار التعاملات الورقية إلى التعاملات الإلكترونية في مختلف الفعاليات الإنسانية و الإجتماعية ، والثقافية ، و السياسية ، والعلمية و القانونية ، وقد وفرت الثورة المعلوماتية ودخول شبكة التواصل– الإنترنت– إلى كل بيت ومؤسسة وشركة ، مما دفع بالكثير إلى التعامل بالحاسب الآلي وذلك نظرا للوظائف التي يقوم بها من سرعة في العمل ، وطاقة كبيرة في استيعاب المعلومات ، جعلت منه يشكل خطورة على حياة الأفراد و أسرار حياتهم الشخصية ، و خطورة لا تنحصر فقط في القدرة الفائقة على استيعاب المعلومات في حالة تزويده بهذه المعلومات فحسب بل حتى في عملية استرجاعها واستخراجها ، إذ تكفي ثواني معدودة لكي يقوم بالإطلاع على هذه المعلومات التجوال في ذاكرة الحاسب الآلي ، لكي لا تطلع على معلومات بهذا الكم فحسب ، بسبب قدرة الحاسب على تخزين هذا الكم الهائل عن حياة الإنسان وقدرته في استرجاعها بوقت قياسي و بدقة تفوق التصور.

ولا يقتصر خطر المعلومات التي يتم تسجليها في الحاسب الآلي على السرعة في اسرجاعها ، ومعرفة أكبر قدر ممكن من المعلومات المتكاملة عن حياة الإنسان فقط إنما الأخطر من ذلك هو أن هذه المعلومات بات من الممكن نقلها من مكان إلى آخر في وقت لا يذكر ومهما بعدت المسافات ،

بفضل تقدم وسائل الإتصالات و دخول شبكة الإتصالات العالمية –الأنترنت– إلى الخدمة ، وربما يمتد الأمر إلى الإتجار بهذه المعلومات ، أو استخدامها للابتزاز[1].

ومن جهة أخرى وفر الإعلام الآلي مساحات واسعة لتبادل الآراء و المشاركة ، وقد إشتمل على صحف إلكترونية و منتديات ومدونات فيس بوك[2] و تويتر...ومع تطور البرامج و الوسائل الخاصة بالإنترنت تطورت أساليب الإجرام في هذا الفضاء ، وبات كل من يستخدم الإنترنت عرضة لأن يكون ضحية جريمة تنفذ عن بعد بآلاف الكيلومترات.

هذا الإنتقال إلى العالم الإفتراضي حوّل الجريمة الميدانية إلى جريمة إلكترونية التي هي أخطر من الجرائم الميدانية المباشرة لإختلاف أشكالها و أنواعها و سهولة إختفاء المجرم بعد أداء الجريمة بهدف إلحاق الضرر بالآخرين ، و يختلف الضرر باختلاف الدوافع و الأهداف المراد تحقيقها من الجريمة ، وقد أصدرت العديد من الدول العربية و حتى الغربية منها قوانين خاصة تهدف إلى تنظيم الفضاء الإلكتروني ومن بين هذه القوانين القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال ومكافحتها ، القانون المتعلق بالجرائم الماسة بأنظمة المعالجة للمعطيات ، مشروع قانون النشر الإلكتروني ومسودة الإعلام الإلكتروني[3]، ومن أكثر صور الإعتداء على الأشخاص الطبيعيين أو الاعتباريين وقوعا عبر شبكة الإنترنت جرائم القذف و السب ، جرائم تمس البريد الإلكتروني جرائم انتحال الشخصية ومن بين الجرائم سنتطرق إلى:

1 ـ جريمة القذف و السب

أ ـ جريمة القذف:

تعتبر جريمة القذف من الجرائم الماسة بشرف الأشخاص و اعتبارهم ، و القرآن هو أول من تطرق إلى هذه الجريمة منذ أربعة عشرة قرنا[4]، وهي من جرائم الحدود أي من الجرائم ذات العقوبة المقررة

[1]- محمد حماد مرهج الهيتي ،جرائم الحاسوب ،دراسة تحليلية، دار المناهج للنشر و التوزيع،الطبعة الأولى ،عمان ،2006،ص101

[2]- الموقع الإجتماعي الفيس بوك : يعد هذا الموقع من أكثر المواقع إنتشارا وكان أول من أنشأهذا الموقع هو – مارك زو كربيرغ- الذي كان طالبا في جامعة هارقود فأخترع هذا الموقع لكي يتواصل مع زملائه في الجامعة ،وقد انطلق هذا الموقع في شباط 2004،وبلغ عدد مستخدمي الموقع من العرب 36مليون مستخدم في سنة 2011.و يظم إليه أكثر من مليون عضو شهريا من أنحاء العالم كله،ويهدف الفيس بوك إلى الدخول المبكر في السباق لبناء دليل إلكتروني عالمي ، كما يحتوي على أكبر قدر ممكن من المعلومات و التفاصيل الشخصية ،مثل السير الذاتية ،وأرقام الهواتف و غيرها من سبل الإتصال بالشخص.و لمزيد من التفصيل أنظر شادي ناصف ،فضائح الفيس بوك ،أشهر موقع استخبارتي على شبكة الأنترنت ،سورية ،دار الكتاب العربي ،سنة 2009،ص237.

[3]- فريال حسين ،مقال منشور بعنوان القدف و الذم في شبكات التواصل بجريدة النور، العدد 732،بتاريخ 10-08-2016.

[4] مجدي محب الدين ، القذف و السب ،مصر 2002،ص11.

شرعا[1]، و لم تكن هذه الجريمة معاقبا عليها في صدر الإسلام و إنما عوقب عليها بعد حادثة الإفك و نزول قوله تعالى { وَالَّذِينَ يَرْمُونَ الْمُحْصَنَاتِ ثُمَّ لَمْ يَأْتُوا بِأَرْبَعَةِ شُهَدَاء فَاجْلِدُوهُمْ ثَمَانِينَ جَلْدَةً وَلَا تَقْبَلُوا لَهُمْ شَهَادَةً أَبَدًا وَأُولَئِكَ هُمُ الْفَاسِقُونَ } "[2].وقد نزلت هذه الأية بسبب الحادثة التي اتهمت فيها أم المؤمنين عائشة رضي الله عنها ، وهي من الجرائم التي نهى القرآن و السنة عن إقترافها و كذا الإجماع.

و لحرص الإسلام على منع شيوع الفاحشة بين المؤمنين لقوله تعالى "إِنَّ الَّذِينَ يُحِبُّونَ أَن تَشِيعَ الْفَاحِشَةُ فِي الَّذِينَ آمَنُوا لَهُمْ عَذَابٌ أَلِيمٌ فِي الدُّنْيَا وَالْآخِرَةِ ۚ وَاللَّهُ يَعْلَمُ وَأَنتُمْ لَا تَعْلَمُونَ "[3].

وقد نهى النبي صلى الله عليه و سلم عن القذف بقوله "إجتنبوا السبع الموبقات قالوا وما هن قال : الشرك بالله و السحر ، وقتل النفس التي حرم الله إلا بالحق و أكل الربا و مال اليتيم و التولى يوم الزحف ، وقذف المحصنات المؤمنات الغافلات .و قوله "ص"إن قذف محصنة يحبط عمل مئة سنة.

وبعد اقتحام التكنولوجيا حياة الأشخاص صارت جرائم القذف بصورة متكررة و اعتبرت من أكثر الجرائم شيوعا في نطاق الشبكة المعلوماتية[4] ، لذلك حاول البعض تعريف القذف حيث عرف الدكتور محمود نجيب حسن القذف بأنه إسناد واقعة محددة تستوجب عقاب من نسبت إليه أو احتقاره إسنادا علنيا عمديا يفيد نسبة الأمر إلى الشخص على سبب التوكيد[5].

في حين عرفه البعض الآخر بأنه إسناد وقائع أو أمور محددة تستوجب احتقار من أسندت إليه ، و معاقبته قانونا إذا كانت صحيحة ، ومن أمثلة ذلك إتهام شخص ما بأنه مجنون أو أودع في مصحة عقلية أو إتهام شخص في الشرف أو الإختلاس ، أو الإغتصاب أو الرشوة أو النصب أو غيرها من التهم التي تستوجب معاقبة المتهم قانونا[6].

وفي هذا السياق عرف المشرع المصري القذف بقوله : يعد قاذفا كل من أسند لغيره بواسطة إحدى الطرق المبينة بالمادة 171 من هذا القانون ، أمورا لو كانت صادقة لأوجبت عقاب من أسند إليه

---

[1]- أبو بكر جابر الجزائري منهج المسلم ، كتاب عقائد و آداب و أخلاق عبادات و معاملات ، دار الغد الجديد للنشر و التوزيع ،الطبعة الأولى، ص 24.

[2]- الآية 04 من سورة النور.

[3]-الآية 19 من سورة النور.

[4]- أحمد حسام طه تمام ، الحماية الجنائية لتكنولوجيا الإتصالات ، دراسة مقارنة ،دون طبعة ، دار النهضة العربية ، مصر، 2002،ص53

[5]- محمود نجيب حسن ،شرح قانون العقوبات ، القسم العام ، الطبعة السادسة ، دار النهضة العربية ،1989، ص614

[6]- عبد الفتاح بيومي ، المبادئ العامة في جرائم الصحف ،دار النهضة العربية ، 2008،ص50

بالعقوبات المقررة قانونا ، وأوجبت احتقاره من أهل وطنه[1] ، أما المشرع الجزائري فقد عرف القذف في القسم الخامس تحت عنوان الإعتداء على شرف واعتبار الأشخاص وعلى حياتهم الخاصة وإفشاء الأسرار بأنه يعد قذفا كل إدعاء بواقعة من شأنها المساس بشرف واعتبار الأشخاص أو الهيئة المدعى عليها أو إسناد التهم أو التشكيك إذا قصد به شخص أو هيئة دون ذكر الإسم و لكن كان من الممكن تحديدهما من عبارات الحديث أو الصياح أو التهديد أو الكتابة أو المنشورات أو اللافتات أو الإعلانات موضوع الجريمة[2]، وقد وسع المشرع الجزائري من دائرة التجريم حيث أشار إلى الأعمال التي تكون سببا في القذف كل من يفض أو يتلف رسائل أو مراسلات موجهة إلى الغير و ذلك بسوء نية ،و يعاقب بالحبس 6 أشهر إلى ثلاث و بغرامة من 50.000 دج إلى 300.000 دج كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأية تقنية كانت و ذلك:

1 – بالتقاط أو تسجيل أو نقل المكالمات أو أحاديث خاصة أو سرية ، بغير إذن صاحبها أو رضاه.

2 – بالتقاط أو تسجيل أو نقل صور لشخص في مكان خاص بغير رضا صاحبها.

ويعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذه المادة بالعقوبات المقررة للجريمة التامة[3].

فيما نصت كذلك على أن القذف الموجه إلى رئيس الجمهورية و الهيئات المؤسسة أو الهيئات العمومية قد تكون بأية آلة لبث الصوت أو الصورة أو بأية وسيلة إلكترونية أو معلوماتية أو إعلامية أخرى ، يتبين لنا جليا أن المشرع الجزائري قد نص على جريمة القذف ضمن أحكام قانون العقوبات وقيد هذه الجريمة بعقوبات الحبس و بغرامات مالية ، على عكس ما فعلت بعض التشريعات و التي أشارت إلى جريمة القذف ضمن أحكام قانون الإعلام كالمشرع الفرنسي.

ب جريمة السب:

يعتبر السب خدش شرف الشخص و اعتباره عمدا دون أن يتضمن ذلك إسناد واقعة معينة إليه[4]، وقد عرف المشرع المصري السب في قانون العقوبات : بأنه كل سب لا يشتمل على إسناد واقعة معينة بل

[1]- أنظر الفقرة الأولى من المادة 302من قانون العقوبات المصري المعدل بالقانون رقم 147لسنة 2006

[2]- أنظر المادة 296 من قانون العقوبات الجزائري ، القانون السابق.

[3]- أنظر المادة 303 و303 مكرر من قانون العقوبات الجزائري ، القانون السابق.

[4] محمود نجيب حسن ،شرح قانون العقوبات ، المرجع السابق ،ص614

يتضمن بأي وجه من الوجوه خدشا للشرف أو الإعتبار يعاقب عليه في الأحوال المبينة في المادة 171.

في حين عرف المشرع الجزائري السب بأنه : كل تعبير مشين أو عبارة تتضمن تحقيرا أو قدحا لا ينطوي على إسناد أية واقعة[1].

كذلك التشهير فهو الأخر نوع من أنواع القذف وهو عبارة عن تشويه أو تهديد لسمعة شخص ما بهدف التقليل من قدره في نظر المجتمع و الناس أيا كانت نوعية هذه العلاقة.

وتعتبر جرائم القذف و السب و التشهير من الجرائم الأكثر شيوعا في نطاق شبكة الإنترنت و إن كانت تقليدية إلا أن وقوعها بواسطة هذه الشبكة جعلها توصف ضمن الجرائم المستحدثة ، و تتنوع صور القذف و السب عبر شبكة الإنترنت بتنوع الغرض منها ، و غالبا ما يرتكب من خلال إسناد مادة كتابية أو صوتية أو فيديو صوتي يسئ إلى أحد الأشخاص من شأنه أن ينال من شرفه أو كرامته أو يعرضه إلى بعض الناس و احتقارهم[2]، ومثال على هذا النوع من الجرائم قضية **هني ست** و تتلخص وقائعها أن إمرأة متزوجة كانت تركب دراجة بصحبة شاب أجنبي عنها في الوقت الذي إلتقط أحد المصورين صورة لها وهي على هذا الوضع و نشرها على موقع المجلة التي يعمل بها بعبارة أيام العطل بلا رقيب ، رفعت الزوجة دعوى ضد المصور على أساس أن ما صدر منه يعد تشهير بها من شأنه أن يلحق بها ضررا و أن يحط من قدرها و مكانتها أمام الناس ، حيث أن الصورة تحمل معنى ضمنيا مؤداه أنها قضت العطلة مع هذا الشاب إلى غير ذلك من المعاني التي تسيء إلى سمعتها كزوجة ، وقضت المحكمة لصالح المدعية على أساس أن ما صدر من المدعى عليه يعد قذفا في حقها ، ومن الواضح أن القذف في هذه القضية يعطي بعض مظاهر الحياة الخاصة للمدعية ، وهي الصورة وقضاء أوقات الفراغ[3].

ويتبين أن الجاني يستعمل القواعد العامة لجرائم القذف و السب بعبارات بذيئة تمس و تخدش شرف المجني عليه ، ومهما كانت الوسيلة المعتمدة مع علمه أن ما يقوم به يعد مساسا بسمعة الغير وأن إرادته اتجهت لذلك بالذات ، ومع التطور أصبحت الإنترنت إحدى هذه الوسائل إن لم نقل أكثر رواجا

[1] ـ أنظر المادة 297 من قانون العقوبات الجزائري ، القانون السابق

[2] ـ نبيلة هبة هروال ، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات ، دار الفكر الجامعي ، الإسكندرية ،2007 ، ص65،66

[3] ـ عاقلي فضيلة ،الحماية القانونية للحق في حرمة الحياة الخاصة ، المرجع السابق، ص 53.

فعادة ترسل عبارات السب و القذف عبر البريد الصوتي أو ترسل أو تكتب على صفحات الويب ما يؤدي بكل من يدخل هذا الموقع لمشاهدتها أو الإستماع إليها ، ويتحقق بذلك ركن العلانية الذي تتطلبه الكثير من التشريعات في السب العلني ، و إذا لم يطلع عليها أحد فإنه يمكن تطبيق مواد السب أو القذف غير العلني[1].

وتعتبر شبكة الإنترنت مسرحا غير محدود فهي تتلقى كل ما يدرج عليها دون قيد أو رقابة لذلك تشكل بعض حالات سوء استخدامها حالات سلبية شاذة تؤذي البعض خاصة إذا تم التشهير بهم عبر إيراد معلومات مغلوطة ، حيث يقوم المجرم بنشر معلومات قد تكون سرية أو مضللة أو مغلوطة عن الضحية ، والذي قد يكون فردا أو مجتمع أو مؤسسة تجارية أو سياسية ، تتعدد الوسائل المستخدمة قي هذا النوع من الجرائم لكن في مقدمة قائمة هذه الوسائل موقع على الشبكة يحتوي المعلومات المطلوب نشرها أو إرسال هذه المعلومات عبر القوائم البريدية إلى أعداد كبيرة من المستخدمين[2].

2ـ جرائم الإستغلال الجنسي:

إن كلمة الإستغلال الجنسي في الإنجليزية تجمع بين جنس و استغلال و هي تعني انتزاع شيء ما من شخص ما باستخدام القوة أو التهديدات ، و يعد الإستغلال الجنسي شكلا من أشكال الإستغلال عبر الإنترنت الذي يقوم به المتحرش بتهديد الضحية بنشر معلومات شخصية خاصة إذا لم يقم الضحية بتنفيذ مطالبه الجنسية أو تزويده بصورة غير لائقة عبر الإنترنت أو الهواتف ، وفي المقابل لقد وفرت شبكة الإنترنت أكثر الوسائل فعالية و جاذبية لصناعة و نشر الإباحة ، وقد شجعتها شتى وسائل عرضها من صور و فيديو، وحوارات بوضعها في متناول الجميع ، ولعل هذا يعد أكبر الجوانب السلبية للإنترنت خاصة في مجتمع محافظ على دينه و تقاليده كمجتمعنا الإسلامي ، وقد ركز أحد الباحثين على صناعة و نشر الإباحة عند تقسيمه لجرائم الإنترنت مما يحرض القاصرين على أنشطة جنسية غير مشروعة ، و صناعة الإباحة من أشهر الصناعات الحالية و أكثر رواجا خاصة تلك التي تستهدف أو تستخدم الأطفال ، ولقد تم إدانة مجرمين في أكثر من مائتي جريمة في الولايات المتحدة الأمريكية خلال سنة 1998تتعلق هذه الجرائم بتغرير الأطفال في أعمال إباحية أو نشر مواقع تعرض مشاهد إباحية للأطفال و أن هذه الجرائم تشكل طائفة تشمل تحريض القاصرين على أنشطة جنسية

[1] ـ صغير يوسف ،الجريمة المرتكبة عبر الانترنت ، الجريمة المرتكبة عبر الانترنت ، مذكرة ماجستير في القانون تخصص ، القانون الدولي للأعمال ، جامعة تيزي وزو ، 2013، ص53.
[2] ـ صغير يوسف ، المرجع نفسه، ص 54.

غير مشروعة و إفسادهم بأنشطة جنسية عبر الوسائل الإلكترونية ، وإغواء أو محاولة إغواء القاصرين لإرتكاب أنشطة جنسية غير مشروعة و التحرش الجنسي بالقاصرين عبر الكمبيوتر و الوسائل التقنية نشر و تسهيل المواد الفاحشة عبر الإنترنت بوجه عام و للقاصرين تحديدا ، ونشر الفحش و المساس بالحياء ـ هتك العرض بالنظر ـ عبر الإنترنت و تصوير أو إضهار القاصرين ضمن أنشطة جنسية ، و استخدام الإنترنت لترويج الدعارة بصورة قسرية أو الإغواء أو نشر المواد الفاحشة التي تستهدف استغلال عوامل الضغط و الإنحراف لدى المستخدمين ، و الحصول على الصورة و الهويات بطريقة غير مشروعة لاستغلالها في أنشطة جنسية ، و بإمعان النظر في هذه الوصائف نجد أنها تجتمع جميعا تحت صورة واحدة هي استغلال الإنترنت و الكمبيوتر لترويج الدعارة أو إثارة الفحش و استغلال الأطفال و القصر في أنشطة جنسية مشروعة و الأكثر من ذلك أن الصور الخليعة التي تظهر على شاشة الكمبيوتر هي نوع من الدعاية المجانية لهذه المواقع التي تتبع الرذيلة و تحقق ملايين الدولارات من الأرباح و تستهدف نشر البغاء في المجتمعات.

و يلجأ هؤلاء لاستغلال هذه الفئة الضعيفة (فئة الأطفال و القصر) من المجتمع من خلال:

أ ــ عرض الصور و الأفلام المخلة بالآداب العامة:

لقد أصبح الترويج للمعطيات الإباحية لغرض إشباع الغرائز الجنسية أو لتحقيق مكاسب تجارية أمرا مألوفا في الإنترنت و التي يكون الطفل فيها محلا للإعتداء من ذلك عرض صور و أفلام إباحية تتضمن صور الأطفال القصر أو صور وأفلام لعمليات التعذيب الجنسي و الأعضاء الجنسية و عمليات الإغتصاب أو العمليات الجنسية التي تمارس على الأطفال القاصرين و على الأخص الذين تتراوح أعمارهم من أربع إلى ست سنوات[1]، حيث اكتشفت الشرطة البريطانية عام 1995شبكة تقوم بعرض الصور الخليعة للأطفال تقدر سعتها ب 50 أسطوانية إضافة إلى عناوين بعض الأشخاص المشغوفين بالأطفال و الذي كان معظمهم من جنوب إفريقيا و ألمانيا ، وسنغافورة ، ولم يقتصر الأمر عند هذا الحد بل تجاوزه إلى استغلال الأطفال لإجراء محاورات أو محادثات عبر ما يعرف بغرف الحوار لتبادل المحادثات الجنسية من ذلك ما كان يعرف في الولايات المتحدة الأمريكية بخط الإتصال ، و الذي كان يتم عن طريق الهاتف قبل أن ينتقل إلى الإنترنت ، و ذلك بتسخير مجموعة من الفتيات القاصرات لتكون على الطرف الآخر من المحادثة ، و خطورة الأمر تكمن فيما ينطوي عليه

[1] ــ رشا خليل ،جرائم الاستغلال الجنسي للأطفال عبر الإنترنت ، جامعة ديالى ، مجلة الفتح العدد 27 ، العراق 2006، ص 10.

تبادل المحادثات الجنسية من الإثارة للشهوات و الغرائز الجنسية ، وما يؤول إليه الأمر من التحريض على البغاء[1].

ونشير في هذا الصدد إلى العمليات الناجحة التي قام بها الإنتربول و التي استمرت نحو عشرة أيام انتهت ظهيرة يوم 2007.11.25 بإلقاء القبض على سفاح الأطفال الذي قام باغتصاب نحو 200 طفل خلال أربع سنوات و قد سميت العملية Vico ،حيث كان السفاح يقوم عند الإعتداء على ضحاياه بتصوير العمليات و يقوم بعرضها على موقعه الخاص على شبكة الإنترنت ، ولقد أشارت في هذا الإطار إحدى المنظمات الخيرية المعنية بشؤون الطفل أن جرائم الجنس ضد الأطفال تزايدت 15 مرة منذ 1988 و أن الإنترنت المتاحة على الهواتف المحمولة التي تتمتع بإمكانيات تصوير الفيديو قد يزيد الأمر سوءا و أن الشبكة المعلوماتية مسؤولية لحد كبير عن الإرتفاع الهائل في الجرائم الإباحية ضد الأطفال[2].

ب التحريض على الفسق و الفجور:

يتم التحريض عن طريق تهييج شعور الفاعل و دفعه إلى ارتكاب أفعال الفسق و الفجور أي التأثير في نفس من يوجه إليه امر ارتكاب أفعال البغاء و يتم التحريض إبتداء عن طريق البريد الإلكتروني ، حيث يتم من خلاله نقل المواد الإباحية أو الفاحشة من صور أو كتابة أو رموز إلى شخص معين أو إلى عدد محدد من الناس ، أو تنظيم إجتمتعات تقوم على علاقات أو ممارسات جنسية يساهم فيها أو يحضرها طفل دون أن يساهم الصغير في هذه اللقاءات إذ يكفي بمجرد المشاهدة ، وعليه فإن أفعال التحريض الموجهة إلى الأطفال و التي يمكن استخدامها في الإنترنت تتخذ لها الصور الآتية:

ـ التحريض عن طريق المحادثات الشفوية أو المكتوبة ، والتي تحض على ارتكاب أفعال الفسق و الفجور و غالبا ما تتم عن طريق غرف الحوار و الدردشة.

ـ التحريض عن طريق وضع مواقع في الإنترنت تعمل على الترويج لتجارة الأجنة (الأطفال و النساء) و بيوت الدعارة فتقوم بتزويد الشخص بمعلومات عن أماكن بيوت الدعارة و صور اللواتي يمارسن الجنس معهن أو بأفلام تظهر ما تفعله العاهرات في التفريط بأعراضهن و كيف يتلذذن بالرجال أو

[1] ـ رشا خليل ،جرائم الإستغلال الجنسي للأطفال عبر الإنترنت ، المرجع السابق ، ص10.
[2] ـ أنظر خمايسية حفيظة ، المرجع السابق،ص 51.

يتلذذ الرجال بهن وكل ما فيه من الإغراء بالعهر خروجا على عاطفة الحياء و هدما لقواعد الآداب العامة.

ـ التحريض عن طريق الرموز أو الرسوم و التي قد تكون دعوى صريحة أو تحمل في طياتها مما لا يدع مجالا للشك معنى التحريض على الفسق و الفجور و يترتب على التعريض المتكرر للمواد الإباحية و الفاحشة قيام شهوة متنامية حتى يصبح إدمانا مع توفير جيل مستمر و متناسق للإثارة[1].

وقد تفاقم الأمر حول موضوع الإستغلال الجنسي للأطفال عبر الإنترنت مما دعى أغلب الدول لمكافحة هذه الظاهرة الإجرامية ، فمثلا قبضت السلطات البريطانية على أكثر من 600 شخص في إطار تحقيق دام ستة أشهر لملاحقة أشخاص يشتبه في اطلاعهم على صور إعتداءات جنسية على أطفال في الإنترنت ، و قالت الوكالة الوطنية لمكافحة الجريمة أن 660 شخصا قبض عليهم بينهم أطباء و معلمون و قادة كشافة و عاملون في الرعاية و ضباط سابقون ، و أضافت الوكالة في التحقيق تمكنا من حماية 400 طفل من الإعتداءات الجنسية المحتملة ، و تم القبض عليهم في مختلف مناطق بريطانيا ، وأغلب المقبوض عليهم لم تكن لهم سوابق مسجلة لدى الشرطة ، وأوضحت الوكالة أن 39 من المقبوض عليهم سبقت إدانتهم بالإعتداء الجنسي وقالت **كليرليلي** مسؤولة هيئة سلامة الأطفال على الإنترنت أن هذه العملية أنقذت أطفالا من الإعتداءات الجنسية ، وأضافت أنه على صناعة الإنترنت أن تبتكر وسائل لحجب مثل هذه الصور الشنيعة و التي تؤخذ على حساب معاناة الأطفال العزل بعضهم لم يصل سن الذهاب إلى المدرسة.

3ـ جريمة إنتحال الشخصية:

يقصد بانتحال الشخصية ما يعمد إليه الجاني من استخدام شخصية آخر للإستفادة من سمعته مثلا أو ماله أو صلاحياته حتى أن البعض من المختصين في أمن المعلومات سماها بجريمة الألفية الجديدة و ذلك نظرا لسرعة إنتشار ارتكابها خاصة في الأوساط التجارية[2]، كذلك يعتبر شكل من أشكال سرقة الهوية على الإنترنت باستخدام بريد إلكتروني مغشوش لإغراء المتلقين من أجل أن يتصلوا بمواقع إلكترونية إحتيالية ، وذلك بغية خداعهم و جعلهم يفشون بياناتهم الشخصية و المالية مثل أرقام

[1] ـ رشا خليل ،جرائم الاستغلال الجنسي للأطفال عبر الإنترنت ، المرجع السابق ،ص 11

[2] عمرو عيسى الفقى ، الجريمة المعلوماتية ،جرائم الحاسوب الآلي و الانترنت في مصر و الدول العربية،المكتب الجامعي الحديث ، الإسكندرية ،2006،ص 102

بطاقات الإئتمان و كلمات السر و أرقام الضمان الإجتماعي ، و مثال على هذه العملية عندما يستلم أحد الأشخاص رسالة إلكترونية تتضمن طريقة إتصال بمواقع إلكترونية ، فعندما ينقر المستلم على هذا الربط (Link) فإنه يدخل إلى الموقع e– baya ولكن هذا الموقع يكون مزيف إلا أنه و بالتفحص الجيد يمكن أن يظهر عنوان الصفحة مختلف عن الموقع الحقيقي ، ولكن الضحية لن يلاحظ هذا الفرق و سوف يقوم بإعطاء معلومات عنه ، مثل كلمة السر و عنوان البريد ومن أمثلة هذا الأسلوب أن شخص يدعى **ويليام جاكسون** إستلم رسالة إلكترونية تظهر أنها من موقع paypal ومن وهذه الرسالة تحذره بأن حسابه سوف يغلق ما لم يجدده بمعلومات مالية محددة و كان يوجد في هذه الرسالة رابط Link بالموقع الذي يستطيع من خلاله تجديد هذه المعلومات ، وقد قام جاكسون بإدخال أرقام بطاقة الائتمان و الحسابات المصرفية و أرقام الضمان الإجتماعي الخاص به ، ومعلومات شخصية أخرى و انتهت هذه العملية الإحتيالية بخسارة بمئات الدولارات[1] .

لذلك فهذا السبب الوجيه يدعوا للإهتمام بخصوصية و سرية المعلومات الشخصية للمستفيدين على شبكة الإنترنت وتتخذ جريمة إنتحال الشخصية عبر الإنترنت أحد الوجهين التاليين إنتحال شخصية الفرد وانتحال شخصية المواقع.

أ ـ إنتحال شخصية الفرد:

تعد جرائم إنتحال شخصية الآخرين من الجرائم القديمة ، إلا أن التنامي المتزايد لشبكة الإنترنت أعطى للمجرمين قدرة أكبر على جمع المعلومات الشخصية المطلوبة عن الضحية ، والإستفادة منها في ارتكاب جرائمهم ، فتنتشر على شبكة الإنترنت من الإعلانات المشبوهة والتي تداعب عادة غريزة الطبع الإنساني في محاولة الإستيلاء على معلومات إختيارية من الضحية ، فهناك مثلا إعلان عن جائزة ضخمة يكسبها من يساهم بملغ رمزي لجهة خيرية ، وهذا يتطلب بطبيعة الحال الإفصاح عن بعض المعلومات الشخصية كالإسم ، والعنوان والأهم رقم بطاقة الإئتمان لخصم المبلغ الرمزي لصالح الجهة الخيرية ، وبالرغم من أن مثل هذا الإعلان يمثل عملية نصب واحتيال واضحة إلا انه ليس من المستبعد أن يقع ضحيته الكثير من مستخدمي الإنترنت ويمكن أن تؤدي جريمة إنتحال الشخصية إلى الإستيلاء على رصيده البنكي أو السحب من بطاقته الإئتمانية أو حتى الإساءة إلى سمعة الضحية.

ب ـ إنتحال شخصية المواقع:

[1] ـ محمد طارق عبد الرؤوف ،جريمة الإحتيال عبر الإنترنت ،منشورات الحلبي الحقوقية ،لبنان ،2011، ص46

ومع أن هذا الأسلوب يعد حديثا نسبيا إلا أنه أشد خطورة وأكثر صعوبة في اكتشافه من إنتحال شخصية الأفراد ، حيث يمكن تنفيذ هذا الأسلوب حتى مع المواقع التي يتم الإتصال بها من خلال نظم الإتصال الأمني ، حيث يمكن وبسهولة إختراق مثل هذا الحاجز الأمني وتتم عملية الإنتحال بهجوم يشنه المجرم على الموقع للسيطرة عليه ومن ثم يقوم المجرم بتحويل موقع مقدمي الخدمة للمشهورين ثم يقوم بتركيب البرنامج الخاص به هناك مما يؤدي إلى توجه أي شخص إلى موقعه بمجرد كتابة إسم الموقع للمشهور ، ويتوقع أن يكثر إستخدام أسلوب إنتحال شخصية المواقع في المستقبل نظرا لصعوبة إكتشافها ، والمحاضر الأمنية والمخالفات النظامية والشرعية واضحة سواءا ما كان منها قاصرا على إنتحال شخصية الأفراد والمواقع[1].

ومثال على ذلك ورد بلاغ إلى إدارة جرائم الحاسوب بوزارة الداخلية المصرية عبر البريد الإلكتروني من إحدى شركات مكافحة جرائم الإحتيال العالمية التي تمثل قانون أحد البنوك البريطانية الكبرى بوجود موقع مزيف على الإنترنت لهذا الموقع البريطاني يستخدم لخداع عملاء البنك وجمع المعلومات عنهم والإستيلاء على أرصدتهم بطريقة إحتيالية ونتيجة البحث والمتابعة تم إلقاء القبض على طالب بكلية الهندسة مقيم بالإسماعيلية لإنشائه هذا الموقع المزيف الذي يحمل نفس مواصفات الموقع الرئيسي للبنك ، وقد استطاع الطالب خداع عملاء البنك في الخارج كما استطاع بمعاونة أشخاص مقيمة في أوروبا الشرقية وروسيا تحويل أرصدة بعض العملاء عن طريق شركات تحويل الأموال وتقسيمها فيما بينهم وقد إرتكب هذا الطالب جريمته عن طريق مقهى إنترنت عائدة لوالده في الإسماعيلية.

ولقد حفظت الشريعة السماوية والأنظمة الوضعية الحقوق الشخصية و صانت الملكية الفردية وجعل التعدي عليها أمر محضورا شرعا و معاقب عليه قانونا وفي انتحال شخصية الآخرين تعدي صارخا على حقوقهم و انتهاكا لملكياتهم التي صانها الشرع لهم ، كما أنه يترتب على انتحال شخصية الآخرين أضرار متنوعة قد تلحق بهم و تتفاوت هذه الأضرار بتفاوت نتيجة الفعل المشروع على مقتنيات مادية للمجني عليه ومهما كان حجم الأضرار الناتجة عن هذا الفعل النظامي ، فإن المجني عليه لابد أن يتضرر من هذا الفعل ، وخاصة أن الهدف الغالب من انتحال الشخصية لن يكون بحسن نية ، أو لخدمة شخص أخر ، كما تتفق الشريعة مع القوانين الوضعية في جعل الإنسان

[1] ـ محمد بن عبد الله بن علي المنشاوي ، جرائم الانترنت في المجتمع السعودي ، د ن ت ، الرياض 2003 ، ص 54.

مسؤولا عن كل فعل ضار بغيره و لاشك أن انتحال شخصية الأفراد أو المواقع مضر بأصحابها الأساسيين و لذلك فهي جريمة قانونية و مخالفة شرعية[1].

ثانيا: جرائم تمس الممتلكات الشخصية إلكترونيا.

1ـ الإعتداء على البريد الإلكتروني:

في ظل التطورات الهائلة في مجال الإتصال و الشبكة المعلوماتية الدولية التي يشهدها العالم و التي أحدثت و بحسب بعض الخبراء ثورة حقيقية في جميع مناحي الحياة وقد أصبحت من أهم وسائل التعامل اليومي بين المؤسسات و الأفراد بمختلف الطبقات ، هذا التطور الكبير أسهم أيضا في ظهور الكثير من الجرائم و ذلك باستخدام شبكات الإتصالات الحديثة مثل الإنترنت لوحات الإعلانات غرف الدردشة ورسائل البريد الالكتروني.

فالبريد الإلكتروني يعتبر من الخدمات المهمة التي تقدمها الشبكة المعلوماتية وهو شكل من أشكال الإتصال الإلكتروني يسمح لمستخدمي الإنترنت بتبادل الرسائل بشكل فوري ، ونظرا لصعوبة إيجاد رقابة المحكمة على الشبكة المعلوماتية فإنه لا يوجد ضوابط تحكم هذا البريد مما نتج عنه ظهور بعض الإستخدامات غير المشروعة للبريد الإلكتروني[2].

ـ تعريف البريد الإلكتروني:

لقد عرف البعض البريد الإلكتروني بأنه: تلك المستندات التي يتم إرسالها أو استلامها وفق نظام إتصالات بريد الكتروني*، و تتضمن ملحوظات ذات طابع حقيقي ، و يمكنه استصحاب مرفقات معالجة الكلمات و أية مستندات أخرى يتم إرسالها رفقة الرسالة ذاتها*.

وقد عرفه البعض الآخر بأنه مكنة التبادل غير المتزامن للرسائل بين أجهزة الحاسب الآلي.
في حين عرفه البعض الآخر بأنه طريقة تسمح بتبادل الرسائل المكتوبة بين الأجهزة المتصلة بشبكة المعلومات[3].

---

[1] ـ محمد بن عبد الله بن على المنشاوي ، المرجع نفسه ،ص 55

[2] ـ خالد ممدوح ابراهيم ، الجرائم المعلوماتية ، دار الفكر الجامعي ، الإسكندرية ، ط1 ،2009، ص283

[3] ـ العوضي عبد الهادي ، الجوانب القانونية للبريد الالكتروني ، دار النهضة العربية ، د ط ،القاهرة ،ص12

*ـ نشأة البريد الإلكتروني : يعتبر راي توملينسون هو مخترع البريد الإلكتروني و الذي أغفله التاريخ كأحد أهم الشخصيات التي ابتكرت أهم وسيلة من وسائل الاتصالات الرقمية ، وكانت البداية عند ما كان هذا الأخير يعمل كموظف بسيط في شركة "بي بي أن" الأمريكية بعد أن تخرج في 1965 من معهد " ماساشوستس "الشهير للتكنولوجيا ،وقد كلفت وزارة الدفاع الأمريكية شركة التي يعمل بها لبناء شبكة اتصالات

وقد عرفت اللجنة العامة للمصطلحات في فرنسا البريد الإلكتروني بأنه : وثيقة معلوماتية تحررها أو يرسلها أو يطلع عليها المستخدم عن طريق الإتصال بشبكة معلوماتية[1].

2- إختراق البريد الإلكتروني و انتهاك السرية:

إذا كانت أغلب الدساتير المعاصرة قد ركزت اهتمامها على الإعتراف للفرد بحقه في سرية المراسلات فإن بعض الوثائق الدستورية تميزت بتسجيلها مبدأ يقرر إحاطة المراسلات لحماية جنائية وكمثال على هذه الدساتير الدستور المصري الصادر في 1971 الذي نص على الحق في سرية المراسلات بل أنه جعل من انتهاك هذا الحق جريمة واعتبر أن الحق في سرية المراسلات هو أحد عناصر الحق في الحياة الخاصة ، حتى بعض القوانين أولت اهتماما بالحماية الجنائية للمراسلات وأقر قانون العقوبات الفرنسي حماية الحق في سرية المراسلات إذ تقرر المادة 187 منه عقوبة الحبس من ثلاثة أشهر إلى خمس سنوات وبغرامة مالية لكل موظف في الحكومة أو مصلحة البريد يستولي أو يفتح عن قصد خطاب عهد به إلى مصلحة البريد أو سهل للغير فعل ذلك ، كما أن الحماية الجنائية للحق في سرية المراسلات في فرنسا إمتد ليشمل المكالمات الهاتفية ، إذ أن كل موظف بمصلحة الهاتف والتلغرافات والبريد خاضع للمحافظة على سرية المراسلات والإتصالات الهاتفية وكافة أنواع الإتصالات الحديثة ، واعتبر عدم الإلتزام بذلك مخالفة قانونية يعاقب عليها القانون[2]، ويكفل سريتها فلا يجوز مراقبتها أو انتهاك سريتها أو الإطلاع عليها إلا في الأحوال المبينة في القانون وذلك ينطبق أيضا على وسائل الإتصال الإلكترونية ومنها البريد الإلكتروني.

ووفقا للقانون الفرنسي فإن البريد الإلكتروني يخضع للحماية التي يفرضها القانون على الحق في الخصوصية ، حيث نجد أن نص المادة 02 الفقرة 02 من القانون المؤرخ ف 03،09،1986 تنص على أنه "يعد اتصال سمعي مرئي كل إجراء إتصالي أو إشارة أو إشارات مكتوبة أو أصوات أو رسائل

آريانت ARPANET، والهدف منها ربط كافة المعهد العلمية و الجامعات في الولايات المتحدة الامريكية لتبقى على تواصل فوري ،وقد عمل توملیسون على إعداد برنامج حاسوب بسيط لكتابة الرسائل أطلق عليهSNDMSG و الهدف منه أن يكتب احد المواطنين رسالة و يتركها للآخرين لكي يطلعوا عليها و ذلك ضمن ملف مثبت على جهاز الحاسوب ، وكذلك تدوين الملاحظات و المهام المنجزة أو التي يجب إنجازها بحيث يتمكن الموظف الذي سيعمل لاحقا على جهاز الحاسوب نفسه من معرفة ما أنجز من أعمال ، وما يجب عليه القيام به دون حاجة لعقد لقاءات متكررة بين الموظفين .و في عام 1981 ظهر أول حاسوب شخصي في العالم كان خلالها توملیسون يصمم برنامج CYPNET الخاص بنقل و تبادل الملفات بين أجهزة الحاسوب المختلفة المرتبطة بشبكة آربانت . وما كاد توملیتسون يفرغ من برنامج CYPNET الخاص بنقل الملفات عبر أجهزة الحاسوب المرتبطة بشبكة آربانت ، حتى لمعت في ذهنه فكرة ربط برنامج CYPNETو برنامج SNDMSG خالد ممدوح إبراهيم ، أمن مراسلات البريد الالكتروني ، المرجع السابق،ص 55

[1] ـ عبد الله بن ناصر، الحماية الجنائية للبريد الالكتروني ،دراسة تأصيلية مقارنة ،جامعة نايف العربية للعلوم الأمنية ، الرياض ، سنة 2012،ص21.

[2] ـ محمد قاسم النصر ، الحق في سرية المراسلات في بعض النظم ، 2006 ، ص 95.

من كافة الأشكال التي لا تكون هيئة إتصال خاص" وفي نفس السياق نصت المادة 226 الفقرة 10 من قانون العقوبات الجديد على أنه: كل فعل أرتكب بسوء نية بقصد قطع أو تحويل أو استخدام أو نشر عن الإتصالات الخاصة ، المرسلة أو المستقبلة بوسيلة إتصالات أو بواسطة إعداد أجهزة مهمتها ارتكاب هذه الأفعال.

لذلك يعد الإختراق من أكثر الجرائم المعلوماتية شيوعا بواسطته يتم إختراق البريد الالكتروني و الإستيلاء على محتوياته ، أو سرقة ما فيه ، أو التجسس أو تدمير الأنظمة المعلوماتية بعدة طرق ووسائل يستخدمها القراصنة ، والإختراق هنا محاولة الوصول إلى أنظمة أو شبكات أفراد أو منشآت بمساعدة بعض البرامج المختصة في سرقة وفك كلمات السر وتصريحات الدخول عن طريق مهارتهم وخبراتهم[1] ، وفي هذا السياق تم اختراق **ياهو** البريد الإلكتروني ، حيث أكدت **ياهو** تعرضها للإعتداء عن طريق أنظمة إحدى شبكات القرصنة التي استهدفت اختراق حسابات البريد الإلكتروني الخاصة بمرتادي الموقع وذلك عبر الإستيلاء على البيانات الشخصية المتعلقة بالدخول على الحساب ، وأشارت **ياهو** إلى أن عدد المستخدمين الذين تعرضت حساباتهم للقرصنة تجاوز الـ 400 ألف شخص ، مؤكدة شروعها في التصدي للعيب التقني الذي استغله القراصنة في السطو على حسابات هؤلاء المستخدمين ، وأكدت ياهو أيضا محاولته التصدي لأي إختراق مماثل في المستقبل قد يتعرض له مستخدمون آخرون دون الإشارة إلى الأشخاص أو الهيئات التي يمكن أن تعرضها لاختراق مماثل في المرحلة المقبلة ، وإن كانت قد ألمحت إلى انه ليس من المستبعد وقوع اختراق مماثل لمتضررين آخرين ، وكانت مجموعة من المتسللين قد نشرت في السابق حسابات وكلمات مرور خاصة بمئات الآلاف من المستخدمين على موقع الكتروني وجاءت سرقت الحسابات في أعقاب إنتهاك تم الإبلاغ عنه من موقع لينكد أن للربط بين الشركات والذي أدى إلى كشف كلمات المرور الخاصة بنحو مليون مشترك[2].

يرتبط الاختراق بشبكة الانترنت التي تعد وسيلة لاختراق الأجهزة والشبكات المعلوماتية بهدف التأثير في أداء أجهزة الحاسب الآلي وتعطيلها ، وتدمير البيانات والنظم والتعدي غلى الممتلكات وبث برمجيات خبيثة تقوم بتدمير معطيات الحاسب ونظم التشغيل ، أو التعدي على البيانات والمعلومات

[1] ـ القاسم محمد بن عبد الله ، أساسيات أمن المعلومات ، مكتبة الملك فهد الوطنية ، ط2 ، الرياض ، 2008 ، ص 32.
[2] ـ مقال منشور على الموقع التالي www.gnume.com وقد تم الإطلاع على الموقع بتاريخ 2017/05/07.

الشخصية ، واستخدام اسم النطاق وغيرها من الأفعال التي تتم بواسطة الإختراق ويعني إختراق البريد الالكتروني الدخول غير المشروع إلى المعلومات والبيانات المرسلة عن طريق البريد الالكتروني.

يعتمد الاختراق على السيطرة عن بعد و هي لا تتم إلا بوجود عاملين أساسين هما:

1. البرنامج المسيطر ويعرف بالعميل.

2. الخادم الذي يقوم بتسهيل عملية الاختراق و عادة ما يتم إختراق البريد الالكتروني من خلال بعض البرامج منها أحصنة طروادة : ويكون البريد الالكتروني و المواقع المشبوهة التي تستخدمها و يمكن صررها في إمكان التجسس و التعرف على كلمات العبور وتدمير الملفات وهذا البرنامج لا يمكن صاحب الجهاز من ملاحظة وجود دخيل على الجهاز في غيابه وكذلك فان البرنامج لا يمكن كشفه بواسطة البرامج المتخصصة في كشف الفيروسات وعليه فإنه لا يمكن في الأغلب الأعم من الأحوال معرفة وجود مثل هذا البرامج المتخصصة في كشف الفيروسات وعليه فإنه لا يمكن في الأغلب الأعم من الأحوال معرفة وجود مثل هذا البرنامج على جهاز الكمبيوتر ، أو الإحساس بوجوده للقضاء عليه.

الدخول الشخصي: ويتم الإختلراق عن طريق دخول شخص على جهاز شخص آخر أو ربط جهاز بين بعضها البعض عن طريق المودام ، وباستخدام بروتوكول IP/TCP وبذلك يمكن السيطرة على الجهاز الآخر بطريقة أو أكثر إما لتخفي أو بطرق ظاهرة ، ويمكن إرسال ملفات أو تحميل ملفات وإجراء محادثة أو كتابة أو مسح معلومات.

الكوكي: يمنك تحقيق الاختراق عن طريق الكوكي ، وهو ملف صغير تضعه بعض المواقع التي يزورها المستخدم على قرصه الصلب ، والهدف منه في الأساس تجاري ، ولكنه يساء استخدامه من قبل المبرمجين المتمرسين بلغة إلحاق JAFA التي لديهم القدرة على التعمق أكثر داخل الأجهزة والحصول على معلومات أكثر عن المستخدم[1].

3 جريمة انتهاك مراسلات البريد الالكتروني: تعد حرمة الرسائل وسريتها من بين بالغ الأهمية فقد كرست الاتفاقيات الدولية بنصوص صريحة ، ورفعته الدساتير والتشريعات الوطنية الى مصاف الحقوق الدستورية حيث قررت عدم جواز مراقبة المراسلات أو مصادرتها أو إفشاء سريتها إلا في

[1] ـ عبد الله بن ناصر، الحماية الجنائية للبريد الإلكتروني ، المرجع السابق ، ص 56 وما بعدها.

الأحوال والحدود المبينة في القانون[1] ، وانتهاك مراسلات البريد الالكتروني من التصرفات الجرمية الجديرة بالاهتمام القانوني والحقوق على اعتبار أن هذا النوع من الانتهاك يتصل بالمعطيات الشخصية التي تندرج ضمن الحريات الضرورية لكل إنسان هذا النوع من الجرائم التي أصبحت شائعة في عدد من البلدان يتم تنفيذها بواسطة وسائل تقنية المعلومات وتنفيذها بهذا الشكل بعد من الظواهر الاجرامية المستجدة والتي تتطلب أشخاص يتمتعون بمؤهلات معينة ويمتلكون وسائل تقنية المعلومات اللازمة لارتكابها ، إن الإعتداء على مراسلات البريد الالكتروني سلوك ينطوي على خطورة كبيرة فيما يتعلق بسرية المعطيات الرقمية والحياة السرية للأشخاص داخل المجتمع الذي يعيشون فيه ، لا سيما وأن هذه الظاهرة الإجرامية المستجدة لا زالت غير مشمولة بالحماية الدستورية والقانونية اللازمة في عدد من البلدان على عكس دول أخرى كالجزائر والمغرب وفرنسا ، لذلك نص الدستور الجزائري في آخر تعديل له 2016 على عدم انتهاك سرية الإتصالات الشخصية واعتبرت حرية المراسلات من الحريات الأساسية والضرورية لكل شخص ، كذلك نص دستور المملكة المغربية في الباب الخاص بالحريات والحقوق على أنه لا تنتهك سرية الإتصالات الشخصية ، كيف ما كان شكلها ولا يمكن الترخيص بالإطلاع على مضمونها أو نشرها ، كلها أو بعضها ، أو بالإستعمال ضد أي كان إلا بأمر قضائي ، ووفق الشروط و الكيفيات التي ينص عليها القانون[2].

4 ـ أهداف إختراق البريد الإلكتروني:

تتعدد الأهداف من وراء اختراق البريد الإلكتروني ولعل من أبرز هذه الأهداف ما يلي:

1 ـ التجسس: سواء على دول أو منظمات أو هيئات أو مؤسسات أو أفراد ، ولقد جاء في تقرير لصحيفة **الصنداي تايمز** البريطانية أن **إسرائيل** تتجسس على **الو م أ** وأن أجهزة الموساد استطاعت اختراق البيت الأبيض واختراق شفرة البريد الالكتروني الخاصة بالرئيس الأمريكي ، وقد استطاعت أجهزة الموساد الوصول إلى شبكة الإتصالات في البيت الأبيض عبر اختراق شركة كمبيوتر أمريكية حصلت على حق تجديد شبكة معلومات كجهاز الطيران الحربي الإسرائيلي.

2 ـ قصد السرقة ومعرفة أرقام بطاقات الإئتمان وأرقام الحسابات وغيرها ، ولذلك يسعى لصوص الكمبيوتر إلى اختراق أجهزة المستخدمين وحل رموز الرسائل السرية ، وسرقة محتويات الأجهزة

[1] ـ السند عبد الرحمان عبد الله، الأحكام الفقهية للتعاملات الإلكترونية ، دار الوراق ، ط 2 ، 2006 ، ص 300.

[2] ـ ورقة علمية بعنوان إنتهاك سرية الاتصالات الشخصية ، نشرت على الموقع www.badil.info.com نشرت بتارخ 2014/08/20 ، تمت زيارة الموقع بتاريخ 2017/04/28.

والمعلومات الخاصة بهم ، ويستغل هؤلاء اللصوص بعض الثغرات الفنية التي توجد في برامج تشفير رسائل البريد الالكتروني ، ولقد اكتشف الباحثون في شركة (**آي آي ديجيتال**) الأمنية الأمريكية عيبا في برامج السرية الخاصة بتشفير رسائل البريد الإلكتروني ويمثل العيب نقطة ضعف داخل شبكة الإنترنت حيث تمكن لصوص الكمبيوتر من مهاجمة الشفرة من طريق البرامج المرافقة كبرنامج المساعدة من مايكروسوفت والذي يستعمله المستخدمون لتشفير برنامجهم البريدي بسهولة ويسر.

3 ـ المنافسة بين الدول أو الشركات أو المؤسسات أو الأفراد ، ومن الأهداف التي يقصدها مخترق البريد الالكتروني الإطلاع على الرسائل الالكترونية للمنافس له كما تقوم بذلك بعض الشركات لمعرفة النشاط الذي تقوم به الشركات الأخرى وما تنوي القيام به من مشاريع وأعمال ، فربما مكن الإطلاع عليها من سبقهم إلى مشروع معين أو صفقة معينة.

4 ـ الفضول والعبث واثبات القدرة على اختراق البريد الإلكتروني فقد يسعى بعض مستخدمي الإنترنت إلى محاولة اختراق بريد إلكتروني معين ، ويقوم بترك رسالة لصاحب البريد الإلكتروني المخترق تفيد بأن بريده الإلكتروني قد اخترق وقصد المخترق من ذلك بيان قدرته على هذا العمل.

5 ـ الحرب المعلنة بين أطراف مختلفين سواء على مستوى الدول أو المنظمات أو الهيئات والسيطرة التامة على البريد الإلكتروني للخصم ولمعرفة جميع تحركاته وتخطيطه ومراسلاته وقد استخدم هذا النوع من الإختراق في بعض الحروب القائمة في هذا العصر.

6 ـ الإختلاف بين الأفراد الذي يصل بالبعض إلى الكيد للآخر ، فيسعى إلى إلحاق الضرر به ، من خلال التجسس عليه ومعرفة أسراره[1].

4ـ جريمة الإحتيال عبر البريد الإلكتروني:

يعتبر الإحتيال عبر البريد الإلكتروني ظاهرة جديدة فقد أتاحت لمرتكبيها دخول المنازل و المكاتب و اجتياز الحدود و الوصول إلى الضحايا بسهولة بالغة ، خاصة مع انتشار الإنترنت كوسيلة مهمة لتقديم الخدمات المالية و المصرفية ، فيما يبتكر المحتالون الإلكترونيون وسائل جديدة يوميا للتغرير بضحاياهم و الإيقاع بهم ، وفي الوقت الذي يعمل فيه قراصنة الإنترنت و المحتالون الإلكترونيون

[1] ـ السند عبد الرحمان عبد الله، المرجع السابق، ص 302.

المحترفون على مدار الساعة لابتكار وسائل جديدة و العثور على ثغرات يمكن من خلالها تنفيذ مهامهم فإن شركات الأمن المعلوماتي ومعها البنوك و المؤسسات المالية و المصرفية أوجدوا أقساما تقنية متخصصة لحماية العملاء و تأمين معاملاتهم المالية عبر الإنترنت ، حيث يكتشف مصرفيون وخبراء كمبيوتر بشكل يومي العديد من الوسائل التي استخدمها في عمليات الإحتيال منها ما يتصل برسائل البريد الالكتروني و أخرى تتعلق بالمحادثات اليومية التي يجريها المستخدمون وغيرها من أنواع الإتصال[1]، لذلك سنتطرق إلى

1ـ تعريف الإحتيال:

في العقد السابع من القرن العشرين كان الإحتيال باستعمال الحاسوب من الجرائم الأولى التي بدأت تعرف على نحو واسع على أنها نوع جديد من الجرائم و نتيجة لذلك تمت أول مواجهة تشريعية لهذه الجرائم خلال قانون فلوريدا لجرائم الحاسوب فهو أول قانون جرم الإحتيال على الحاسوب و قد صدر هذا القانون في عام 1978و ذلك بعد حادثة ذائعة الصيت في أحد الأحداث الرياضية حيث قام البعض بطباعة بطاقات مزورة في ذلك الوقت ، ومع بداية الثمانينات بدأت معظم حكومات العالم بتبني قوانين مماثلة فكانت كندا من أوائل الدول التي سنت قانونا إتحاديا يخاطب جرائم الحاسوب و في عام 1990 في بريطانيا صدر قانون إساءة إستخدام الحاسوب الذي جرم الإحتيال في الفصل الثالث[2] ومن هنا ظهرت فكرت الإحتيال عبر الإنترنت ، وفي هذا السياق تعددت التعريفات حول الإحتيال عبر الإنترنت.

2ـ الإحتيال عبر الإنترنت:

أي سلوك إحتيالي ينتهج منهج الحوسبة بنية الحصول على امتياز مالي كما عرف البعض الإحتيال المعلوماتي : بأنه التلاعب العمدي بمعلومات و بيانات تمثل قيما مادية يختزنها نظام الحاسب الآلي أو الإدخال غير المصرح به لمعلومات و بيانات صحيحة أو التلاعب في الأوامر و التعليمات التي تحكم عملية البرمجة ، أو أية وسيلة أخرى من شأنها التأثير على الحاسب الآلي حتى يقوم بعملياته بناءا على هذه البيانات أو الأوامر أو التعليمات من أجل الحصول على ربح غير مشروع و إلحاق الضرر بالغير.

[1] ـ نضال يوسف إليا ، ورقة علمية بعنوان الاحتيال الالكتروني عبر الإنترنت في اطار ندوة علمية ، واقع خدمة الانترنت و انعكاسها على المستهلك العراقي ، جامعة الموصل ، بغداد 23،12،2008، العراق ، ص 01.

[2] ـ محمد طارق عبد الرؤوف ، المرجع السابق ، ص36، 37.

وقد عرف مكتب التحقيقات الفيدرالي الأمريكي الإحتيال عبر الإنترنت بأنه :أي مخطط إحتيالي عبر الإنترنت يلعب دور هام في عرض سلع أو خدمات غير موجودة أصلا أو طلب دفع ثمن تلك الخدمات أو السلع عبر الشبكة المعلوماتية ، أما وزارة العدل الأمريكية فعرفته بأنه شكل من التخطيط الذي يستخدم محتويات الإنترنت مثل الدردشة ، البريد الإلكتروني ، المواقع الإلكترونية و غيرها لتقديم صفقات إحتيالية أو لإرسال نتائج الإحتيال إلى المؤسسات المالية.

أما من الناحية القانونية فعلى صعيد الفقه فقد وردت تعريفات متعددة حيث عرفه الدكتور عبد الرؤوف عبيد بأنه كل كذب مصحوب بوقائع خارجية أو أفعال مادية يكون من شأنها توليد الإعتقاد لدى المجني عليه بصدق هذا الكذب بما يدفعه إلى تسليم ما يراد منه طواعية أو اختيارا ، في حين عرف **إياد الغزاوي** تلك الجريمة التي تتحقق من خلال توصل الجاني أو شخص آخر إلى تسليم مال منقول للغير دون وجه حق ، نتيجة استخدام الجاني لإحدى وسائل الخداع المنصوص عليها في

القانون على سبيل الحصر و التي تسفر عن وقوع المجني عليه في الغلط الدافع إلى التسليم[1].

كذلك هناك من عرفه بالاحتيال التقني : إن عملية الإحتيال التقني يقوم بها محترفون وذلك خلال بحثهم في كل نظام تشغيل حاسوبي لاختراقه مشير إلى العديد من مواقع و برامج الإختراق المتوفرة على الإنترنت و يتداولها دون مصاعب لتنفيذ عمليات القرصنة و السرقة و الاحتيال[2].

من أساليب الاحتيال عن طريق البريد الإلكتروني: الرسائل الشهيرة، رسالة تصل من شركة تطلق على نفسها اسم lottery Watergate ومركزها جوهانسبورغ، وهي رسالة محترمة جدا و كأنها صادرة فعلا عن شركة تجارية، حيث تعلمك بأنك ربحت 2.5 مليون دولار و تطلب منك تأكيد نيتك باستلام المبلغ كما تطلب منك المعلومات التالية: الإسم الثلاثي، عنوان المسكن، رقم الهاتف، رقم الفاكس، صورة عن الهوية، و عندما ترسل هذه المعلومات يرسلون إليك فاتورة باسمك تطالبك بمبلغ معين لقاء خدمات برية، و إذا أعطاهم الشخص المعني رقم حسابه أو رقم بطاقة الائتمان، فسوف يجد مفاجأة كبيرة في كشف المصرف آخر الشهر ، والأكثر إثارة في هذا النوع من الرسائل هو مدى جديته فقد طلبت إدارة هذه الشركة الوهمية من أحد الأشخاص ألا يرسل أي أوراق عبر البريد، وإنما يمكنه أن

[1] ـ ماجد عمر عبادي ، جريمة الاحتيال عبر البريد الالكتروني ، دراسة مقارنة ، جامعة النجاح الوطنية على الموقع الأتي : www adelmor com وقد تم الاطلاع على الموقع بتاريخ 09،05،2017

[2] ـ نضال يوسف إيليا ، المرجع السابق، ص05.

يحضرها بنفسه عند زيارته إلى مكتب الشركة المنتشرة في 11 دولة بين آسيا و أوروبا و بالولايات المتحدة الأمريكية[1].

3ـ تمييز جريمة الإحتيال الإلكتروني عن الجريمة الإلكترونية.

الجريمة المعلوماتية يطلق عليها جرائم الكمبيوتر و يقصد بها كل سلوك غير مشروع يتعلق بالمعلومات المخزنة في الكمبيوتر من حيث معالجتها و التلاعب بها باستخدام جهاز الكمبيوتر ينشأ عنها خسارة تلحق بالمجني عليه أو كسب غير مشروع يحققه الفاعل ، والجريمة المعلوماتية لها صور و أشكال متنوعة كسرقة المعلومات المخزنة أو التلاعب بها بالإضافة أو الحذف أو التعديل ، ووسيلة التوصل إلى مثل هذه المعلومات عادة ما تتم بطريق التحايل[2].

إن الجريمة المعلوماتية تتفق مع جريمة الإحتيال عبر البريد الإلكتروني في عدة أمور ، منها أن كل منها يعد من الجرائم الإلكترونية المستحدثة و كلاهما يعتمد على طرفي الجريمة الجاني و المجني عليه في استخدامهم لجهاز الكمبيوتر لتنفيذ الجريمة كما أن الركن المادي في كل منهما يتشابه إلى حد بعيد لأن الجاني يعتمد على ما يحمله من فطنة و خديعة و دهاء و حيلة و كلاهما يعدان من جرائم الواقعة على المال ، ومع ذلك توجد هناك عدة فوارق منها:

ـ يتوقف ارتكاب جريمة الإحتيال عبر البريد الإلكتروني على تحقيق شرط توفر خدمة الإنترنت ، في حين لا يتوقف ارتكاب الجريمة المعلوماتية على تحقيق مثل هذا الشرط.

ـ محل جريمة الإحتيال عبر البريد الإلكتروني هو المال المنقول المادي و المعنوي ، في حين أن محل الجريمة المعلوماتية لا يشمل المال المنقول المادي بل يقتصر على المال المنقول المعنوي و

نقصد بها البيانات و المعلومات المخزنة.

ـ يتمثل القصد الجنائي الخاص في جريمة الإحتيال عبر البريد الإلكتروني بالإستيلاء على الحيازة الكاملة لمال الغير ، في حين يتمثل القصد الجنائي الخاص قي الجريمة المعلوماتية بالتلاعب بالمعلومات و البيانات المخزنة داخل الكمبيوتر[3].

[1] ـ محمد طارق عبد الرؤوف ، المرجع السابق ، ص66.
[2] ـ أنظر علي عدنان الفيل ، الإجرام الإلكتروني دراسة مقارنة ، منشورات زين الحقوقية ، الطبعة الأولى ، 2011،ص 21.
[3] ـ أنظر علي عدنان الفيل، المرجع السابق، 22.

5ـ جريمة الإعتداء على مواقع التواصل الإجتماعي:

لقد بدأ بروز نظام جديد للتواصل الإجتماعي الرقمي بالصورة الحديثة منذ 1995، وهذا بأفكار ذات إهتمامات محدودة من الجانبين الجغرافي و الشخصي كالموقع الذي أنشأه Randy Cornades مع زملائه في الدراسة للتواصل الطلابي ، الذي لاقى التجاوب الواسع في المجال الذي أنشئ لأجله ليليه بعد سنتين موقع Sixbegees الذي بلغ عدد الأعضاء المسجلين فيه ، في أوج انتشاره إلى أزيد من ثلاثة ملايين و نصف عضو ، وقد كان يعتمد على تقنيات الجيل الأول من الويب يفتح صفحات شخصية للمستخدمين وعلى إرسال رسائل لمجموعة من الأصدقاء و الربط المباشر فيما بينهم ، رغم هذه المحدودية من الخدمات المقدمة إلا أن هذه المواقع لقيت تجاوب غير عادي من الساحة الإفتراضية هذا ما حفز على ظهور العديد من المواقع المشابهة لكن مع ظهور الجيل الثاني من الويب وضعت هذه المواقع و الشبكات أمام محك التأقلم و الإندثار مما فتح المجال إلى جيل جديد من المواقع الإجتماعية كموقع Friendster الذي كان وسيلة للصداقات و التعارف بين المجتمع العالمي و نال هذا الموقع شهرة كبيرة عالميا.

ولقد حاول البعض تعريف مواقع التواصل الإجتماعي ومن بين هذه التعريفات ما عرفه **زاهر راضي** على أنها: منظومة من الشبكات الإلكترونية التي تسمح للمشترك فيها بإنشاء موقع خاص به ، ومن ثم ربطه عن طريق نظام إجتماعي إلكتروني مع أعضاء آخرين لديهم الإهتمامات و الهويات نفسها[1].

إن ظهور وسائل التواصل الحديثة أحدث طفرة نوعية في الإتصال بين الأفراد و الجماعات ، ونتج عنها ممارسات و تأثيرات سلبية وايجابية انعكست بمجملها على المجتمع عموما وعلى الأسرة بصفة خاصة و في هذا الصدد حذر الدكتور **كوكشي** الخبير في تقنية المعلومات و مواقع التواصل الإجتماعي من خطورة التعاطي مع هذه القنوات في ظل الدراسة التي أعلنتها مؤسسة تكنولوجي "**جيت**" البريطانية التي أشارت فيها إلى ارتفاع معدل جرائم الإبتزاز الإلكتروني عبر الإنترنت في منطقة الشرق الأوسط بنسبة 33% ، وأوضح الدكتور أن جرائم الإبتزاز التي يتم تنفيذها عبر مواقع التواصل الاجتماعي باتت منظمة و ممنهجة و مدروسة من قبل عصابات دولية تقيم خارج الدولة ، وتستهدف الإيقاع بفئة الشباب خصوصا الذين يشغلون مناصب دولية مرموقة في عدد من المؤسسات أو

[1] ـ زاهر راضي، استخدام مواقع التواصل الاجتماعي في العالم العربي، مجلة التربية، العدد 15، جامعة عمان الأهلية، سنة 2003، ص23

الإعلاميين و أصحاب الحسابات الكبيرة في الفايس بوك الذين لديهم متابعات كبيرة في فئات المجتمع حتى يسهل عليهم إبتزازهم بحكم أن تلك الفئة تحرص على سمعتها بشكل كبير[1].

1. المس بحسابات الأشخاص عبر مواقع التواصل الإجتماعي:

إن مواقع التواصل الإجتماعي هي مواقع خدمات تؤسسها وتبرمجها شركات كبرى ، لجميع المستخدمين و الأصدقاء لمشاركة الأنشطة و الإهتمامات و البحث عن تكوين صدقات و اهتمامات أخرى ، ومن أشهر هذه المواقع موقع توتر twitter موقع إنستجرام instagram موقع الفايس بوك facebook ، و بالتالي فإن جميع هذه المواقع أصبحت تضم منخرطين فيها ، وتخزن معلومات ذات طابع شخصي لهؤلاء المنخرطين و أصبح الحصول على و معرفة تلك المعلومات متاحا للجميع بواسطة هذه المواقع ، ومن بين أوجه انتهاكاتها ، أقدم البعض على إنشاء حساب شخصي له باسم طرف آخر يتضمن كافة البيانات المتعلقة بالطرف الثاني من هويته ، عنوانه ، مهنته ، بل حتى رقم هاتفه الشخصي إضافة إلى صوره الفوتوغرافية ... وهي معطيات يحصل عليها الطرف المحتال بأية طريقة معينة ، كما أن من مظاهر الإنتهاك أيضا قرصنة البريد الإلكتروني للشخص مرورا بمواقع التواصل الإجتماعي ووصولا لحسابات شخصية أخرى.

2 ـ قضية إنتهاك خصوصية رسائل المستخدمين ضد الفيس بوك:

منذ أن تم افتتاح الفيس بوك و دائما ما تقع الشركة في فخ الكثير من مشاكل إنتهاك الخصوصية و لكن هذه المرة تأتي المشاكل من خلال ماسنجر الفيس بوك ، حيث أنه يقوم بقراءة كافة رسائل المستخدمين الخاصة بهم بدون الحصول على موافقة خاصة من المستخدمين وهو الأمر الذي جعل المستخدمين يقومون برفع دعوى على الشركة في هذا الصدد ، و في **أوكلاند** قرر القاضي المختص بالقضية بأنه وجب رفع دعوى قضائية جماعية من المستخدمين في حق الفيسبوك و ذلك لانتهاكه المباشر خصوصية المستخدمين من خلال ما يحدث في ماسنجر الفيس بوك وهو ما يجعله يستطيع جمع بيانات عنهم بشكل كبير و ذلك من أجل استهدافهم ومن غير الحصول على موافقة رسمية منهم لهذا الأمر ، وفي عام 2013 تم رفع دعوى قضائية على الفيس بوك تفيد بأن الشبكة الإجتماعية الأكبر في العالم تعمل على مسح و قراءة الرسائل المكتوبة من خلال نظام الرسائل في ماسنجر

[1] ـ رامي عايش، شبكة التواصل الإجتماعي عند ما تصبح فخا، ورقة علمية نشرت بتاريخ 19، 09، 2015 على الموقع www.albayan.com وتم الإطلاع على الموقع بتاريخ 2017/05/31.

الفيس بوك و خصوصا فيما يتعلق بالروابط المنقولة ، حيث تسعى الدعوى لمطالبة الفيس بوك بالتوقف فورا عن قراءة أي من الرسائل المتبادلة بين المستخدمين فهو تصرف مخالف تماما لكافة القوانين الخاصة بحقوق الإنسان لكن الفيس بوك مازالت تدافع عن نفسها في هذا الأمر و توضح أن ما تقوم به هو تصرف محمي بشكل كامل من قبل قانون خصوصية الإتصالات الإلكترونية الفدرالي فهو يأتي في سياق أنه تصرف متاح و عادي و لكن المحكمة تقول أنه كيف ترى الفيس بوك نفسها بما تقوم به أنه أمر عادي فهو إنتهاك مباشر لحقوق المستخدم؟ كما أن الفيسبوك توضح أنها تقوم بقراءة الرسائل من خلال العمل على حماية المستخدمين من كافة

الفيروسات المنتشرة و رسائل البريد الإلكتروني[1].

6ـ المواقع المعادية:

يعتبر مصطلح المواقع المعادية من المصطلحات الحديثة حيث بدأ استخدامه بعد هذا التطور التكنولوجي الذي نشهده اليوم فمصممي تلك المواقع المعادية قد استغلوا هذه التكنولوجيا المعلوماتية لخدمة أغراضهم الشخصية في عرض أفكارهم الشخصية التي لم يمتلكوا الشجاعة الكافية في سلك الطرق الشرعية المباحة في عرض تلك الأفكار و الآراء و غالبا ما يكون الغرض من المواقع المعادية:

ـ الإساءة إلى دين معين من الأديان و نشر الأفكار السيئة عنه وحث الناس على الإبتعاد عنه و تلك المواقع غالبا ما يكون القائمين عليها من معتنقي الديانات الأخرى المتشددين في دينهم الذين لا يعتنقون فكرة التسامح و التعايش بين الأديان ،أو يكون هدفهم بث الشقاق فيما بين أفراد الشعب الواحد و المعتنقين لأكثر من دين ، فيحاولون إثارة الفتنة بينهم عن طريق نشر الأخبار الكاذبة و المضللة في محاولة منهم لتحقيق هدفهم الخبيث.

ـ الإساءة إلى شخص معين بما يمثله من مواقف سواء دينية أو سياسية أو وطنية ، وما إلى ذلك من الأهداف التي لا يجد القائمون عليها من يستمع إلى آرائهم المغلوطة أو التي تتنافى مع الدين و المبادئ ، وعليه يجد هؤلاء في شبكة الإنترنت ضالتهم المنشودة في الوصول إلى أكبر عدد من

[1] ـ أنظر مقال بعنوان قضية إنتهاك خصوصية رسائل المستخدمين ضد الفيس بوك من الموقع الآتي https//pro3xplain.com وقد تم الإطلاع على الموقع بتاريخ 05/07/ 2017.

الأشخاص لعرض آرائهم عليهم في محاولة منهم لكسب تأييدهم دون تعريف أنفسهم في محاولة منهم للتخفي خوفا من رد فعل الناس التي غالبا ما ترفض مثل تلك الآراء التي بدلا من أن يجاهر أصحابها و اتخاذ الطريق القانوني الصحيح في نشر أفكارهم و آرائهم ليكون من حق أفراد الطرف الثاني عرض وجهة نظرهم وردهم على تلك الإتهامات نجد أنهم يتخوفون و يختفون دون أن يمتلكون أنواع الشجاعة في الإعلان عن أنفسهم و في عرضهم لأرائهم[1] ، والتعرض للأديان يعد من الأمور المجرمة و غير المقبولة على الإطلاق خاصة في البلاد الإسلامية التي يحث الدين الإسلامي و هو الدين الغالب فيها على احترام الأديان الأخرى وعدم التعرض لمعتنقي أي دين و أسباب ذلك التجريم تنطوي على أن الحرية و الديمقراطية التي تنعم بها الشعوب لا يجب أن تنطوي على الإخلال بها و الإساءة للأشخاص في أعراضهم و مبادئهم و شرفهم و نسب أمور غير صحيحة لهم بغرض التشهير بهم و بمبادئهم و الخوض في أعراضهم و في حياتهم الخاصة التي هي ملك لهم وحدهم دون أن يكون لأي شخص آخر أن يخوض أو يتدخل فيها بأي شكل من الأشكال.

ـ الإساءة إلى بلد معين و إلى مواقف قادته السياسيين من قضاياه الوطنية وهم غالبا ما يكونون معارضين للنظام السياسي القائم في بلد ما فيحاولون نشر الأفكار و الأخبار الفاسدة التي تنشر الفرقة بين أفراد الشعب السياسي القائم[2].

وفي تقرير حديث نشر عام 1998 بمجلة إنترنت العالم العربي " بعنوان جرائم ويب " إحصائيات و أرقام أن موقع شرطة إنترنت www.webpolice.org يستقبل شكاوى يومية من مستخدمي الإنترنت في مختلف بلدان العالم و يحقق فيها ، وتدور هذه الشكاوى حول جرائم التزييف ، الإحتيال ، السرقة التي تجرى عبر شبكة الإنترنت ، وخرق القوانين المعمول بها بوضع صور أطفال إباحية بها ، وتشير هذه المواقع لتقارير إحصائية تتحدث باستمرار عن جرائم الشبكة من خلال الشكاوى التي تصل يوميا ، ونعرض فيما يلي التقرير الذي نشره هذا الموقع بتاريخ 1998.1.1:

1ـ إساءة استخدام البريد الإلكتروني بنسبة 41%من جملة الجرائم المبلغ عنها.

2ـ إساءة استخدام غرفة الدردشة بنسبة 21%.

[1] ـ منير محمد الجنبهي، ممدوح الجنبهي، جرائم الإنترنت و الحاسب الآلي ووسائل مكافحتها، المرجع السابق، ص، ص37

[2] ـ منير محمد الجنبهي، ممدوح الجنبهي، المرجع نفسه، ص82،81.

3ـ صور الأطفال الإباحية بنسبة 11%و تبين البنود من 04الى 13من هذا التقرير أن جرائم الغش و خرق حقوق النشر ، المضايقات ، التهديد ، السرقة ، إساءة التعامل مع الأطفال لتدمير محتويات الكومبيوتر ، الصور الإباحية ، الاغتصاب تشكل 28%.

هذا بالإضافة إلى إقرار المشرع الجزائري بمسؤولية الشخص المعنوي في الجرائم المعلوماتية ، وقد نص على ذلك في قانون العقوبات " يعاقب الشخص المعنوي الذي يرتكب الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي[1]".

المطلب الثاني: الجرائم التي تقع على الأموال عبر المعطيات الرقمية.

إن جرائم الإعتداء على الأموال عبر الشبكة المعلوماتية لم تقتصر على أساليب إساءة إستخدام الثورة

التقنية على الأشخاص فحسب ، بل تتعداها لتطال الذمة المالية للغير مما يشكل إعتداءا على أموالهم المادية ، وإذا كان هذا الإعتداء في نطاق المعالجة الآلية سواء كانت معلوماتية أو رقمية فإنه ينصب على الحاسب الآلي ذاته و ما يتصل به من ملحقات ، حيث يعتبر الحاسب أداة سلبية لإرتكاب الجريمة ضد الفرد عند استخدامه عبر الشبكة كوسيلة لتنفيذ الجرائم و الإعتداء على أموال الغير ومن هنا قسمنا هذا المطلب إلى فرعين تناولنا في الفرع الأول : جرائم تمس الأموال المادية عبر المعطيات الرقمية و في الفرع الثاني الجرائم التي تمس الأموال المعنوية عبر المعطيات الرقمية.

الفرع الأول: جرائم تقع على الأموال المادية عبر المعطيات الرقمية.

شهد القرن الماضي ثورة من نوع غير مألوف إصطلح على تسميتها بثورة المعلومات و الإتصالات وقد حققت هذه الأخيرة نجاحا ملموسا في التعامل بين الأفراد و الشركات الإقتصادية الكبرى أدت إلى تغيير طبيعة و نمط الحياة الإقتصادية لكافة المستهلكين سواء في الدول المتقدمة أو النامية على حد سواء ومن جهة أخرى ظهور المؤسسات المالية و المصرفية و التجارية العالمية التي تسعى بشكل دائم للتدخل المتنامي في الحياة الإقتصادية بشكل عام و حياة الأفراد خاصة مما أدى لظهور بطاقات إلكترونية أطلق عليها ببطاقة الإئتمان تقدم خدمات و مزايا لجميع المتعاملين بها.

[1] ـ أنظر المادة 394 مكرر 4 من قانون القعوبات الجزائري القانون السابق.

1 ـ الإحتيال عبر بطاقات الإئتمان:

و كان أول ظهور لبطاقات الإئتمان في أمريكا و أصبحت تحتل مساحة كبيرة في تعاملات الأفراد على حساب باقي وسائل الدفع الأخرى و أدى هذا الإنتشار محليا و دوليا إلى ظهور أساليب و طرق للتلاعب و الإحتيال باستخدامها ، حيث أدى ذلك إلى صعوبة إثبات العميل وإلى الإستغلال غير المشروع للبطاقة الذي يشكل جريمة مستحدثة تضم مجرما جديدا و مفهوما جديدا للجريمة و مسرحا واسعا يشمل كافة أقطار العالم ، وخلق هذا الإنتشار فرصة لمحترفي السرقة و التزوير في استخدام بطاقات الائتمان للتحايل و التلاعب من خلالها خاصة أن هذه النوعية من البطاقات تعتمد في طريقة التعامل بها على النظام المعلوماتي الذي تتدفق فيه البيانات و المعلومات و الذي تكون فيه النقود عبارة عن رموز و بيانات مشفرة إلكترونيا يستطيع محترفو جرائم الحاسب فكها و تزويرها بهدف الحصول على الأموال بطريقة غير مشروعة ، فقد أصبحت جرائم بطاقة الدفع الإلكتروني تمثل تهديدا يتأثر به حامل البطاقة وجمع أطراف عمليات البطاقة في جميع أنحاء العالم و في ذات الوقت حيث يتم إعداد و تضييع البطاقات المزورة في دولة ما بينما تجمع المعلومات اللازمة عن بطاقة الدفع الصحيحة في دول أخرى و يجرى ترويج البطاقات المزورة في مكان آخر من العالم ، كما أن التقنية الحديثة مثل الفاكس و الإنترنت ووسائل الإتصال المتقدمة و المعلومات الإئتمانية الآلية المنتشرة عالميا قد أتاحت جميعها للمزور فرصة سلب حقوق الآخرين في أي مكان في العالم.

2ـ جريمة الإحتيال باستعمال بطاقات الدفع الإلكتروني:

يعتمد هذا النوع من الجرائم على بطاقات الدفع الإلكتروني أثناء عمليات التحويل من حساب بطاقة العميل إلى رصيد التاجر بالبنك الذي يوجد في حسابه و ذلك من خلال الشبكة الصوتية الإلكترونية لهيئات دولية كهيئة فيزاكارد ، وماستركارد و تعطي هذه البطاقة للعميل الحصول على السلع و خدمات أخرى على الشبكة بواسطة تصريح كتابي أو تليفوني بخصم القيمة على حساب البطاقة[1] ، ومن هنا يستعمل القراصنة أرقام بطاقات الإئتمان بواسطة برامج تشغيل تتيح إمكانية تخليق بطاقات بنك معينة من خلال تزوير الحساب برقم خاص بالبنك مصدر البطاقة و استخدامها بطريقة غير شرعية في عملية التسويق عبر الشبكة ، كما أن الإستيلاء على بطاقات الإئتمان أمر ليس بالصعوبة

[1] ـ محمد صالح الألفي، جرائم الإعتداء على البطاقات الإئتمانية كأحد الأنماط الإجرامية المستحدثة، ورقة عملية منشورة على الموقع الآتي http:// www.eastlaws.com و تم الإطلاع على الموقع بتاريخ 2017/06/20، ص07.

بمكان ، فلصوص بطاقات الإئتمان مثلا يستطيعون الآن سرقة مئات الألوف من أرقام البطاقات في يوم واحد من خلال شبكة الإنترنت ، ومن ثم بيع هذه المعلومات للآخرين.

وقد أثبتت شركة MSNBC عمليا مدى سهولة الحصول على أرقام البطاقات الإئتمانية من شبكة الإنترنت ، حيث قامت بعرض قوائم تحتوي على أكثر من 6500 رقم بطاقة ائتمانية حصلت عليها من سبع مواقع للتجارة الإلكترونية وذلك عن طريق إستخدام قواعد بيانات متوافرة تجاريا و لم يكن من الصعب على أي متطفل أو متسلل إستخدم تلك الوسيلة البدائية للوصول و الإستيلاء على أرقام و استخدامها في عمليات شراء يدفع الثمن فيها أصحاب البطاقات الحقيقية ، و يتعدى الأمر إلى المخاطر التي يمكن أن تتعرض لها البطاقة الإئتمانية الحالية فنحن الآن في بداية ثورة تقنية يطلق عليها إسم "النقود الإلكترونية "و التي يتنبأ لها أن تكون مكملة للنقود الورقية ومن المتوقع أيضا أن يزداد الإعتماد على هذا النوع الجديد و الحديث من النقود وأن تجوز الثقة التي تحوزها النقود التقليدية[1].

و يعتمد المجرمون على العديد من الأساليب للاستيلاء على البيانات و الأرقام السرية لبطاقات الإئتمان لاستخدامها في الإحتيال ومن أهم هذه الأساليب:

ـ أسلوب إنتحال الصفة: يتم هذا الأسلوب عن طريق إنشاء مواقع مزيفة على الشبكة المعلوماتية ، على غرار مواقع الشركات و المؤسسات التجارية الأصلية الموجودة على هذه الشبكة ، حيث يبدوا هذا الموقع المزيف و كأنه الموقع الأصلي المقدم لتلك الخدمة ، و بعد إنشاء الموقع المزيف ، يستقبل عليه الجناة جميع المعاملات المالية و التجارية التي يقدمها عادة الموقع الأصلي لعملائه عبر شبكة الإنترنت ، فيتم استقبال الرسائل الإلكترونية الخاصة بالموقع الأصلي و الإطلاع عليها ، ومن ثم يتم الإستيلاء على البيانات الخاصة ببطاقات الإئتمان أو بطاقات الدفع الإلكتروني ، وفي إحدى القضايا تم القبض في مصر على عصابة مكونة من ثلاثة أشخاص لقيامهم بتصميم مواقع تشبه مواقع بعض المصارف ، ثم قيامهم بإرسال رسائل عشوائية عن طريق البريد الإلكتروني إلى عملاء حقيقيين فينخدعون و يقومون بكتابة بياناتهم و يتبعون الخطوات التي يحددها لهم المتهمون ، وبعد التعرف على البيانات السرية للعملاء خاصة كلمات المرور السرية يتم الإستيلاء على أرصدة هؤلاء الضحايا.

[1] ـ محمد صالح الألفي، جرائم الإعتداء على البطاقات الائتمانية كأحد الأنماط الإجرامية المستحدثة، المرجع السابق، ص08.

ـ أسلوب التجسس: حيث يقوم الجناة وفقا لهذا الأسلوب باستخدام برامج لاختراق الأنظمة المعلوماتية للشركات و المؤسسات التجارية العامة على الشبكة المعلوماتية ومن تم يستطيع هؤلاء الجناة الإطلاع على البيانات و المعلومات التجارية بهذه الشركات ومنها المعلومات المتعلقة ببطاقات الإئتمان أو الدفع الإلكتروني المستخدمة في التجارة الإلكترونية عبر الشبكة و بذلك يتمكن الجاني من الإستيلاء على بيانات البطاقات الصحيحة و استخدامها عبر شبكة الإنترنت على حساب الحامل الشرعي للبطاقة ومن أمثلة ذلك في عام 1997 قام شخص يدعى "كارلوس سادالغو" بالإستيلاء على أرقام 100.0000 بطاقة إئتمان و بيانات أخرى من خلال اختراقه لمجموعة من مزودي خدمات الإنترنت ، وقام بوضع هذه الأرقام على أسطوانة مضغوطة ، ثم قام بتشفيرها و عرضها للبيع بمبلغ 250 ألف دولار و لقد إكتشف عملاء المباحث الفيدرالية هذه الجريمة و حوكم و عوقب بالسجن 30 شهرا[1].

ـ أسلوب الشفط:

هو طباعة التفاصيل المخزنة على الشريط الممغنط لبطاقة الائتمان عن طريق تمرير البطاقة على

قارئ إلكتروني ، وبمجرد الحصول على تفاصيل البطاقة ، مثل رقم التعريف بهوية الحامل و تاريخ انتهاء صلاحية البطاقة يستطيع المحتال إنشاء بطاقة مطابقة للبطاقة الأصلية لاستعمالها في الصفقات التي تعقد على الإنترنت و خطورة هذا النوع من الإستيلاء على بيانات البطاقات هو أن حامل البطاقة لا يعلم بأن بطاقته تم اختراقها لذا لا يبلغ أحدا لإلغائها ، و بذلك يستطيع المحتال استخدام البطاقة المزورة خلال فترة طويلة ، وهذا بعكس الأسلوب التقليدي المتبع في الإستيلاء على بيانات البطاقة و هو سرقة البطاقة و في عام 2005 تم الحكم في إنكلترا على أربعة من أعضاء عصابة لمسح البطاقات و سحب الأموال ، بالسجن لمدة أربع سنوات لارتكابهم الإحتيال الذي قدرت خسارته ب200.000 جنيه إسترليني ، ومن الجدير بالذكر أن هناك أسلوب ميكانيكيا للإستيلاء على بيانات بطاقات الإئتمان ، حيث يتم تحويل التفاصيل المنقوشة على البطاقة البلاستيكية ميكانيكا من بطاقة إلى أخرى و هذه الطريقة أسهل من أسلوب سرقة البطاقة برمتها أثناء نقلها ما بين البنك و الزبون[2].

[1] محمد طارق عبد الرؤوف، جريمة الإحتيال عبر الإنترنت، المرجع السابق، ص 82.
[2] ـ محمد طارق عبد الؤوف، جريمة الإحتيال عبر الإنترنت، المرجع نفسه، ص 84.

ـ تخليق أرقام البطاقات:

ويقوم هذا الأسلوب على تخليق أرقام بطاقات إئتمانية اعتماد على إجراء معادلات رياضة و إحصائية ، بهدف الحصول على أرقام بطاقات ائتمانية مملوكة للغير ، وهي كل ما يلزم للشراء عبر الشبكة المعلوماتية ، وهذا الأسلوب يعتمد على أسس رياضية في تبديل و توفيق أرقام حسابية ، تؤدي في النهاية إلى ناتج معين ، وهو الرقم السري لبطاقة ائتمان متداولة ثم يتم استخدامها غبر الشبكة المعلوماتية[1].

3. جريمة السطو على أموال البنوك:

تتجسد جريمة السطو على أموال البنوك عن طريق استخدام الشخص الحاسب الآلي للدخول إلى شبكة

الإنترنت و الوصول غير المشروع إلى البنوك و المصاريف و المؤسسات المالية ، و تحويل الأموال من تلك الحسابات الخاصة بالعملاء إلى حسابات أخرى و ذلك بإدخال بيانات غير حقيقية أو تعديل أو مسح البيانات الموجودة بقصد اختلاس الأموال أو نقلها أو إتلافها ، وتقوم هذه التقنية على الإستيلاء على الأموال بكميات صغيرة جدا من الحسابات الكبيرة بحيث لا يلاحظ نقصان هذه الأموال ، وتكون عن طريق اختلاس البيانات والإفادة منها باستخدام المختلس للمعلومات الشخصية مثل الإسم ، العنوان ، الأرقام السرية الخاصة بالمجني عليهم و الإستخدام غير الشرعي لشخصية المجني عليه ليبدأ بها عملية السرقة المتخفية عبر الإنترنت بحيث تؤدي بالغير إلى تقديم الأموال إلي الجاني عن طريق التحويل البنكي[2].

4ـ جريمة غسيل الأموال عبر الإنترنت.

جريمة غسيل الأموال تعني إخفاء حقيقة الأموال المستمدة من طريق غير مشروع ، عن طريق القيام بتصديرها أو إيداعها في مصارف دول أخرى ، أو نقلها أو إيداعها أو توظيفها و استثمارها في أنشطة مشروعة ، سواء كان الإيداع أو النقل أو التحويل أو الإستثمار قد تم في دول متقدمة أو في دول نامية ، كما توجد مسميات أخرى يطلقها الناطقون باللغة العربية على غسيل الأموال مثل تبيض الأموال ، و تطهير الأموال ، وتنظيف الأموال تنقيح الأموال ، و تؤدي إلى نفس المعنى و إذا كانت الترجمة

[1] ـ محمد طارق عبد الؤوف، المرجع السابق، ص85.
[2] ـ صغير يوسف، المرجع السابق، ص46

الدقيقة للمصطلح الانجليزي Money Laundring ، هو غسيل الأموال ، وهي الترجمة التي أخذت بها الأمم المتحدة في وثائقها[1] ، ومصطلح غسيل الأموال هو مصطلح حديث إلى حد ما ، وقد بدأ استخدام هذا المصطلح في الولايات المتحدة الأمريكية عام 1931 حيث تمت محاكمة أحد زعماء المافيا و مصادرة أمواله على أساس أن مصدرها هو تجارة غير مشروعة (تجارة المخدرات) ،و عليه فإن غسيل الأموال هو تحويل مصدر الأموال غير المشروع إلى مصدر مشروع ، و تشمل عمليات غسيل الأموال المتحصلة عن أنشطة غير مشروعة كالإتجار في المخدرات و عمليات تهريب الذهب و الأحجار الكريمة و التهرب من الضرائب و الإتجار في الأعضاء البشرية و الرقيق الأبيض و السلاح و إدارة شبكات الدعارة والتجارة غير المشروع في الأسلحة و المواد النووية و الإبتزاز و تزيف العملات و غيرها من الجرائم المنظمة المعاصرة[2].

وفي هذا الصدد يقول الأستاذ عبد الله درميش : " تتسم إجراءات غسيل الأموال بأنها جرائم لاحقة لأنشطة الجريمة حققت عوائد مالية خيالية ، فكان لزاما إضفاء المشروعية عليها بوسائل و أساليب تعتمد تقنيات عالية لتبسيطها وإخفاء طبيعتها و تخرج بواسطتها المختلسون و محترفوا الجريمة المنظمة و أباطرة المخدرات من عنق الزجاجة ، فهي إذن مخرج للتجارة ، كما أنها نشاط إجرامي تعاوني تتقاطع فيه مجهودات شريرة للخبراء في عالم الأعمال و الأموال و لرجال البنوك و المؤسسات المالية و للتقنين في عالم المعلومات و المتطلعين في الجريمة و المستثمرين في أفعال الخداع و النصب فهي حصيلة مجهودات متضافرة من قوى الشر محبوكة بصناعة عالية".

وقد أعطت شبكة الإنترنت عدة مميزات لمن يقومون بعمليات غسيل الأموال منها السرعة الشديدة و تخطي الحواجز الحدودية بين الدول ، و تفادي القوانين التي قد تضعها بعض الدول و تعيق نشاطهم و كذلك تشفير عملياتهم مما يعطيها قدرا أكبر من السرية[3] ، و استخدام الإنترنت في غسيل الأموال له وجوه كثيرة مثل استخدام بطاقة الائتمان لشراء مجوهرات ثم سداد الفاتورة الخاصة بها بالنقد العائد من عمليات الإتجار في المخدرات أو الدعارة وغيرها من الجرائم.

[1] ـ مباركي دليلة ، غسيل الأموال، أطروحة دكتوراه علوم تخصص، قانون جنائي باتنة، الجزائر، 2008، ص08.

[2] ـ عبد الله أحمد المشرخ، مكافحة الإجرام الاقتصادي و المالي، مجلة الفكر الشرطي، إدارة شرطة الشارقة، العدد الثالث، سنة 2000،07،13،ص12.

[3] ـ منير محمد الجنبهي ، ممدوح محمد الجنبيهي، جرائم الإنترنت و الحاسب الآلي ووسائل مكافحتها، المرجع السابق ،ص79.

و أيضا إنتشار التجارة الإلكترونية عبر شبكة المعلوماتية خير معين لهؤلاء القائمين على عمليات غسيل الأموال كالتجارة الإلكترونية و انتشارها عبر أنحاء العالم ، قد ساعد كثيرا في عمليات غسيل الأموال نظرا لسرعة الإتفاق على الصفقات و إتمامها من خلاله دون أن يكون في معظم الأحيان تحت رقابة قانونية صارمة بل إنه في حالة وجود رقابة قانونية يكون من الممكن تفادي تلك الرقابة و إتمام تلك الصفقات عبر الإتفاق على خطوات و ترتيبات يتم تنفيذها عبر الإنترنت و بطريقة تشفير معقدة لا يمكن حلها و بالتالي لا يمكن من خلالها معرفة كيفية إتمام تلك الصفقات[1].

5- جريمة القمار عبر الإنترنت:

تدخل هذه الجريمة ضمن عملية غسيل الأموال مع أندية القمار المنتشرة عبر العالم ، الأمر الذي جعل مواقع الكازينوهات الإفتراضية عبر الإنترنت محل اشتباه و مراقبة من قبل السلطات الأمريكية ، و أن المشاكل القانونية التي تواجه أصحاب مواقع القمار الإفتراضية على الإنترنت غير مصرح بها بعكس النوادي الحقيقية و كل هذا من أجل أموال باهضة نتيجة القمار عبر الشبكة كما يوجد على الإنترنت أكثر من 100 موقع للقمار تمارس فيه جميع أنواع القمار التي توفرها المواقع الحقيقية ، وسوق القمار في أمريكا يعد الأسرع نموا على الإطلاق حيث يلجأ أصحاب تلك المواقع إلى إنشائها و إدارتها من أماكن مجاورة لأمريكا وتعلن هذه النوادي عبر الإنترنت عن تواجدها فيزيائيا في منطقة حوض الكاربي و لقد تابعت شرطة FBI المباحث الفيدرالية مواقع الإنترنت التي تقوم بنشاطات غسيل الأموال وركزت أعمالها و تحقيقاتها على عمليات المقامرة و الأشخاص الذين يقومون بهذه الأعمال و تبين أن هذه المواقع موجودة في "كاركار ، وجزر الأنتيل ، جزيرة إنيتجوا ، وجمهورية الدومينيكان[2]".

الفرع الثاني: جرائم تقع على الأموال المعنوية عبر المعطيات الرقمية.

لقد صاحب التطور الذي شهده العالم في الفترة الأخيرة في القرن الماضي في شتى المجالات تطورا

هاما و خاصة في مجال الإتصالات فيما يتعلق بالتقنيات المعلوماتية و التي تزايد التعامل بها و ذلك لسرعتها و لما توفره من وقت ، ولقد كانت المعلومات المتولدة عن التفاعلات البشرية محددة إلى حد

[1] - منير محمد الجنبهي، ممدوح محمد الجنبيهي، المرجع السابق،ص80.

[2] - ممدوح عبد الحميد عبد المطلب، جرائم الكومبيوتر و شبكة المعلومات العالمية مكتبة الحقوق، الشارقة (الإمارات العربية المتحدة)، الطبعة الأولى،2001، ص70.

كبير و لم يمثل حجمها أي مشكلة أمام جمعها و تخزينها ، ولكن مع تقدم البشرية و تزايد كم المعلومات أصبحت الطرق التقليدية لجمع المعلومات عاجزة عن تلبية الإحتياجات بكفاءة و فعالية ، و أصبح من الضروري وجود وسائل أكثر تطورا لحماية وجمع هذه المعلومات و بظهور هذه المعلومات برزت مشاكل قانونية حول مدى إمكانية اعتبار أن هذه المعلومات أموال معنوية ؟

لذلك سنتطرق إلى تعريف المال بصفة عامة : فالمال هو ما يصلح أن يكون محلا للحق ذو القيمة المالية و الشيء هو محل الحق ، وتنقسم الأشياء إلى أشياء مادية و أشياء غير مادية أو معنوية علما بأن الأموال من وجهة النظر التقليدية لا ترد على أشياء مادية و لهذا كان تعريف المال بصدد جرائم الأموال بأنه " كل شيء مادي يصلح لأن يكون محلا لحق من الحقوق المالية[1] ، وقد عرفت الأموال المعنوية : بأنها الأموال التي لا يمكن تحديدها باللمس بل بالحواس الأخرى و يعترف بالحقوق التي تقرر عليها ، وما يرد عليها من حقوق هي حقوق معنوية أو سلطات يقرها القانون لشخص على شيء معنوي ومنها حق المؤلف على مصنفه الأدبي ، أو الموسيقى و حق المخترع على اختراعه و كذلك المصمم على تصميمه[2].

ولكن مع التطور ازدادت الأشياء المعنوية عددا و تفوق بعضها من حيث قيمتها على الأشياء المادية مما استدعى البحث عن معيار آخر غير طبيعة الشيء الذي يرد عليه الحق المالي حتى يمكن إسباغ صفة المال على الشيء المعنوي ومن الأشياء المعنوية ذات القيمة الإقتصادية العالمية برامج الحاسب الآلي فهذه البرامج تكون عادة مثبتة على دعامة أو حامل مثل الأقراص أو الأشرطة الممغنطة من البلاستيك أو الورق المقوى أو مادة أخرى ، ويعتبر الإعتداء على الدعامة في هذه الحالة قد وقع على شيء مادي مما يصلح تكييفه حسب النشاط الإجرامي بإحدى جرائم الأموال التي يتطابق نموذجها مع هذا النشاط ، أما إذا وقع الإعتداء على البرامج مستقلا عن دعامته ، فإن الأمر يختلف حيث يكون قد وقع على شئ معنوي ، هذا الشئ لا بد لأن أن تثبت له صفة المال أولا حتى يمكن البحث بعد ذلك في إمكانية وقوع جرائم الأموال عليه ، وقد انقسم الفقه في هذا الصدد إلى اتجاهين هما:

[1] ـ أحمد عبد الرزاق السنهوري، الوسيط في شرح القانون المدني ، حق الملكية ، الجزء الثاني ، دار إحياء التراث العربي ، بيروت ، 1952، ص09.

[2] ـ أحمد عبد الكريم سلامة القانون الدولي الخاص، دار النهضة العربية، القاهرة، 2008، ص 1010.

1ــ الإتجاه الأول: الفقه المؤيد لإضفاء المال على البرامج.

يرى جانب من الفقه أن المعلومات صالحة لأن تكون محلا للإعتداء عليها طالما كانت هذه المعلومات تعكس الرأي الشخصي لصاحبها و لا يتوقف عند نطاق المعلومات العامة ، وذلك على أساس أن هذه المعلومات صادرة عن صاحبها أي ترتبط بشخصيته وهو الذي فكر فيه ، أو هذا يعني أنها من الحقوق اللصيقة بشخصية صاحبها ، وهي المعلومات ذاتها موضوع هذا الحق ومن خصائصها القابلية للإنتقال و هذا يعني أن هناك طرفا آخر يستقبل هذه المعلومات ، ومن هنا تنشأ علاقات إما بينها و بين صاحبها و إما بين صاحبها و الغير ، فالمعلومات بإعتبارها نتاجا ذهنيا لمن يعطيها شكل المعلومات فهي تعد محور العلاقات مثل تلك التي تنشأ بين المالك و بين ما يملك فيكون له نقلها و إيداعها و حفظها و تأجيرها و بيعها ، ومن أمثلة هذه المعلومات برامج الحاسب الآلي إذ أن هذه البرامج ترتب حقوقا لصاحبها و تخول له إبرام عقود متعلقة مثل الإيجار و البيع و الحفظ و أية صورة أخرى من صور الإستغلال لأن من خصائصها القابلية للإنتقال ، كل هذه التصرفات و الحقوق هي التي دفعت جانب من الفقه إلى القول بأن المعلومات مال ليس فقط لوجود علاقة حق استئثار خاص عليها ، وإنما أيضا لأنها تعتبر قيمة إقتصادية فهي تطرح في السوق للتداول مثلها في ذلك مثل أي سلعة و لها سوق تجاري يخضع لقوانين السوق الإقتصادية و إذا كان الفقه التقليدي قد استبعد المعلومات من طائفة الأموال على أساس أنها غير مادية أي أن عدم مادية المعلومات هو الذي أدى إلى عدم الإعتراف لها بصفة المال فإن الفقه الحديث يرى على العكس أن معيار الشيء بأنه مال ليس على أساس ماله من كيان مادي و إنما على أساس قيمته الإقتصادية ، و أن القانون الذي يرفض إصباغ صفة المال على الشيء له قيمة إقتصادية هو بلا جدال قانون ينفصل تماما عن الواقع و مادامت البرامج في جوهرها معلومات معالجة بطريقة ما و لها قيمة إقتصادية فإنه يجب معاملتها على أنها مال وما يؤكد هذا المعنى أن المشرع الحديث يعترف لصاحب هذه المعلومات بما يطلق عليه الحق في الملكية الفكرية ، ولو أن المعلومات مالا ما كان المشرع ليستطيع التسليم لها بهذا الحق و إن كانت طبيعة هذه الملكية محل جدل فقهي[1].

2ـ الإتجاه الثاني: الفقه المعارض لإضفاء وصف المال على البرامج.

الجانب الآخر من الفقه يرى عدم صلاحية المعلومات لأن تكون محلا للإعتداء عليها ، حيث ذهب

[1] ـ عطاء الله فشار، مواجهة الجريمة المعلوماتية في التشريع الجزائري، مقال منشور بكلية الحقوق و العلوم السياسية، جامعة الجلفة، ولم يذكر عنوان المجلة، العدد، و السنة، ص465.

جانب من الفقه في فرنسا أن المعلومة في حالتها المجردة و الفكرة في حد ذاتها لا تقبل التملك و الإستئثار ، وأن تداولها و الإنتفاع بها من حق الكافة دون تمييز ومن ثم لا يمكن أن تكون محلا للملكية الفكرية[1] ، ويفرق البعض الأخر بين المعلومات و البيانات التي تمت معالجتها إلكترونيا فيرون أن الأولى بإعتبار أن عنصرها الأساسي هو أن الدعامة التي تجسدها لها طبيعة غير مادية و لا سبيل من ثم إلى اختلاسها أما البيانات التي تمت معالجتها إلكترونيا فتتحدد في كيان مادي يتمثل في نبضات أو إشارات ممغنطة يمكن تخزينها على وسائط معينة و نقلها و استغلالها و إعادة إنتاجها فضلا عن إمكانية تقديرها كميا و قياسها فهي إذن ليست شيئا معنويا كالحقوق و الآراء و الأفكار بل له في العالم الخارجي المحسوس وجود مادي ووفقا لهذا الرأي فإن المعلومات إذا لم تعالج آليا عن طريق الحاسب لا تعتبر من قبيل الأموال الخاضعة للحماية الجنائية باعتبار أن هذه المعالجة تتم في صورة نبضات إلكترونية ، مما يمكن القول معه بأنه بعملية المعالجة تلك تتحول من أموال معنوية إلى أموال مادية الأمر الذي يخضعها للنصوص التقليدية لجرائم الأموال ، و يأخذ نفس حكمها البيانات المخزنة سواء في برامج الحاسب أو في ذاكرته ، وبالتالي تأخذ برامج و بيانات الحاسب حكم الأموال و بالتالي تتمتع بالحماية الجنائية المقررة لها باعتبار المعلومات مالا قابلا للتملك بالإضافة إلى مجموعة الأموال التي يحميها القانون الجنائي ، حيث يمكن إسباغ حماية النصوص التقليدية عليه و ذلك على أساس أن هذه النصوص جاءت عامة و لم يشترط أن تقع جرائم الأموال على منقول مادي ، وعليه يكون من المتصور أن تقع هذه الجرائم على مجال غير مادي طالما اعترف لها بصفة المال و قابلية التملك ، وقد سايرت هذا الإتجاه محكمة النقض الفرنسية في العديد من أحكامها[2]، ومن خلال ما سبق سنتطرق إلى الإعتداء على الأموال المادية و الأموال المعنوية.

لا يخفى علينا أن المعلومة هي أحد ثمرات الإنسان التي تتحول فيها إلى رصيد معرفي تستقي منه البشرية كل ما هي بحاجة إليه لتيسر لها سبل الحياة ، فهاته الخدمة التي يقدمها البشر لبعضهم البعض إستوجبت الإعتراف لأصحاب هاته الأعمال بحقوقهم في أن تنسب إليهم أعمالهم و يبدوا أن هذا الإعتراف ليس كافيا لإيفائهم حقهم بل لا بد من حماية الحقوق ، وتظهر صورة الأموال المعنوية في المال المعلوماتي لذلك سنتطرق:

[1] ـ عطاء الله فشار، المرجع السابق، ص465.
[2] ـ عطاء الله فشار، المرجع نفسه، ص467.

أولا: سرقة المال المعلوماتي.

في خضم التطور التكنولوجي ازدادت أهمية المعلومات ، ولا سيما تلك المخزنة داخل أنظمة المعالجة الآلية ومع الإنتشار الهائل لشبكات الإتصال الخاصة بالحاسب الآلي –الإنترنت– ازدادت صور الإعتداءات على المعلومات التي تتوقف قيمتها على ما يتوفر لها من اعتبارات الخصوصية و الأمنية ومن صور الإعتداء التي تقع على المعلومات سرقة المال المعلوماتي وهنا يثور الإشكال خاصة عندما تكون هذه المعلومات داخل الجهاز دون وجه حق أو نسخ هذه المعلومات ، وهو ما عرفه البعض سرقة المعلومات من برامج و بيانات مخزنة في دائرة الكمبيوتر بصورة غير شرعية أو نسخ برامج معلوماتية بصورة عير شرعية أو نسخ برامج بصورة غير شرعية بعد تمكن مرتكب هذه العملية من الحصول على كلمة السر أو بواسطة إلتقاط الموجات الكهرومغناطيسية الصادرة عن الحاسب الآلي أثناء تشغيله و باستخدام هوائيات موصلة بحاسبة خاصة[1].

و تتم عملية سرقة المال المعلوماتي بأشكال مختلفة ، فقد تتم عن طريق الإلتقاط الذهني للبيانات ، بالنظر و الإستماع ، وقد تتم عن طريق نسخ البيانات المخزنة إلكترونيا داخل الحاسب الآلي ، سواء أكان مخزن داخل نظام الحاسب الآلي أو على وسائط التخزين المتعارف عليها و قد ترتكب بعد تركيب من اختراق نظام الحاسب الآلي و أخيرا قد ترتكب عمليات سرقة المال المعلوماتي عن طريق اعتراض معطيات الحاسب خلال عملية نقله.

ثانيا: الملكية الفكرية

ـ معنى الملكية الفكرية: هي ثمرة الإبداع و الإختراع البشري و سمتها بعض القانونين بالملكية الذهنية [2]لأنها ترد على نتاج ذهني ، ومثالها حق المؤلف ، وحق المخترع على اختراعه وحق التاجر في علامته التجارية ، وغير ذلك.

ـ أهم المعاهدات الخاصة بحقوق الملكية الفكرية: وقد ظهرت العديد من المعاهدات التي تهدف إلى حماية الملكية الفكرية ومن السطو عليها خصوصا مع إنشاء عمليات السطو الإلكتروني على الأعمال

[1] ـ إنتصار نوري الغريب ، أمن الكمبيوتر و القانون ، دار الراتب الجامعية ، بيروت ،1994،ص57.

[2] ـ و يقصد بالملكية الذهنية تلك الحقوق التي ترد على شيء غير مادي أي غير محسوس و يطلق العلماء على هذا النوع من أنواع الحقوق اسم حقوق الابتكار و الإبداع ، و يسميها القانون بالحقوق المعنوية و هي التي تخص الحقوق الذهنية ،لأنها تتعلق بالنشاط الذهني أو الفكري.و لمزيد من التفصيل أنظر محمد محمد الشلش ، مقال بعنوان حقوق الملكية الفكرية بين الفقه و القانون ، جامعة القدس المفتوحة ، مجلة جامعة النجاح الوطنية ، فلسطين ، 2006، ص08.

الفنية دون إعطاء مالكيها حقوقهم المادية والمعنوية ومن بين هذه المعاهدات:

ـ معاهدات التعاون بشأن البراءات 1970 وهي تتضمن أحكام خاصة بالطلب الدولي للبراءة.

ـ معاهدات بودابست لعام 1977 الخاصة بإبداع الكائنات الدقيقة لأغراض الإجراءات الخاصة بالبراءات.

ـ معاهدات نيروبي لعام 1981بشأن حماية الرمز الأولمبي ، تضمن هذه المعاهدة حماية الرمز الأولمبي من استخدامه لأغراض تجارية دون تصريح من اللجنة الأولمبية.

ـ إتفاقية باريس ، تم توقيع هذه الإتفاقية في باريس عام 1983 تتضمن هذه المعاهدة أحكام براءات الإختراع و أحكام العلامات التجارية ، وأحكام الرسوم و النماذج الصناعية.

إعتبر الفقه أن الأفكار و الحقائق و النتائج هي حصيلة جهد و عمل و سهر و بحث المؤلف ، لذلك فهي من حقوقه الخاصة التي يحرص عليها ، ولقد سمى العلماء منتحل أعمال الآخرين (العلمية و الأدبية أو الفنية) سارقا ، وإذا كانت هذه المؤلفات و الإبداعات و الإبتكارات حقا لمن اجتهد في تحصيلها و تأليفها و إظهارها وقد أقر المشرع الجزائري للمؤلف بهذه الحقوق بقوله: يتمتع المؤلف بحقوق معنوية و مادية على المصنف الذي أبدعه[1].

و يمتلك المؤلف في القانون حق تقرير النشر و بطريقته ، وحق نسبة المؤلف إليه ، فيكتب إسمه و لقبه و مؤهلاته العلمية و غير ذلك ، كما يملك حقه في دفع الإعتداء عن مصنفه ، فله وحده حق التعديل و التغيير و ليس لغيره أن يباشر ذلك إلا بإذن كتابي منه أو من ورثته من بعده [2]، و يتمتع المبدع بموجب حق المؤلف وورثته بحقوق أساسية أخرى ، إذ أن لهم الحق الإستئثاري في الإنتفاع بالمصنف أو التصريح للآخرين بالانتفاع به بشروط متفق عليها ، ويمكن للمؤلف أن يمنع أو يصرح بما يلي:

1 ـ إستنساخ المصنف بمختلف الأشكال كالنشر الطبيعي أو التسجيل الصوتي.

2 ـ أداء المصنف أمام الجمهور كما في المسرحيات أو الأعمال الموسيقية.

3 ـ إجراء التسجيلات للمصنف على أقراص أو أشرطة سمعية أو أشرطة فيديو.

4 ـ بث بواسطة الإذاعة أو القنوات الفضائية.

[1] ـ أنظر المادة 21 الفقرة الأولى من الأمر رقم 03 ـ 05المؤرخ في 19 يوليو 2003 المتعلق بحقوق المؤلف و الحقوق المجاورة، ج ر،العدد 44، المؤرخة في 23،07،2003.

[2] ـ محمد محمد الشلش، حقوق الملكية الفكرية بين الفقه و القانون، المرجع السابق، ص17.

5 ـ ترجمته إلى لغات أخرى أو تحويره من قصة عمل روائي إلى عمل سينمائي أو تلفيزيوني أو إذاعي[1].

ـ الإعتداءات الواقعة على حقوق المؤلف في البيئة الرقمية:

مفهوم الإعتداء على حقوق المؤلف : الإعتداء هو تجاوز الحدود المسموح بها كما أنها انتهاك شيء محمي قانونا أو الإستعمال بدون وجه حق لشيء ما دون استئذان صاحبه أو مالكه ، و الإعتداء على حقوق المؤلف هي الإستغلال أو الإستعمال غير المشروع لحق من حقوق المؤلف المنصوص عليها دون إذن من صاحبها أي المؤلف أو من آلت إليه الملكية لذلك سنتطرق إلى :

1ـ أنواع التعديات الواقعة على حق المؤلف:

رغم أن حقوق المؤلف أحد أقسام الملكية الفكرية و يحميها قانون الملكية الفكرية و الأدبية و الفنية غير أنه من جانب التجريم و العقوبات و الحماية الجنائية فيحميها قانون العقوبات ، وفي كثير من الدول تعتبر من الجرائم الواقعة على الأموال لأن نتاج المؤلف أي المصنف هو مال منقول لذا تطبق عليه هذه القوانين و أهم هذه الإعتداءات هي الإعتداء على حق من حقوق المؤلف الأدبية أو المالية أو على أصحاب الحقوق كمنع المؤلف مثلا من نشر مصنفه أو نسبته إلى غير مؤلفه الحقيقي ، أو القيام بتعديل و تشويه أو تحريف يؤدي بالأضرار بحقوق المؤلف المادية و هز و زعزعة مكانته في التمتع ، وكل هذه الإعتداءات تقع في غياب ترخيص من المؤلف للمعتدي و من شروط هذا الإذن أو الترخيص أن يكون مكتوبا[2].

كما يمكن أن يقوم المعتدي بنشر المؤلف على شبكة الإنترنت دون أن يستأذن مؤلفه و كم هي كثيرة هذه الحوادث خاصة في عصرنا الرقمي هذا فهناك من رقمن كتبا و مؤلفات كثيرة ووضع منها مكتبة رقمية على شبكة الإنترنت دون استئذان من أصحابها ، كما قد تباع أو تأجر مصنفات محمية و يعتبر هذا أيضا إعتداءا على حقوق المؤلف دون وجه حق ، وقد يكون الإعتداء لغرض البيع أو التأجير أو التداول لأي مصنف أو نسخ مقلدة أو لأية أجهزة ووسائل أو رسائل أو أدوات مصممة للتحايل على الحماية الفنية لهذه المصنفات ، و يتحقق بتغيير المعطيات الموجودة داخل النظام و

[1] ـ محمد محمد الشلش ، المرجع السابق ، ص17.

[2] ـ حقاص صونية ، حماية الملكية الفكرية الأدبية و الفنية في البيئة الرقمية في ظل التشريع الجزائري، مذكرة ماجستير، جامعة قسنطينة، 2002، ص67.

استبدالها بمعطيات أخرى بالإضافة إلى التعطيل أو التعييب دون وجه حق لأي حماية تقنية أو معلومات إلكترونية تستهدف تنظيم و إدارة الحقوق المقررة في بعض القوانين بالإضافة إلى تحميل أو تخزين على الحاسب بأية نسخة من برامج الحاسوب وتطبيقاته أو قواعد البيانات دون ترخيص من المؤلف أو صاحب الحقوق أو خلفهما ، ولقد إتبعت هذه الجرائم منتجي المعلومات و كذا التقنين و كذلك القضاة لكن لم يقف أصحاب هذه الحقوق بمساندة الدولة مكتوفي الأيدي بل وجد حلا تتكاثف فيه جهود كل الأطراف لحماية هذه الحقوق وهي ما يعرف بالإدارة الجماعية لحقوق المؤلف[1].

2 ـ الإعتداءات الواقعة على حقوق المؤلف في المكتبة الرقمية:

لم تشهد المكتبات التقليدية إنتهاكات كبيرة فيما يخص حقوق المؤلف في هذه البيئة الورقية و حتى و إن حصل ذلك فمن السهل اكتشاف الإعتداء و كذلك من السهل تطبيق القوانين التي نصت عليها التشريعات بوضوح و دون التباس مقارنة بما يحصل اليوم في بيئة أكثر ما يميزها هو السرعة الفائقة في انتشار المعلومة بمجرد ضربة واحدة أو نقرة على الفأرة أو زر من أزرار لوحة مفاتيح الحاسوب ، كما أن الوسائل التكنولوجية الحديثة ساهمت و بشكل رهيب في انتشار هذه الإعتداءات حتى و لو لم يكن سبب اختراعها هو انتهاك أو المساهمة في الإعتداء على حقوق الغير في حين أن ذلك يكون بطريقة غير مباشرة و بوعي أو دون وعي من مستعمل هذه الوسائل أو التقنيات الحديثة ، كما أن شراء المكتبة للنسخة المطبوعة يخولها إعارتها لمن يريد و بأي عدد من المرات و بدون الحصول على أي ترخيص من مالك حقوق النشر[2]، كما أن المستفيد من المكتبة التقليدية يقوم باستعارة وعاء المعلومات من أجل القراءة و الإطلاع ومن ثم يقوم بإعادته للمكتبة بينما في المكتبة الرقمية فالأمر مختلف تماما ، فلا توجد هناك عملية إستعارة أساسا فالمستفيد يقوم بعملية إنزال مصدر المعلومات الرقمية من موقع المكتبة مما يخوله الملكية الكاملة ، كما أن المكتبة تتيح أي عدد مهما بلغ من عمليات إنزال مصدر المعلومات الرقمي ، و قد يتعدى الأمر إلى تغيير في المحتوى أو حتى العنوان و استبدالها بأفكار ربما تكون غير ملائمة لمعتقدات و أفكار المؤلف الأصلي مما يجعل في ذلك خطرا على سمعته الفنية بين قرائه و حتى مع الناشرين.

[1] ـ حقاص صونية، المرجع السابق، ص67.
[2] ـ حقاص صونية، المرجع نفسه، ص67

كما أن في هذا التنزيل أو النسخ غير الرخص به إعتداء على حقوق النشر بحيث أنه سيتم نشر المصنف بطرق غير مشروعة و ربما بأقل تكلفة و أقل جهد مما يجعل في ذلك إعتداءا على حقوق الناشر و بالتالي حقوق المؤلف المالية خاصة ، كما أننا نجد أن هناك خصائص في المكتبة الرقمية تفيدها كثيرا في جلب أكبر عدد ممكن من المستفيدين غير أن هذا خطير جدا على حقوق المؤلفين و الناشرين خاصة إذا لم تحدد أمور كثيرة لها علاقة بطريقة تداول المصنف في هذه البيئة ضمن ما يعرف بعقود التراخيص و التي تتم في أغلب الأحيان بين مسؤولي المكتبة و مالكي الحقوق أو ممثل عنهم[1].

ثالثا ـ جريمة تجارة المخدرات الرقمية:

تنفذ هذه الجرائم بالخصوص عبر تلك المواقع المنتشرة عبر الشبكة و التي تتعلق بالترويج للمخدرات و التسويق السيئ لاستخدامها بل تتعداه إلى تعليم كيفية زراعة و صناعة المخدرات بكافة أصنافها و بيعها[2]، ولا يقتصر الأمر على هذه المواقع فحسب بل تساهم حتى المنتديات و غرف الدردشة في ذلك فلم يعد إستهلاك المخدرات يقتصر على ما كان يجري سابقا بحقنها في الوريد أو بمضغها أو شمها....وإنما تطور الفكر الإنساني ليحول نظام التعاطي إلى تعاطي إلكتروني أو تعاطي رقمي يحدث ذات التأثير الذي تحدثه المخدرات الطبيعية ، ويتمثل تعاطي المخدرات عبر شبكة الإنترنت في جلوس تاجر المواد المخدرة أمام جهاز الحاسب الآلي الخاص به ليتلقى طلبات الشراء للمواد المخدرة عبر موقعه الإلكتروني، وهنا لا يقوم بإرسال أحد تابعيه ليسلم المادة المخدرة المشتراة ، وإنما يقوم المشتري بإجراء عملية تحميل المخدر الذي يرغب في شكل ملفات وهو ما يعرف بالمخدرات الرقمية.

و المخدرات الرقمية عبارة عن ملفات صوتية تحتوي على نغمات أحادية أو ثنائية يستمع إليها المستخدم تجعل الدماغ يصل إلى حالة من الخدر تشابه تأثير المخدرات الحقيقية أو على الأقل هذا ما يدعيه البعض ، وقد صممت هذه الملفات الصوتية ـ أو المخدرات الرقمية ـ لمحاكات الهلاوس و حالات الإنتشاء المصاحب لتعاطي المواد المخدرة عن طريق التأثير على العقل بشكل اللاوعي هذا التأثير الذي يحدث عن طريق موجات صوتية غير سمعية للأذن تسمى الضوضاء البيضاء مغطاة

[1] ـ حقاص صونية، المرجع السابق، ص 80.

[2] محمد محمد صالح الالفي، بحث علمي بعنوان:أنماط جرائم الانترنت، ص 11 منشور على الموقع التالي http// www.eastlaws.com وتم الاطلاع على هذا الموقع بتاريخ 2017.06.28

ببعض الإيقاعات البسيطة لتغطية إزعاج تلك الموجات كما وجدت المخدرات الرقمية رواجا هائلا بين مستخدمي الإنترنت و خاصة بين فئة الشباب[1].

وقد ذكر موقع "سي نت "الأمريكي أن عدد الملفات الموسيقية التي قام بتحميلها تكرر إستعمالها أكثر من 1.4 مليون مرة خلال أسبوع واحد، بينما يقوم موقع "آي دوزر" بعملية إغراء مكشوفة إذ يمنح مستخدميه تجربة مجانية في البداية و يشجع المروجين لبيع ملفاته على شبكة الإنترنت لقاء عمولة تزيد على 20% و يتراوح سعر الملف الواحد بين 3 و 9 دولارات، بينما يكون الملف الأول للمستخدم مجانيا و تنقسم الملفات أو الجرعات كما يسميها الموقع إلى تصنيفات مثل هلوسة مخدرات روحية ، جنسية ، سعادة ، مضادات للقلق ، مخدرات سريعة ، مخدرات تقنية.

هذا الإنتشار المزعج للمخدرات الرقمية دعا المدارس في الولايات المتحدة الأمريكية إلى منع دخول أجهزة الآي بود ipod من أجل مكافحة مسألة الإدمان الرقمي ، كما ذكر بيان صادر عن مكتب مكافحة المخدرات الأمريكي أن خطورة هذا النوع الجديد من المخدرات تكمن في صعوبة ضبطها ، كما أنها قد تقود المدمن إلى أماكن أخرى لا نستطيع التكمين بها لأن كل شيء يجري في عالم إفتراضي ، وقد احتلت أخبار هذا الوباء القادم أغلب المواقع الإخبارية في العالم التي نوهت عن المخاطر الكبيرة التي يمكن حدوثها من وراء هذه المخدرات الرقمية خوفا من إمكانية تطوير هذه الأفكار لتصبح وباء يخرج عن السيطرة ، أما في وطننا العربي فلم يتخلف كعادته عن الركب حيث أكدت المواقع على أن الكثير من المنتديات العربية بدأت تروج إلى[2] هذه النوعية من المخدرات الرقمية حتى أن بعضها قدم للمشتركين جرعات مجانية للتحميل.

رابعا: جرائم الإعتداء على البيانات.

1ـ جرائم المعالجة الإلكترونية للبيانات الشخصية دون ترخيص: إن اقتراف هذا النوع من الجرائم المتمثلة في المعالجة الإلكترونية للبيانات الإسمية يتم دون مراعاة للإجراءات الأولية و يلزم لقيامه توافر عنصرين أساسيين:

أولا: سلوك إجرامي يتخذ شكل المعالجة الإلكترونية للبيانات أو تسجيلها ، تحليلها و تصنيفها ثم

[1] ـ أبو سريع أحمد عبد الرحمن، بحث علمي بعنوان إستخدام الانترنت في تعاطي المخدرات ـ المخدرات الرقمية ـ في ديسمبر 2010 ،ص 05، 06 على الموقع www.child-trafficking.org وتم الاطلاع على الموقع بتاريخ 15،06،2017.

[2] ـ أبو سريع أحمد عبد الرحمن، المرجع نفسه، ص 08، 09.

حفظها أو محوها و يكون الفعل قد تم حتى و لو كانت المعالجة بإهمال من الفاعل.

ثانيا: عدم مراعاة الإجراءات الأولية الخاصة بالمعالجة الإلكترونية للبيانات الشخصية بدون ترخيص من الجهات المعنية و التي تمت معالجة بياناتها.

2- جريمة التسجيل غير المشروع للبيانات الإسمية : وهي كل طلب لإجراء معالجة إلكترونية دون أن يأخذ الجاني كل الإحتياطات المجدية لضمان أمن هذه المعلومات وعلى وجه الخصوص من تشويهها أو إتلافها أو الوصول إليها عن طريق التدليس و الغش من شخص غير مصرح له بذلك.

3 ـ جريمة الحفظ غير المشروع للبيانات الإسمية: هي كل حفظ للبيانات و المعلومات دون تصريح مسبق و لمدة تزيد عن المدة التي سبق طلبها أو التي تضمن الأخطار المسبقة ومنع الكشف عنها من قبل أشخاص غير مرخص لهم بالإطلاع عليها[1].

4- جريمة الإنحراف عن الغرض أو الغاية من المعالجة الإلكترونية للبيانات الإسمية : تتوفر هذه الجريمة عند كل حيازة بيانات إسمية بمناسبة قيام الجاني بتسجيلها أو تصنيفها أو نقلها أو أي إجراء آخر من أوجه المعالجة إذا غير من الوجهة النهائية المقررة لهذه البيانات.

5- جريمة الإفشاء غير المشروع للبيانات الإسمية : تنحصر هذه الجريمة في استقبال أو تلقي كل شخص بمناسبة التسجيل أو التصنيف أو النقل أو أي إجراء آخر من إجراءات المعالجة الإلكترونية لكل البيانات الإسمية التي من شأنها أن تفشي السر عن صاحب الشأن أو حرمة حياته الخاصة وتم نقلها إلى من لا حق له في الإطلاع عليها و حتى و لو كان ذلك عن طريق الإهمال ، و تتم هذه الجريمة بناءا على شكوى يتقدم بها المجني عليه أو ممثله الرسمي أو القانوني.

6 ـ جريمة الإلتقاط غير المشروع للبيانات: و تتمثل هذه الجريمة في الدخول غير المشروع إلى النظام المعلوماتي أو البقاء فيه دون إذن من قبل صاحبه ، حيث يتيح للمجرم المعلوماتي ممارسة نشاطاته الإجرامية من أجل تحقيق مكاسب شخصية متباينة و متعلقة بذات الجرم من إلتقاط البيانات المخزنة

[1] ـ مقال بعنوان الجريمة الإلكترونية منشور على الموقع الآتي :www.droit-dz.com و قد تم الإطلاع على الموقع بتاريخ 29،10، 2017

في قواعد البيانات أو المتبادلة عبر قنوات الإنترنت لإستخدامها للأغراض الشخصية بطرق غير شرعية[1].

7 ـ جرائم سرقة منفعة الحاسب الآلي: و يقصد بجرائم سرقة منفعة الحاسب الآلي هو استخدامه لأغراض شخصية أو تجارية بدون علم مالكها أو حائزها القانوني ، في وقت معين لتحقيق أهداف ذاتية قد تكون دون ربح أو استفادة كالأعمال الخيرية و نسخ ألعاب الفيديو أو غيرها من الأعمال التي تتم عبر الحاسب.

8ـ جريمة إتلاف نظام المعلوماتية عبر الإنترنت: تقع هذه الجريمة بالإعتداء على الوظائف الطبيعية للحاسب الآلي وذلك بالتعدي على البرامج و البيانات المخزنة و المتبادلة بين الحواسب و الشبكات الداخلية أو العالمية و يكون ذلك عن طريق التلاعب بالبيانات ، سواء بإدخال معلومات مصطنعة أو إتلاف معلومات مخزنة بالحواسب و المتبادلة عبر الشبكة العالمية بمحوها أو تعديلها أو تغير مناهجها أو بطريقة التشويش على النظام المعلوماتي مما يؤدي إلى سير عمل النظام الآلي بصورة مختلفة و يكون هذا الإتلاف العمدي للبرامج و البيانات ومحوها أو تدميرها إلكترونيا بصفة كاملة ، وتأخذ جريمة الإتلاف في نطاق المعلوماتية إما صورة الإتلاف المادي و هذا بالإعتداء على المكونات المادية للحاسب أو صورة الإعتداء على البرامج أو البيانات و المعلومات المخزنة في قواعد الحواسب[2].

9 ـ جرائم و صور الإعتداء على البيانات و البرامج داخل نظام المعالجة الآلية للبيانات: و تهدف هذه الجرائم إلى إتلاف البيانات و الأموال اللامادية سواء بمحوها أو تدميرها إلكترونيا أو تشويشها أو تعديل طرق معالجتها و قد تكون نتيجة إستخدام الطرق التقنية و الفنية كفيروسات الحاسب الآلي أو التدخل في المعطيات كإدخال معلومات وهمية في النظام المعلوماتي و تزوير المعطيات الموجودة قصد تزوير بيانات مخزنة على الكمبيوتر و يتم وضع معلومات أخرى بديلة للمعلومات الحقيقية و تزييف المخرجات و تمس جميع المبادلات المعلوماتية عبر الشبكة هذا من جهة أما من جهة أخرى فيتم التدخل في الكيان المنطقي و المتمثل في مجوعة البرمجيات المخصصة للقيام بالمعالجة و يتم

[1] ـ الجريمة الإلكترونية، الموقع السابق.
[2] ـ الجريمة الإلكترونية، الموقع نفسه.

ذلك إما بتعديل برنامج معين أو التلاعب بداخله أو خلق برنامج جديد وهمي مصطنع يهدف للغش المعلوماتي.

10 ـ الجرائم المستعملة بالطرق الفنية لإتلاف المال المعلوماتي: و تتمثل هذه الجرائم في طرق فنية و تقنية مستخدمة في إتلاف البيانات و البرامج بدءا من فيروسات الحاسب الآلي مزودة ببرامج الدودة و انتهاء بالقنابل المنطقية أو الزمنية و كل ذلك يؤدي إلى الإتلاف الذي يترتب عنه مشاكل قانونية[1].

[1] ـ الجريمة الالكترونية، الموقع السابق.

المبحث الثاني: الجرائم الماسة بالأمن الوطني عبر المعطيات الرقمية (الإرهاب الإلكتروني).

يعد الإرهاب الإلكتروني من أخطر الإرهاب على الدول في العصر الحاضر ، نظرا لاتساع نطاق استخدام التكنولوجيا في العالم ، وقد أدى ظهور هذا النوع من الإرهاب إلى جرائم مست أمن الدول خاصة المتطورة كالتجسس و الإختراقات البنكية المالية و المعلوماتية منها ناهيك عن الدول المتخلفة ، ومصطلح الإرهاب الالكتروني الذي ظهر وشاع استخدامه عقب الطفرة الكبيرة التي حققتها تكنولوجيا المعلوماتية و استخدامات الحواسيب الآلية و الإنترنت تحديدا في إدارة معظم الأنشطة الحياتية ، وهو الأمر الذي دعا 30 دولة إلى التوقيع على الإتفاقية الدولية الأولى لمكافحة الإجرام عبر الإنترنت في بودابست عام 2001 و الذي يعد من أخطر أنواع الجرائم التي ترتكب عبر شبكة الإنترنت ، ويتضح هذا جليا من خلال النظر إلى فداحة الخسائر التي يمكن أن تسببها عملية واحدة تكون ناجحة تدرج تحت مفهومه.

وقد كشف خبير الإرهاب الدولي الأمريكي **جابر ويمان** عن زيادة كبيرة في عدد المواقع الإلكترونية التي تديرها المنظمات الإرهابية على شبكة الإنترنت العالمية، فقد قفز عدد تلك المواقع من 12 موقع عام 1988إلى 4800 موقع في الوقت الحالي.

وقال الخبير الدولي إن الإرهاب الحديث أصبح أكثر ضراوة لإعتماده على التكنولوجيا المتطورة للإنترنت مما زاد من اتساع مسرح عملياتهم الإرهابية ، وبالتالي أصبح من الصعب اصطياد هذا الوحش الإلكتروني الجديد[1]، لذلك قسمنا هذا المبحث إلى مطلبين تناولنا في المطلب الأول : ماهية الإرهاب الإلكتروني ، أما في المطلب الثاني مظاهر الإرهاب الإلكتروني.

المطلب الأول: مفهوم الإرهاب الإلكتروني.

لقد أدى ظهور الحاسبات الآلية إلى تغيير شكل الحياة في العالم ، وأصبح الإعتماد على وسائل تقنية المعلومات الحديثة يزداد يوما بعد يوما ، سواء في المؤسسات المالية ، أو المرافق العامة ، أو المجال التعليمي أو الأمني أو غير ذلك ، ويبدوا أنه و إن كان للوسائل الإلكترونية الحديثة ما يصعب حصره من فوائد ، فإن الوجه الآخر و المتمثل في الإستخدامات الضارة لهذه التقنيات الحديثة ومنها الإرهاب الإلكتروني صبح خطرا يهدد العالم بأسره ، إن خطر الإرهاب الإلكتروني يكمن في سهولة استخدام

[1]-علي عدنان الفيل ، الإجرام الإلكتروني دراسة مقارنة، منشورات زين الحقوقية و الأدبية، الطبعة الأولى، سنة 2011، ص50.

هذا السلاح مع شدة أثره وضرره فيقوم مستخدمه بعمله الإرهابي و هو في منزله أو مكتبه أو في مقهى أو حتى في غرفته في أحد الفنادق.

حقا لقد أصبح الإرهاب الإلكتروني هاجسا يخيف العالم الذي يتعرض لهجمات الإرهابيين عبر التكنولوجيا، و بث أفكارهم المسمومة ، ومما يزيد الأمر صعوبة ، أن التقدم الإلكتروني لا يتوقف لحظة ، لذا يجب على الأفراد مواجهة هذه العمليات الإرهابية التي تتخذ من التقنية أداة لتنفيذ مخططتها.

و نظرا للتطور الرهيب و المتنامي في مجال الإنترنت و تكنولوجيا المعلومات فإن الإرهابيين سوف يكونون أكثر اعتمادا على تكنولوجيا الإتصالات الإلكترونية في المستقبل ، و سوف يصبح الإرهاب أكثر تعقيدا أو خطورة ، فلا يجب البتة المبالغة في حجم الأخطار الحالية حتى يتسنى مواجهة تلك التحديات بشيء من الروية و حسن التصرف ، وكما يستطيع الإرهابيون استخدام تلك الشبكة بكفاءة كذلك يستطيع صانعوا السلام إستخدام الإنترنت لموهبتهم و المقصود هو نشر الأفكار السامية و المتحضرة التي تدعوا إلى السلام و المحبة و التعايش السلمي بين الحضارات المختلفة ، و بالتالي تطغى تلك المواقع الصالحة على السموم التي تنشرها المواقع الإلكترونية الإرهابية تلك الأنشطة التي تدعم الدبلوماسية و إدارة الأزمات السياسية بالطرق السلمية عبر الشبكات العالمية للإنترنت ، كما أنه لابد و أن تسعى الدول و الحكومات إلى فرض الرقابة الكافية على كل ما تقدم من خلال الشبكة لمنع الدخول على بعض المواقع التي تبث الفكر الإرهابي، لذلك تسعى هذه الدراسة إلى تسليط الضوء على تعريف الإرهاب الإلكتروني في الفرع الأول وفي الفرع الثاني: أسباب الإرهاب الإلكتروني.

الفرع الأول: تعريف الإرهاب الإلكتروني.

من المعلوم أن التطور الذي شهده العالم اليوم على جميع الأصعدة كان نقطة تحول و قسم العالم إلى شقين: شق متطور جدا و شق متخلف ، وقد كان لتكنولوجيا الإتصالات مكانتها البارزة لكن البعض من هذه الدول استغلها لأعمال إرهابية ، لذلك يعتبر الإرهاب من الظواهر الإجرامية التي تجاوزت آثارها حدود الدولة الواحدة فاكتسب بذلك طابعا عالميا يهدد أمن و سلامة البشرية و حقوق الإنسان ، وحرياته الأساسية ، و مصالح الشعوب الحيوية و ذلك بهدف إحداث تغييرات في الأوضاع الدولية.

وعليه يجب وصف الظاهرة الإرهابية باتزان و تجرد و شمول لأنه في عصرنا هذا قاما استعملت كلمة ـ أسيئ استعمالها ـ أو استعملت على نحو تعسفي مثل كلمة إرهاب فلطالما اعتبر لفظ الإرهاب لفظا معقدا في مدلوله ، و هذا راجع لاختلاف وجهات النظر حوله ، وخاصة على مستوى القانون الدولي ، و هذا لإختلاف مصالح الدول وتباينها[1]و عليه سنتطرق إلى تعريف الإرهاب بشكل عام في الإتفاقيات الدولية ، والتعريف الفقهي ثم التشريعات بعدها سنتطرق إلى تعريف الإرهاب الإلكتروني بشكل خاص.

وقد ظهرت عدة تعريفات للإرهاب الإلكتروني ومن بينها:

أنه يعتبر الإرهاب الإلكتروني تلك الهجومات غير المشروعة ، أو تهديدات لهجمات ضد الحاسبات أو الشبكات أو المعلومات المخزنة إلكترونيا، توجه من أجل الإنتقام أو ابتزاز أو إجبار أو التأثير في الحكومات أو الشعوب ، أو المجتمع الدولي بأسره لحقيق أهداف سياسية أو دينية أو إجتماعية معينة ، وبالتالي فلكي ينعت شخصا ما بأنه إرهابي إلكتروني، وليس فقط مخترقا، فلابد و أن تؤدي الهجمات التي شنها إلى عنف ضد الأشخاص أو الممتلكات، أو على الأقل تحدث أذى كافيا من أجل نشر الخوف و الرعب[2].

كذلك هناك من عرف الإرهاب الإلكتروني بأنه كل من يعتمد على استخدام الإمكانيات العلمية و التقنية ، و استغلال وسائل الإتصال و الشبكات المعلوماتية ، من أجل تخويف و ترويع الآخرين ، و إلحاق الضرر بهم أو تهديدهم مثل ما حصل في عام 200 م حينما أدى فيروس الحاسوب

I LOVE YOU إلى إتلاف معلومات قدرت قيمتها بنحو 10 مليارات دولار أمريكي ، وفي عام 2003 ، شاع فيروس في نصف مليون جهاز من أجهزة الحاسوب ، وقدر مجلس أوربا في الإتفاقية الدولية لمكافحة الإجرام عبر الأنترنت كلفة إصلاح الأضرار التي تسببها فيروسات المعلوماتية بنحو 12 مليار دولار أمريكي سنويا[3].

لكن بعض الفقهاء لم يشيروا صراحة إلى الإرهاب الإلكتروني لكنهم عبروا عن ذلك بالإرهاب المعلوماتي أو بالإجرام الإلكتروني لذلك سنطرق إلى تعرف الإجرام المعلوماتي ثم إلى الإرهاب المعلوماتي:

---

[1]- وحمود عرابي ، الارهاب ،مفهومه ،أواعه ، أسبابه آثاره ، أسباب المواجهة ، دار الثقافة للنشر ، الطبعة الأولى ، القاهرة 2007،ص40

[2]- علي عدنان الفيل ، المرجع السابق ، ص60.

[3]- إيهاب شوقي ،الإرهاب الإلكتروني ، مقال منشور بتاريخ 11ديسمبر 2015على الموقع الآتي http//www.assakina.com وقد تم الإطلاع على هذا الموقع بتاريخ 18-11-2016.

1 – الإجرام الإلكتروني:

إختلف الفقه حول تعريفه وانقسم الفقهاء إلى اتجاهين ،الإتجاه الأول: دعا إلى التضييق في مفهوم الجريمة الإلكترونية و عرفها على أنها كل سلوك غير مشروع أو غير مسموح به يتعلق بالمعالجة الآلية للبيانات و نقله.

أما الإتجاه الثاني: فدعا إلى التوسع و عرف الجريمة الإلكترونية بكل الأفعال غير المشروعة التي يستخدم فيها الحاسوب[1].

2–الإرهاب المعلوماتي:

و يتمثل في استخدام المواد المعلوماتية ، و المتمثلة في شبكات المعلوماتية وأجهزة الكمبيوتر و شبكة الإنترنت ، من أجل أغراض التخويف أو الإرغام لأغراض سياسية ، و يرتبط هذا الإرهاب إلى حد كبير بالمستوى المتقدم للغاية الذي باتت تكنولوجيا المعلومات تلعبه في كافة مجالات الحياة في العالم ، وقد يتسبب الإرهاب المعلوماتي في إلحاق الشلل بأنظمة القيادة و السيطرة و الإتصالات أو قطع شبكات الإتصال بين الوحدات و القيادات المركزية ، و تعطيل أنظمة الدفاع الجوي أو إخراج الصواريخ عن مسارها أو اختراق النظام المصرفي أو إرباك حركة الطيران المدني أو شل محطات الطاقة الكبرى[2].

وقد عرف المستشار القانوني أمير فرج يوسف الإرهاب الإلكتروني بأنه: العدوان أو التخويف أو التهديد المادي أو المعنوي الصادر من الدول أو الجماعات أو الأفراد على الإنسان ، في دينه أو نفسه أو عرضه أو عقله أو ماله بغير حق باستخدام الموارد المعلوماتية والوسائل الإلكترونية ، بشتى صنوف العدوان و صور الإفساد ، فالإرهاب الإلكتروني يعتمد على استخدام الإمكانيات العلمية و التقنية ، واستغلال و سائل الإتصال و الشبكات المعلوماتية من أجل التخويف و ترويع الآخرين وإلحاق الضرر بهم أو تهديدهم.

وعليه يمكننا تعريف الإرهاب الإلكتروني:

بأنه تلك الأعمال و الأنشطة غير المشروعة التي يقوم بها الأفراد أو الجماعات باستخدام تكنولوجيا

[1]- هدى حامد قشقوش، جرائم الحاسوب الآلي في التشريع المقارن، دار النهضة العربية، القاهرة، 1992، ص20.
[2]- أمير فرج يوسف، الجريمة الإلكترونية و المعلوماتية، المرجع السابق، ص206.

المعلومات و الشبكة العنكبونية من العدوان و التخويف المادي و المعنوي ، وإحداث جرائم تمس المعلومات الخاصة بالدول و البيانات خاصة السرية منها ...الخ من هذه الأعمال غير القانونية.

الفرع الثاني: أسباب ظهور الإرهاب الإلكتروني وعوامل انتشاره.

إن أكثر الأنظمة التقنية تقدما و أسرعها تطورا هي الأنظمة الأمنية ، وعلى الرغم من سرعة تطورها إلا أنها أقل الأنظمة استقرارا و موثوقية ، نظرا لتسارع وتيرة الجرائم الإلكترونية و أدواتها و التغييرات الأمنية التي لا يمكن أن يتم الحد منها على المدى الطويل ، فمجال أمن المعلومات في الإنترنت أخذ في التطور بشكل كبير تماشيا مع التطور في الجريمة الإلكترونية.

ولقد أصبح الإرهاب الإلكتروني هاجسا يخيف العالم الذي أصبح عرضة لهجمات الإرهابيين عبر الإنترنت الذي يمارسون نشاطهم التخريبي و بث أفكارهم المسمومة من أي مكان في العالم وهذه المخاطر تتفاقم بمرور كل يوم ، لأن التقنية الحديثة وحدها غير قادرة على حماية الناس من العمليات الإرهابية و الإلكترونية ، والتي سببت أضرارا جسيمة على الأفراد و المنظمات و الدول ، ولقد سعت العديد من الدول إلى اتخاذ لعديد من التدابير و الإحترازات لمواجهة الإرهاب الإلكتروني.

بعد التطور الذي شهده عالم التكنولوجيا خاصة في زمن قيام حكومات إلكترونية ، دفع ذلك نمط الحياة إلى التغيير و بالتالي ظهور أنماط جديدة من الجريمة و التي قد يحتفظ بعضها باسمها التقليدي مع تغيير جوهري أو بسيط في طرق ارتكابها ، والتي أخذت أشكال حديثة تتماشى مع التطور التقني ، فقد غدا الإرهاب الإلكتروني هو السائد حاليا ، وأصبح اقتحام المواقع و تدميرها و تغيير محتوياتها و الدخول على الشبكات و العبث بمحتوياتها بإزالتها أو بالإستيلاء عليها أو الدخول على شبكات الإتصالات أو شبكات المعلومات بهدف تعطيلها عن العمل أطول فترة ممكنة، أو تدميرها نهائيا أصبح هو أسلوب الإرهاب حاليا في محاولة الوصول إلى أغراضه.

و الإرهاب الإلكتروني اليوم يأخذ أشكالا متعددة حتى أصبحت الجريمة اليوم دولية ، وقد أصبحت ثورة المعلومات تساعد في نقل أدوات الجريمة المنظمة و التزوير..وهذه كلها مفاسد تغزو العالم اليوم ، و يحظى هذا النوع من الإرهاب بجاذبية خاصة عند الجماعات الإرهابية، وذلك لأن الإنترنت مجال مفتوح وواسع ، ليس له حدود ، يتوسع في كل يوم و يمكنهم الوصول إلى أي مكان في العالم دون أوراق أو قيود ، كل ما يحتاجه هو بعض المعلومات ليستطيع اقتحام الحوائط الإلكترونية، كما أن

تكاليف القيام بمثل هذه الهجمات الإلكترونية قليلة بسبب التوسع في استخدام الإنترنت باعتبارها وسيلة لتسهيل عمليات الإختراق و سرقة المعلومات ، مما زاد في عدد هذه الجرائم في المنطقة خاصة العربية[1].

ومما زاد في اتساع مسرح عملياتهم الإرهابية ، وقد صرح أحد الباحثين في هذا الصدد بأن الإرهاب الرقمي أو الإلكتروني أصبح بأهمية و خطورة الكلاشينكوف و القذيفة قائلا على لسان أحد قادة الإرهاب عندما ذكر بالحرف إننا نخوض أكثر من نصف معركتنا في الساحة الإلكترونية و الإعلامية ، وقدم هذا الإرهابي نصيحته لكوادره قائلا : عليكم أن تدركوا أن كل لقطة تلتقطونها هي بأهمية صاروخ يطلق على العدو ....لقد استغل الإرهاب الحاسب ، و الكاميرا إلى أقصى حد ممكن فأصبحت تقدم أدلة عسكرية على شكل كتب و أقلام ، حيث تتضمن معلومات شتى عن الأسلحة و تقنيات وضع المتفجرات و السموم ، لقد أصبحت شبكة الإنترنت الواسعة و كأنها معسكر تدريب إفتراضى للإرهابيين ، ولقد أصبح كل ما يحتاجه الإرهابي المحترف في هذا المجال الحيوي و المعقد هو جهاز حاسب آلي و اتصال شبكة الانترنت مما يتيح لهذا الإرهابي القيام بأعمال تخريبية وهو آمن في مقره بواسطة نقرات بسيطة على لوحة المفاتيح قد تنطوي على أوامر موجهة لبعض الخلايا للقيام بأعمال إرهابية معينة.

كما أن الوجود الإرهابي النشيط على الشبكة العنكبوتية متنوع و مراوغ بصورة كبيرة ، فإذا ظهر موقع إرهابي اليوم فسرعان ما يتغير نمطه الإلكتروني ، ثم يختفي ليظهر مرة أخرى بشكل و عنوان إلكتروني جديدين بعد فترة قصيرة و مما لا شك فيك أن الإرهاب الإلكتروني أو المعلوماتي هو إرهاب الغد نظرا لتوسع و تعدد مجال الأهداف التي يمكن مهاجمتها مع توفير قدر كبير من السلامة للمهاجمين و عدم تعرضهم لخطر إكتشاف هوياتهم أو حتى المواقع التي شنوا هجومهم عليها إلا بعد وقت طويل وجهد في البحث ، هذا الإرهاب يله خسائر غير متصورة و هائلة ، فتوقف التجارة الإلكترونية مثلا ليوم واحد قد يتسبب في خسائر لأكثر من ستة مليارات و نصف المليار دولار و هكذا يمكن منظمة إرهابية من إلحاق الكثير من الأذى و الخلل في أعمال البنوك ، و البورصات و

[1]- عبد الحميد ابراهيم، العلاقة بين الإرهاب المعلوماتي و الجرائم المنظمة، الدورة التدريبية مكافحة الجرائم الإرهابية المعلوماتية خلال الفترة من 9-13 مارس 2016 بالقنطيرة بالمغرب، ص، ص 5.4.3.

حركة الطيران بل وحتى تغيير مواصفات تركيبية لأدوية في مصانع الأدوية مما يترتب عليه خسائر في أرواح البشر[1]، ومن خلال ما سبق ذكره يمكن القول أن أسباب الإرهاب الإلكتروني تتمثل في:

1- ضعف بنية الشبكات المعلوماتية و قابليتها للإختراق:

إن شبكات المعلومات مصممة في الأصل بشكل مفتوح دون قيود أو حواجز أمنية عليها ، رغبة في التوسع و تسهيل دخول المستخدمين و تحتوي الأنظمة الإلكترونية والشبكات المعلوماتية على ثغرات معلوماتية و يمكن للمنظمات الإرهابية إستغلال هذه الثغرات في التسلل إلى البنى المعلوماتية التحتية و ممارسة العمليات التخريبية و الإرهابية[2]، مثل ما دمرت منظمة إرهابية في استراليا عام 2000شبكة الصرف الصحي بواسطة عملية إلكترونية كما العالم نفسه عندما أفلحت منظمة أومشيريكو الإرهابية اليابانية من إختراق نظام البرمجة المتحكم في مسار أعداد هائلة من سيارات الخدمة العامة ، وقد نجحت تلك المنظمة بواسطة التلاعب بأنظمة الحاسب من تعطيل أنظمة عشر إدارات حكومية و توجيهها لصالحها ، و لم يتم اكتشاف هذه الإختراقات إلا بعد أن تكبدت الشريكات و الحكومة خسائر باهضة ، كذلك استطاعت إحدي النظمات الإرهابية من مسح جميع البيانات السكانية للبيانات بواسطة اختراق أحد المواقع الحكومية، وفي عام2000 وحدة حصلت أكثر من مائة و ثمانين ألف حالة اختراق إلكترونية لمؤسسات إقتصادية ومالية كبرى غير العالم، وهذه الهجمات و الإختراقات تزيد بمعدل 60 % سنويا[3].

2- غياب الحدود الجغرافية وتدني مستوى المخاطر:

إن غياب الحدود المكانية في الشبكة المعلوماتية بالإضافة إلى عدم وضوح الهوية الرقمية للمستخدم المستوطن في بيئته المفتوحة بعد فرصة مناسبة للإرهابيين ، حيث يستطيع مخترق الحاسبة الإلكترونية أن يقدم نفسه بالهوية و الصفة التي يرغب بها أو يتخفى تحت شخصية وهمية ، ومن يشن هجومه الإلكتروني وهو مسترخ في منزله ومن دون مخاطر مباشرة ، بعيدا من أعين الناظرين[4]، وقد أصبح الإعتماد على شبكات الكمبيوتر مطلق خاصة في عالم المال و الأعمال مما جعل هذه

[1]- مدير البحث العلمي في وزارة الأوقاف، الإرهاب الإلكتروني، الثوابت و المتغيرات، مقال منشور على الموقع الإلكتروني بتاريخ 14-12-2014 http// www baathpaty.sy وقد تم للإطلاع على هذا الموقع بتاريخ 29-11-2016.

[2]- علي عدنان الفيل، الإجرام الإلكتروني، المرجع السابق، ص72.

[3]- مدير البحث العلمي في وزارة الأوفاق، الإرهاب الإلكتروني الثوابت و التغيرات، المرجع السابق.

[4]علي عدنان الفيل، الإجرام الإلكتروني، المرجع السابق، ص72.

الشبكات نظرا لطبيعتها المترابطة و انفتاحها على العالم هدفا مغريا للإرهاب الإلكتروني لذلك أصبح غياب الحدود الجغرافية في النظام المعلوماتي جعلها مؤذية جدا.

ومن الأمثلة على ذلك قيام بعض الإرهابيين بتحويل ملايين الدولارات من بعض الحاسبات الشخصية لكبار العملاء بعد اختراق نظام التحويلات المشفر الدولي بين البنوك ، وقيام بعض المنظمات الإرهابية الإلكترونية بالعمل على تدمير إقتصاد إحدى دول الشرق الأوسط بشراء سندات دولية لتلك الدولة من داخلها عبر البورصات العالمية و بيعها بالخارج بأسعار أقل من قيمتها مما أدى لانهيار عملتها و لتوفير تمويل الأعمال الإرهابية في الدول التي تم بيع السندات فيها[1].

2- سهولة الإستخدام و قلة التكلفة:

إن السمة العالمية لشبكات المعلوماتية تتمثل في كونها و سيلة سهلة الإستخدام نظرا لطبيعة الإنقياد و قلة الكلفة لا تستغرق وقتا ولا جهدا كبيرا مما هيأ للإرهابيين فرصة ثمينة للوصول إلى أهدافهم غير المشروعة ومن دون الحاجة إلى مصادر تمويل ضخمة فالقيام بشن هجوم إرهابي إلكتروني لا يتطلب أكثر من جهاز حاسب آلي متصل بالشبكة المعلوماتية و مزود بالبرامج اللازمة[2].

وعادة ما يلجؤون إلى الشبكة العنكبوتية لعدة أسباب منها:

*التنقيب عن المعلومات :

إن شبكة الإنترنت في حد ذاتها تعتبر مكتبة إلكترونية هائلة الحجم ، وتكتظ بالمعلومات الحساسة التي يسعى الإرهابيون للحصول عليها مثل أماكن المنشآت النووية ، والمطارات الدولية والمعلوماتية المختصة بذلك يكون 80% من مخزونهم المعلوماتي معتمد في الأساس على مواقع إلكترونية متاحة للكل دون خرق لأي قوانين أو بروتوكولات الشبكة.

*الإتصالات:

تساعد الإنترنت المنظمات الإرهابية في الإتصال ببعضها البعض و التنسيق فيما بينها ، وذلك نظرا

[1]- عبد الرحمان عثمان، الإرهاب الإكتروني، أنماطه و سبل مكافحته، مقال منشور بتاريخ 26-11-2016 www.egynews.net و قد تم الإطلاع على هذا الموقع بتاريخ 02-12-2016.
[2]- أمير فرج يوسف، الجريمة الإلكترونية و المعلوماتية، المرجع السابق، ص228.

لقلة تكاليف الإتصالات باستخدام الإنترنت مقارنة بالوسائل الأخرى ، كما أنها تمتاز بوفرة المعلومات التي يمكن تبادلها.

* التبعية و تجنيد إرهابيين جدد:

إن استخدام عناصر جديدة داخل المنظمات الإرهابية ، يحافظ على بقائها و استمرارها ، وهم يستغلون تعاطف الآخرين من مستخدمي الإنترنت مع قضاياهم ، و يجذبون هؤلاء الأشخاص بعبارات براقة وحماسية من خلال غرفة الدردشة في مقهى الإنترنت للثرثرة مع جميع أنواع البشر في مختلف أنحاء العالم.

* إعطاء التعليمات و التلقين الإلكتروني:

تمتلئ الإنترنت بكم هائل من المواقع التي تحتوي على كتيبات و إرشادات تشرح طرق صنع القنابل اليدوية و الإلكترونية و الأسلحة الفتاكة ، وعند استخدام محرك غوغل Googleعام 2005 للبحث عن مواقع تضم في موضوعاتها كلمة مثل إرهابي Terroristeو دليل –book herd فكانت نتائج البحث ما يقارب من ثمانية آلاف موقع.

* التخطيط و التنسيق:

تعتبر شبكة الإنترنت وسيلة للإتصال بالغة الأهمية بالنسبة للمنظمات ، حيث تتيح لهم حرية التنسيق الدقيق لشن هجمات إرهابية محددة ، كما أن أعضاء منظمة القاعدة البارزين إعتمدوا بشكل مكثف على الإنترنت في التخطيط لهجمات 11 سبتمبر و يستخدم الإرهابيون الرسائل الإلكترونية العادية email و غرف الثرثرة chat room لتدبير الهجمات و تنسيق الأعمال و المهام لكل عنصر إرهابي.

* الحصول على التمويل:

يستعين الإرهابيون ببيانات إحصائية سكانية منتقاة من المعلومات الشخصية التي يدخلها المستخدمون على الشبكة من خلال الإستفسارات و الإستطلاعات الموجودة على المواقع الإلكترونية ، في التعريف على الأشخاص ذوي القلوب الرحيمة ومن ثم يتم استدراجهم لدفع تبرعات مالية لأشخاص إعتباريين يمثلون واجهة لهؤلاء الإرهابيين ، ويتم ذلك بواسطة البريد الإلكتروني بطريقة ماكرة لا يشك فيها

المتبرع بأنه ساعد إحدى المنظمات الإرهابية ، وعادة ما تستخدم الإنترنت كحلبة مصارعة بين المنظمات الإرهابية ، وبين أعضاء المنظمة الواحدة ، وتكثر المناظرات و الخلافات بين منظمات مثل حماس و القاعدة و تملئ المواقع الإلكترونية بالسب و اللعان حتى بين أعضاء المنظمة الواحدة[1].

4- صعوبة إكتشاف و إثبات الجريمة الإرهابية:

في كثير من أنواع الجرائم المعلوماتية لا يقع العلم بوقوع الجريمة أصلا و خاصة في مجال جرائم الإختراق و السرقة ، مثل ما فعله أحد المخترقين الإلكترونيين من سرقة بيانات كوارت الإئتمان من بعض أكبر معاقل التسوق الإلكتروني الدولية، وخصم ملايين الدولارات من أصحاب تلك البطاقات، هذا ما ساعد الإرهابي على الحركة داخل المواقع التي يستهدفها قبل أن ينفذ جريمته ، كما أن صعوبة الإثبات تعتبر من أقوى الدوافع المساعدة على ارتكاب جرائم الإرهاب الإلكتروني لأنها تعطي المجرم أملا في الإفلات من العقوبة.

5- الفراغ التنظيمي و غياب الرقابة على الشبكات المعلوماتية:

إن الفراغ التنظيمي و القانوني لدى بعض المجتمعات حول الجرائم المعلوماتية و الإرهاب الإلكتروني يعتبر من الأسباب الرئيسية في انتشار الإرهاب الإلكتروني ، كما أنه حتى لو وجدت قوانين تجريمية متكاملة فإن المجرم يستطيع الإنطلاق من بلد لا توجد فيه قوانين صارمة ثم يقوم بشن هجومه الإرهابي.

كما أن عدم وجود جهة مركزية موحدة تتحكم فيما يعرض على الشبكة و تسيطر على مدخلاتها ومخرجاتها يعد سبب مهم في تفشي ظاهرة الإرهاب الإلكتروني ، حيث يمكن لأي شخص الدخول ووضع ما يريد على الشبكة ، وكل ما تملكه الجهات التي تحاول فرض الرقابة هو المنع من الوصول إلى بعض المواقع المحجوبة ، أو إغلاقها و تدميرها بعد نشر المجرم لما يريده فيها[2].

[1]- أنظر جابريال ويمان، الإرهاب على الشبكة العالمية، منشور على الموقع الآتي **www.assakina.com** تاريخ النشر 2006 و تم الإطلاع على الموقع بتاريخ 29-11-2016.

[2]- علي عدنان الفيل، المرجع السابق، ص73.

المطلب الثاني: صور جرائم الإرهاب الإلكتروني الماسة بالأمن الوطني.

يرتبط الإرهاب الإلكتروني بالمستوى المتقدم للغاية الذي باتت وسائل الإتصالات وتقنية المعلومات تلعبه في جميع مجالات الحياة و في العالم بأسره ، ومن خلال الأنظمة الإلكترونية و الشبكات المعلوماتية إتخذ الإرهاب الإلكتروني أبعادا جديدة و ازدادت خطورته على المجتمعات الدولية ، كون إعتداءاته مست جوانب جوهرية تخص الأفراد و المؤسسات و الدول في كافة نواحي الحياة الإقتصادية و الثقافية و الأمنية كما أن هذه الجرائم تركت في النفوس شعور بعدم الأمان ، وغياب الثقة الأمر الذي يؤدي إلى تهديد هذه التقنية لحياة الأفراد و أمنهم[1].

وفي القرن الحادي و العشرين أصبح الإرهاب الإلكتروني يستهدف التقنية التي تؤثر على القوة الإنتاجية و الثقة الصناعية ، واعتماد الدول على وسائل الإتصالات و شبكات المعلومات سيكون عاملا في فتح المجال أمام الإرهابيين لتحقيق أهدافهم و تدمير منتجات التقنية الحديثة التي تخدم الإنسانية و تسهل التواصل المعرفي و العلمي و الثقافي ، ومن هنا فإن المعلومات في هذا القرن عرضة لكافة المخاطر المحتملة من هذا النمط المتجدد من الإرهاب المعاصر ، فالإرهاب الإلكتروني يهدف إلى تدمير البنية التحتية المعلوماتية ، و تعريض المجتمعات العالمية إلى مخاطر غير محتملة و غير متوقعة[2] ، لذلك قسمنا هذا المطلب إلى فرعين تناولنا في الفرع الأول : القرصنة الإلكترونية و التجسس الإلكتروني ، وفي الفرع الثاني: تدمير المواقع و البيانات الإلكترونية.

الفرع الأول: القرصنة والتجسس الإلكتروني.

من المتعارف عليه أن العالم يعيش تغيرا نوعيا في جميع أوجه الحياة ، في الإقتصاد و السياسة و الثقافة و العلاقات الإجتماعية ، وذلك يجرى بفعل زخم الثورة التكنولوجية في مجال المعلومات و الإتصالات التي تتخذ طابعا كونيا حوّل العالم إلى قرية صغيرة ، وما إن دخلت المعلوماتية تاريخ الإنسانية الجديدة حتى بدأ التداخل بين وسائل الإعلام يأخذ منحى متسارعا ، وانتقل عصرنا إلى مرحلة الوسائط المتعددة التي لا يتوقف انتشارها إلا أنه في الوقت نفسه فتح جبهات للصراع لا تقل خطورة عن الصراعات العسكرية ، و الإقتصادية و الدبلوماسية بل إنها تتفوق عليها في معظم الأحيان

[1]- محمود أحمد عبابنة، جرائم الحاسوب و أبعادها الدولية، المرجع السابق، ص06

[2]- علي عدنان الفيل، الإجرام الإلكتروني، المرجع السابق، ص78.

لأنها تمس كل هذه المحاولات ، وعادة ما يلجأ الإرهاب الإلكتروني في أعماله الإرهابية لعدة أعمال منها القرصنة الإلكترونية ، و التجسس الإلكتروني.

أ/القرصنة الإلكترونية:

ـ تعريف القرصنة الإلكترونية:

القرصنة الإلكترونية أو المعلوماتية هي عملية إختراق لأجهزة الحاسوب تتم عبر شبكة الإنترنت غالبا، لأن أغلب حواسيب العالم مرتبطة عبر هذه الشبكة أو حتى عبر شبكات داخلية بما يرتبط فيها من جهاز حاسوب ، ويقوم بهذه العملية شخص أو عدة أشخاص متمكنين في برامج الحاسوب و طرق إدارتها ، أي أنهم مبرمجون ذو مستوى عالي يستطعون بواسطة برامج مساعدة إختراق حاسوب معين و التعرف على محتوياته ، ومن خلالها يتم اختراق باقي الأجهزة المرتبطة معها في نفس الشبكة ، كما يستطيع القرصان الإلكتروني الإستخدام و النسخ غير المشروع لنظام التشغيل أو لبرامج الحاسوب الآلي ، وقد تطورت وسائل القرصنة واتسعت و أصبح من الشائع جدا العثور على مواقع للإنترنت خاصة لترويج البرامج المقرصنة مجانا أو بمقابل مادي رمزي ، وأدت قرصنة البرامج إلى خسائر مادية باهضة جدا ، وعادة ما يفضل القراصنة العمل في جماعات عن العمل الفردي وغالبا ما يكون دافعهم لإرتكاب الجريمة إما الحصول على المال أو بغرض الشهرة ، أو إثبات تفوقهم العلمي وما يتمتعون به من ذكاء[1].

كما أن العدوان على هذه البرامج عن طريق قرصنتها يعد شكلا من أشكال العدوان على الملكية الفكرية و ينتج عنه خسائر مادية كبيرة مباشرة أو غير مباشرة ، بالإضافة إلى ذلك فإن قرصنة برامج الحاسب الآلي تسهم و بشكل كبير في انتشار الفيروسات مما يعني تدمير للنظم المعلوماتية أو إعتداء على الخصوصية ، ناهيك عما تسببه من ارتفاع ، أضف إلى ذلك الأموال الكثيرة التي تنفق من أجل حماية هذه البرامج من القرصنة.

وقد شهدت ظاهرة القرصنة الإلكترونية انتشارا واسع النطاق وتعاني منها الكثير من الشركات و البلدان المصنعة للبرمجيات ، و يترتب على ذلك الكثير من الأعباء الإقتصادية و الخسائر المالية في مجال صناعة البرمجيات خاصة مع الإستخدام الكبير لتقنية الشبكات ، حتى يشمل الإختراق الهجوم

[1]- خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص145.

على شبكات الحاسوب من قبل مخترقي الأنظمة الإلكترونية ومنتهكي القوانين ، كما يتبن التطور الحاصل في مجال سرية المعلومات التي تغطي الإنترنت بالإضافة على تقنيات أخرى كالإتصالات [1].

ـ أشهر الطرق التي تتم بها القرصنة الإلكترونية.

عادة ما تتم القرصنة الإلكترونية بإحدى الطرق الآتية:

1 ـ الإنزال و التحميل: و يتضمن إنزال برنامج ما أو جزء منه تم تحميله من موقع ما عبر شبكة الإنترنت بقصد الإستخدام الخاص ثم يستخدم بعد ذلك تجاريا سواء عن طريق شبكة الإنترنت أو عن طريق الطرق التقليدية في العالم المادي[2].

2 ـ العرض على شبكة الإنترنت: هذه الصورة تتمثل في قيام الجاني بنسج برنامج ما مبتكر و معد للتداول بطريقة تقليدية معتادة ، كأن يكون على CD أو FLOPPY DISK ، ومن ثم رفعها على شبكة الإنترنت UPLOAD ، سواء بهدف العرض المجاني لهذا البرنامج أو بهدف تسويقه و بيعه عبر بعض المواقع المنتشرة على شبكة الإنترنت و المتخصصة في بيع هذه البرامج المقرصنة.

3 ـ التسويق عبر شبكة الإنترنت: تتمثل هذه الصورة في قيام بعض المحنكين ذوي الخبرة العالية في كيفية فك شفرة البرامج المشفرة ضد عمليات القرصنة و الموجودة على شبكة الإنترنت ومن ثم بيعها عبر بعض المواقع على شبكة الإنترنت محققين بذلك مكاسب خيالية.

4 ـ النشر عبر شبكة الإنترنت: هذه الطريقة كسابقتها إلا أنها تختلف في الغرض، فالأولى كانت

بهدف الربح المادي ، أما هنا فإن الهدف هو إتاحة البرنامج للجمهور من خلال شبكة الإنترنت مما يعنى إلحاق الضرر بمنتجي هذه البرامج.

5 ـ الإعتداء على أمن حماية التقنية: غالبا ما يعمد مصممو البرامج لأجل تنظيم أو تقييد الإطلاع على برامجهم إلى استخدام تقنية خاصة عادة ما يطلق عليها أمن حماية التقنية[3].

[1]- محمد بن عبد اللهيان علي المنشاوي، جرائم الإنترنت في المجتمع السعودي، أكادمية نايف العربية للعلوم الأمنية،الرياض، سنة2003، ص79.

[2] ـ خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 445.

[3] ـ خالد ممدوح إبراهيم، المرجع نفسه، ص 446.

ومع ذلك يعمد بعض الأشخاص و هم غالبا ما يكونون من المحنكين ذوي المهارة الفائقة في مسائل التقنية بإزالة هذه التقنية أو تعطيلها أو تعييبها بحيث تصبح غير صالحة و غير فعالة و عندها تصبح هذه البرامج متاحة للجميع و بالتالي الإضرار بحقوق مؤلفيها و مصمميها.

ب/التجسس الإلكتروني:

لقد أصبحت العولمة و فاعلية الإتصال وسعة قنوات المعرفة أسلحة جديدة يمكن أن تحسم النزاع لصالح من يجيدها و يسيطر عليها ، وقد أتاحت هذه الآفاق الجديدة المنبثقة عن ثورة الإتصالات و المعلوماتية نوعا خطيرا وجديدا من أنواع التجسس ، وعلى الرغم من أن ظاهرة التجسس في الأصل هي ظاهرة غير أخلاقية وقد نهي الله عن هذا الفعل في قوله تعالى: " **يَا أَيُّهَا الَّذِينَ آمَنُوا اجْتَنِبُوا كَثِيرًا مِّنَ الظَّنِّ إِنَّ بَعْضَ الظَّنِّ إِثْمٌ ۖ وَلَا تَجَسَّسُوا وَلَا يَغْتَب بَّعْضُكُم بَعْضًا ۚ أَيُحِبُّ أَحَدُكُمْ أَن يَأْكُلَ لَحْمَ أَخِيهِ مَيْتًا فَكَرِهْتُمُوهُ ۚ وَاتَّقُوا اللَّهَ ۚ إِنَّ اللَّهَ تَوَّابٌ رَّحِيمٌ** " [1]. صدق الله العظيم.

فالمتجسس هدفه فضح عورات الناس و هتك أستارهم.

ولقد تطور التجسس في عصرنا هذا و أصبح من الممارسات اليومية التي تعتمد عليها الدول في حماية أمنها، وتطوير صناعتها، بل وفي التعامل مع أصدقائها، ونتيجة للتطور في عالم الإتصالات ظهر ما يعرف بالتجسس الإلكتروني الذي طغى بإمكانياته الهائلة ودقة نتائجه على التجسس[2] القديم الذي عرفه العالم ، واستخدمته الدول و الحكومات لمعرفة أسرار الخصم أو من تسعى للسيطرة عليه ، فتجمع المعلومات السرية و العلنية عن مصادر القوة ومواطن الضعف لديهم وتسعى الدولة المتجسسة كذلك لمعرفة درجة الوعي و الروح المعنوية في المجتمع ، والقوة العسكرية ، لذلك سنتطرق إلى تعريف التجسس الإلكتروني.

---

[1]-انظر الآية رقم 12 من سورة الحجرات.

[2]- أما عن تاريخ التجسس فهناك أحداث توثيقية تنطوي على التجسس على مر التاريخ ،وقد كانت بين الجيشين الصيني و الهندي و تم فيها استخدام عمليات التجسس و الإغتيالات و العملاء السربين، وكان المصريون القدماء قد نظموا عمليات التجسس تنظيما دقيقا و العبرانين كدلك استخدموا الجواسيس.وكان نظام الجواسيس أيضا سائدفي الامراطورية اليونانية و الرومانية خلال القرن 13و 14،وقد اعتتمدوا المغول اعتمادا كبيرا على التجسس في فتوحاتهم في آسيا و أوربا، وقد كانت اليابان الاقطاعية غالبا ما تستخدم النينجا لجمع المعلومات الإستخبارية ،ولعب الجواسيس دورا ها في إنجلترا ، وأنشئت العديد من رسائل التجسس الحديثة منذ الحين .
وقد شهدت الحرب الباردة المشاركة المكثفة لأنشطة التجسس بين الولايات المتحدة الأمريكية و حلفاء في الآونة الأخيرة و استهدفت وكالات التجسس و تجارة و تجارة المخدرات غير المشروعة منذ عام 2008.ولمزيد من التفصيل أنظر تجسس ،ويكيبيديا (الموسوعة الحرة) على الموقع التالي:.http//wikip édia.arg/wiki.

التجسس: هو محاولة الإستيلاء على معلومات سرية بقصد إبلاغها إلى جهة معادية، وقد نصت المادة التاسعة عشرة من إتفاقية لاهي لعام 1907 على الآتي يعد جاسوسا ذلك الذي يعمل سرا أو وراء ستار زائف ، للحصول على معلومات في منطقة العمليات بنية تبليغها للفريق الآخر.

التجسس الإلكتروني أو ما يعرف بالتجسس المعلوماتي: هو عبارة عن عدة طرق لاختراق المواقع الإلكترونية ومن ثم سرقة بعض المعلومات و التي قد تكون فائقة الأهمية و الخطورة للطرف المتلقي و المسروقة منه.

و التجسس الإلكتروني هو شكل من الإرهاب يستخدام التكنولوجيا بشكل سلبي من أجل إحداث آثار مدمرة و أضرار بالغة و كبيرة لمحطات التحكم و أجهزة الكمبوتر و شبكات الإتصال بدوافع مختلفة ، كما عرف التجسس الإلكتروني بأنه العدوان أو التخويف أو التهديد ماديا أو معنويا بإستخدام الوسائل الإلكترونية الصادرة من الدول أو الجماعات أو الأفراد على الإنسان بغير حق ، ويربط بعض الباحثين بين التجسس الإلكتروني و الإرهاب الإلكتروني ، فهما نوع من العدوان أو التخويف أو التهديد المادي أو المعنوي الصادر من الدول أو الجماعات أو الأفراد على الإنسان ، في دينه أو نفسه أو عرضه أو عقله أو ماله بغير حق ، باستخدام الموارد المعلوماتية و الوسائل الإلكترونية بشتى صنوف العدوان و صور الفساد.

وقد انتشرت في الألفية الجديدة بانتشار طرق الإختراق ، و أحيانا قد يكون الإختراق من أشخاص عابثين ليس إلا و أحيانا بغرض سرقة معلومات مهمة مثل ما حدث لوزارة الدفاع الأمريكية البنتاغون ، كما تم اختراق موقع وزارة الدفاع الفرنسية بغرض سرقة معلومات عن الإستطلاعات و المناورات و النظام الصاروخي الفرنسي ، و الإختراق ليس محصورا على المؤسسات العسكرية فقد تتعرض له

المؤسسات النقدية وخصوصا البنوك المركزية و المؤسسات العملاقة[1].

كما أن مصادر محاولات إختراق الأنظمة و الشبكات الإلكترونية لا تقتصر على الجماعات و الأفراد أو منظمات عالم الإنترنت السرية مثل منظمات الهاكرز ، إنما دخلت ميادين جديدة وخطيرة ، هي التجسس الدولي الذي ينقل أسرار دول بأكملها إلى دول أخرى معادية ، و يهدف أيضا إل زعزعة

[1]- أنظر مقال منشور بجريدة الوطن بعنوان قضايا، الإرهاب الإسرائيلي الإلكتروني ، العرب و التجسس الإسرائيلي الإلكتروني على الموقع الآتي: http//alwatan.com/details/57008 وقد تم الإطلاع على هذا الموقع بتاريخ 04-12-2016.

الأمن ونشر الخوف و الرعب و الإخلال بنظام دول العالم ، و تهديد و إبتزاز الأشخاص و السلطات العامة و المنظمات الدولية ، والسطو و جمع الأموال إضافة إلى جذب الإنتباه و الدعاية و الإعلام ، ومن خلال ما تقدم يتبن لنا أن هناك أنواع من التجسس الإلكتروني منها:

***التجسس عن طريق الإنترنت على الأفراد:**

أبسط أنواع التجسس الإلكتروني معروف ومنتشر بين الأفراد مستخدمي الكمبيوتر الشخصي بشكل عام ، هذا النوع من التجسس يستخدم فيه المخترق أومن يكون برنامج خارجية مبنية على أساس العميل و الخادم أو ما يعرف بـ client وSemer ، ويشترط في هذه العملية أن يكون برنامج الخادم يعمل في نظام الهدف ليقوم بعد ذلك المخترق بالإتصال من الخارج ببرنامج العميل لتبدأ عملية التجسس ، هذا النوع من برامج التجسس يعمل على الكمبيوتر الشخصي ، وقد ظهرت برامج كثيرة لأنظمة وندووز ولينكس من أشهرها Back orifice. Subi 7 net bus والجدير بالذكر أنه مع انتشار الأجهزة الكفية و الموبايلات في الآونة الأخيرة التي تستخدم أنظمة تشغيل متطورة مثل النظام Symbian الذي يسمح بتطوير برامج خارجية وتشغيلها على الجوال ، فقد ظهرت لهذه الأنظمة برامج تجسس مشابهة للفكرة السابقة و أمثلة على ذلك برنامج FlexiSpy الذي يثبت على الجوال للتجسس على المكالمات و الرسائل القصرة SMS و سجل المكالمات وغيرها[1]، ومن بين أمثلة التجسس على الأفراد إعتراض مكالمة هاتفية جرت بين الزعيم الراحل جمال عبد الناصر والملك الأردني الراحل الحسين بن طلال ، وذلك أول أيام حزيران 1967 وكذلك اعتراض مكالمة هاتفية بين ياسر عرفات و مسلحين تابعين لمنظمة جبهة التحرير الفلسطينية.

***التجسس من خلال الشبكات السلكية و اللاسلكية:**

ظهرت أنواع للتجسس الإلكتروني في الشركات التي تستخدم الشبكات بكل أنواعها الصغيرة و الكبيرة السلكية و اللاسلكية ، ومن أشهر أنواع التجسس بداخل الشبكات ما يعرف بـSniffer واصطياد حزم البيانات المرسلة ومن أشهر هذه البرامج لأنظمة وندووز و لينكس هو برنامج Ethereal للشبكات الداخلية و برامج tcpdump و winetunq و غيرها ، هذه البرامج تستطيع اصطياد البيانات المرسلة

[1]- حسن بن أحمد الشهري، الأنظمة الإلكترونية الرقمية المطورة لحفظ حماية سرية المعلومات من التجسس، المجلة العربية للدراسات الأمنية و التدريب، المجلد 28، العدد 56، ص12.

داخل الشبكة و تعمل على مراقبة أغلب البوتوكولات و لذاك فإن أي مستخدم بداخل شبكة محلية يستطيع الوصول و التجسس على بقية المستخدمين.

كما يستطيع أي شخص التجسس على مستخدمي الشبكات الداخلية بسهولة فائقة باستخدام البرامج السابقة و لكن ظهرت بروتوكولات تقوم بتشفير بسيط للبيانات قبل إرسالها في شبكة داخلية و لذلك قد لا تفيد بعض البرامج وهذا الموضوع أدى لظهور برنامج قد يكون خرافي هو Caïn Is Abel poussoir recovery يعتقد أنه يتجسس على كل أنواع البروتوكولات و يفك كلمات المرور و أكثر و الغريب أنه توجد نسخة من البرامج للأجهزة الكفية ، وتوجد برامج Sniffer تتجسس على برامج المحادثة و الشات مثل الماسنجر.

ومن أمثلة التجسس السلكي و اللاسلكي كثيرة ومنها ، ما أفادت به تقارير إخبارية عن تورط عملاق الإنترنت غوغل فيما أسمتها أكبر فضيحة دولية في تاريخ الإنترنت و ذلك بظهور تورطه في التجسس على المراسلات الإلكترونية التي تتم بتقنية واي فاي اللاسلكية عبر الإنترنت التي يستخدمها ملايين الناس في مدن العالم ، واعترفت شركة غوغل بأن الأجهزة المنصوبة على سيارتها إلتقطت مقاطع من المراسلات لدى مرورها في شوارع المدن إلا أنها أشارت إلى أن تلك لا تشكل أي معلومات من المواقع الإلكترونية المحصنة الأمينة مثل المصارف، وجاء الإعتراف بعد أن فتحت الحكومة الألمانية تحقيقا للتعرف على الأسباب التي حدثت ببوابة غوغل لجمع بيانات مرسلة عبر تقنية واي فاي للإتصالات اللاسلكية.

وقد أثار هذا الإعتراف مخاوف مستخدمي الإنترنت في خصوصياتهم ، وأصبحت هذه المخاوف أكبر بكثير من مخاوف تسلل الإرهاب الإلكتروني نظرا لما تملكه غوغل من إمكانيات هائلة في جمع البيانات من النصوص والمقاطع الصوتية و الصور و الفيديو، إضافة إلى رصدها الدائم لأذواقهم و نزعاتهم الشخصية من خلال استخدامهم لمحرك البحث لديهم.

وقد أخد التجسس من خلال هذه الشبكات أبعادا دولية خاصة مع سرعة تطور الإنترنت و انتشارها فقد ظهرت الكثير من الثغرات الأمنية التي تشكل تهديدا لا يقتصر على مستخدمها من الأفراد و إنما على إقتصاد الدول و أمنها و التي تعتمد عليها ، كما تفعل إسرائيل حيث تتجسس على الفلسطينيين أفراد و سياسيين وحكومة من باب إستباق الأحداث وتحرص أجهزة الأمن الإسرائيلية على عدم إستثناء أية

حكومة أو مسؤول مهم أو ترى أنه من المناسب لها وضع عمله تحت رقابتها ، وقد أكدت وسائل الإعلام الإسرائيلية عرض شارون أمام الرئاسة الأمريكية لمحادثات هاتفية لعرفات وهو يؤيد الأعمال المسلحة في انتفاضة الأقصى، بهدف إيجاد المبررات لإسرائيل فيما تقوم به من عنف موجه للشعب الفلسطيني أو أية جهة عربية تؤيده ، كما تحرص أجهزة الأمن الإسرائيلية على معرفة اتجاهات الرأي العام الفلسطيني ورأي المجتمع إزاء الأحداث الجارية، فتقوم بالتجسس على هواتف الكثير منهم خاصة العاملين في المجال الإعلامي و الإنساني ومؤسسات المجتمع المدني[1].

الفرع الثاني: تدمير المواقع و البيانات الإلكترونية

يقوم الإرهاب الإلكتروني بشن هجمات إلكترونية من خلال الشبكات المعلوماتية ، بقصد تدمير المواقع و البيانات الإلكترونية والنظم المعلوماتية ، وإلحاق الضرر بالبنية المعلوماتية التحتية وتدميرها ، و يقصد بتدمير المواقع و البيانات الإلكترونية إتلاف أو محو تعليمات البرامج أو البيانات ذاتها ، و يطلق عليها مصطلح تدمير نظم المعلومات و عادة لا يستهدف مرتكب هذا الإعتداء فائدة مالية لنفسه ، بل لمجرد إعاقة نظام المعلومات عن الأداء بوظائفه و إحداث ضرر[2]، كما يقصد بالتدمير الدخول غير المشروع على نقطة إرتباط أساسية أو فرعية متصلة بالشبكة المعلوماتية من خلال نظام آلي أو مجموعة نظم مترابطة شبكيا ، بهدف تخريب نقطة الإتصال أو النظام.

فالإرهاب الإلكتروني عادة ما يستهدف مخازن للمعلومات الحساسة كالملفات المغلقة بالحالة الجنائية و المعلومات العسكرية و خطط التسويق وغيرها ، ولم يتوقف نشاط الإختراق على الملفات و الأنظمة غير الحكومية بل يمتد إلى الأنظمة الخاصة التي تتضمن بيانات ذات قيمة ، و يتضمن بعض طوائف هذا النمط كهدف أنشطة السرقة و الإعتداء على الملكية الفكرية ، كسرقة الأسرار التجارية، وإعادة إنتاج ونسخ المصنفات المحمية و تحديدا برامج الكمبيوتر[3].

ومما لاشك فيه أن الحاسب الآلي ينطوي على برامج بمختلف أنواعها إلى جانب ذلك ينطوي على معلومات ، سواء تم جمعها وحفظها ، أو بيانات تمت معالجتها ، أو معلومات تم تسجيلها كمجموعة

---

[1]- حسن بن أحمد الشهري، الأنظمة الإلكترونية الرقمية، المرجع السابق، ص14.

[2]- محمود أحمد عبابنة ، جرائم الحاسوب و أبعادها الدولة ، المرجع السابق ،ص100.

الموقع: هو موقع ينشأ على شبكة الأنترنت تستضيفه إحدى الشركات أو مزود خدمة ،أو ما شابهها ،مقابل أجر مائي سنوي ، وقد يكون مجانا ،ويسمح الموقع لمستخدم الأنترنت بالتجول في صفحاته المتعددة و الإطلاع على محتوياته إما مجانا أو بمقابل مادي ،كما قد يسمح بشراء ما يعرض في الموقع من مواد تجارية ، وقد يكون باالموقع قائمة بريدية يشترك بها متصفح الأنترنت.

[3]- خالد ممدوح ابراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الطبعة الأولى، الإسكندرية، 2009،ص113.

البيانات في الحالة الشخصية لأحد الأفراد ، الأمر الذي يترتب عليه ألا يقتصر أمر الحماية الجنائية على برامج الحاسب الآلي فقط ، إنما يجب أن تقتضي هذه الحماية حماية المعلومات المودعة فيه ، و التي قد يتضمن ذيوعها و انتشارها إلى إصابة المصالح التي تتعلق بها تلك المعلومات بضرر ، أو تهديدها بخطر.

ووجه وجوب أن تكون المعلومات المخزنة في الحاسب الآلي أيا كان مصدرها محلا للحماية الجنائية من كل اعتداء ينشأ من خلال الإعتداء على الحاسب الآلي ، خاصة أن المعلومات أصبحت تشكل جزء هاما من مكونات الحاسب الآلي حيث باشرت الكثير من المؤسسات و المصالح في مختلف البلدان الإعتماد على الحاسب الآلي في تقديم خدماتها ، حيث أدخلت أغلب الهيئات الحكومية و غير الحكومية الحاسب الآلي في نظام عملها ، بالإضافة إلى الإعتماد على الحاسب الآلي في جوانب مهمة تتعلق بالحياة الخاصة للأفراد و تتصل بها إلى حد كبير ، هذا إلى جانب أن من الأمور التي يتعرض لها الفرد و تقتضي الظروف التي يمر بها أن تحفظ أسراره في مكان معين كتسجيل بعض البيانات عنه عند فتح حساب له في البنك ، أو تدوين تلك المعلومات عند تسجيله ببطاقة هاتفه المحمول[1]، وعادة تستهدف الهجمات الإرهابية في عصر المعلومات هدفين أساسين هما العسكري و الإقتصادي:

- الهدف العسكري:

إن الظروف التي مر بها العالم العربي منذ ثورات الربيع العربي وقبلها غزو العراق وما أعقب ذلك من إستخدام التنظيمات الإرهابية المتطرفة مثل داعش للفضاء الإلكتروني في تجنيد عناصر من مواطني دول غربية ، وجهت الإنتباه إلى أهمية المجال الإلكتروني في حركة العلاقات الدولية و الأمن و السلم العالميين خاصة مع دوره في الحشد و التعبئة و التجنيد و استخدامه في نشر الأفكار المتطرفة ، فلقد نجحت منظمات و جماعات إرهابية دولية وعلى رأسها داعش و القاعدة في التخطيط و التنسيق لعمليات إرهابية كبرى في أوروبا ، وخاصة في فرنسا ، بلجيكا من خلال شبكات معلومات و تواصل إجتماعي مغلقة لا يمكن رصدها ، بل و تمحى بعد قراءتها مباشرة من خلال أجهزة ألعاب الفيديو المتصلة عبر الإنترنت ، وأدى التجسس الإرهابي لمقتل نحو 200 شخص في نوفمبر 2015 ، وقد

[1]- محمد حماد مرهج الهيتي ، جرائم الحاسوب دراسة تحليلة، المرجع السابق، ص104.

فشلت أجهزة المخابرات الأوروبية في رصد العمليات قبل وقوعها لكنها إكتشفت هويات منفذيها من خلال هواتفهم المحمولة و مكالمتهم المتبادلة مع أفراد المنظمة[1].

– الهدف الإقتصادي:

أصبحت كل الدول المتقدمة و كثير من دول العالم تعتمد على شبكات المعلومات لإدارة نظم الطاقة الكهربائية ، لكن الإرهاب الإلكتروني إخترق هذه المواقع مما أدى إلى نتائج خطيرة وحقيقية ، وخصوصا في ظل اعتماد الإنسان المعاصر على الطاقة الكهربائية ، وكانت عدة مدن كبرى في العالم قد تعرضت لعمليات إنقطاع كهرباء كاملة نتيجة إختراق هذه المواقع الغير مبرر وأدى ذلك لخسائر مادية كبيرة و خسائر في الأرواح نتيجة لتعطيل المستشفيات و مصاعد المباني و مرافق المياه و الصرف الصحي ، ومن الإحصائيات البشعة التي يمكن لها أن تدل على فعالية مثل هذا النوع من الإختراقات تلك المتعلقة بالهجمات على العراق خلال حرب الخليج الثانية ، حيث تشير مصادر كلية الحرب الأمريكية إلى أن ضرب مولدات الطاقة الكهربائية العراقية أدى بشكل غير مباشر إلى موت ما بين 70 إلى 90 ألف مواطن عراقي نتيجة مباشرة لعدم توفر الطاقة الكهربائية ، لذلك فإن شبكات المعلوماتية المرتبطة بشكل مباشر أو غير مباشر بشكل الطاقة الكهربائية تعتبر من الأهداف الأولى التي يستهدفها الإرهاب الإلكتروني[2].

وليس هناك وسيلة يمكن تطبيقها وتحول تماما دون تدمير المواقع أو اختراقها بشكل دائم ، فالمتغيرات التقنية و إلمام المخترق بالتغيرات في التطبيقات و التي ثبت معظمها على أساس التصميم المفتوح لمعظم الأجزاء سواء كان ذلك في مكونات نقطة الإتصال أو في النظم أو في الشبكة أو في البرمجة ، جعلت الحيلولة دون الإختراقات أمر صعب جدا ، بالإضافة إلى أن هناك منظمات إرهابية يدخل من ضمن عملها و مسؤولياتها الرغبة في الإختراق و تدمير المواقع ومن المعلوم أن لدى المؤسسات من الإمكانات و القدرات ما ليس لدى الأفراد ، ويستطيع الإرهاب الإلكتروني الوصول إلى المعلومات السرية و الشخصية ، و اختراق الخصوصية و سرية المعلومات بسهولة ، وذلك راجع إلى أن التطور المذهل في عالم الحاسب الآلي و الشبكات المعلوماتية يصحبه تقدم أعظم في الجرائم المعلوماتية و

[1]- عبد الرحمان عثمان، الموقع السابق.
[2]- عبد الرحمان عثمان، الموقع نفسه.

سبل ارتكابها ، ولاسيما وأن مرتكبيها ليسوا مستخدمين عاديين بل قد يكونون خبراء في مجال الحاسبة الإلكترونية.

إن عملية الإختراق الإلكتروني تتم عن طريق تسريب البيانات المعلوماتية الرئيسية و الرموز الخاصة ببرامج شبكة الإنترنت ، وهي عملية تتم من أي مكان في العالم دون الحاجة إلى وجود شخص المخترق في الدولة التي يتم اختراق مودعها ، ولاتزال نسبة كبيرة من الإختراقات لم تكتشف بعد بسبب التعقيد الذي يتصف به نظام تشغيل الحاسبة الإلكترونية و الشبكات المعلوماتية[1]، حيث يسعى الإرهاب الإلكتروني إلى تدمير المواقع و البيانات الإلكترونية[2] لتحقيق عدة أهداف وأهمها أن يشيع الفوضى فهناك مثلا شبكات المعلوماتية الطبية ، والتي يمكن لمهاجمتها ، وإختراقها أن يؤدي إلى خسائر في أرواح المرضى ، وهناك حالات في العالم الغربي حيث قام الإرهاب الإلكتروني بالنفاذ إلى سجلات المستشفيات و التلاعب بسجلات المرضى بشكل أدى إلى خنق هؤلاء بأدوية وعلاجات كانت مميتة بالنسبة لهم ، وحتى لو افترضنا أن الشبكات المعلوماتية الخاصة بالمؤسسات الطبية منيعة ، فإن رسالة واحدة تنتشر مثلا بالبريد الإلكتروني أو عبر رسائل التواصل الإجتماعي ، مفادها أن هناك دماء ملوثة في المستشفيات وما إلى ذلك يمكن لها أن تحدث آثار مدمرة على الصعيد الإجتماعي وهناك أيضا تخريب ومهاجمة نظام التحكم الوطني في الطيران و القطارات لإحداث تصادم بين الطائرات ، ومهاجمة قطارات السكك الحديدية و تعديل كل من ضغط الغاز عن بعد في أنابيب الغاز لتفجيرها ، ونظام السلامة في المصانع الكيماوية لإحداث أضرار.

ومن أبرز ماقامت به أجهزة المخابرات الأمريكية و الإسرائيلية في هذا الصدد هو نشر فيروسات تهدف لتدمير أجهزة الطيران المركزي لبعض المنشآت النووية الإيرانية مما أدى لتغيير برمجها النووي بعض الوقت ، ومن أخطر قضايا الإرهاب الإلكتروني في القرن الحالي ، ما يعرف بإعصار ويكيليكس الذي حدث عام 2010 ، حيث تم استغلال شبكة الإنترنت العالمية في تسريب وثائق تحوي معلومات سرية للغاية متداولة بين الإدارة الأمريكية و قنصلياتها الخارجية في دول العالم[3]، ومن المتصور شن هجوم إلكتروني على البنية التحتية للشبكة المعلوماتية بقصد تدميرها و توقيفها عن

[1]- علي عدنان الفيل، الإجرام الإلكتروني، المرجع السابق ،ص86.

[2]- بالنسبة لتدمير المواقع و البيانات قد يكون بمحتوي و إزالة كل أو جزء من المعطيات الموجودة داخل النظام و يعتبر المحو جريمة إتلاف طالما وقع إتلاف الشيئ بأنه وسيلة سواء بالإدخال أو التعديل أو المحو بشكل جريمة تزوير و اعتبر المحوللبرامج أو المعطيات جريمة إتلاف .و لمزيد من التفصيل أنظر المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات المنعقد في البرازيل بتاريخ تشريت الأول 1994بشأن جرائم الكمبيوتر.

[3]-عبد الرحمان عثمان، الإرهاب الإلكتروني، أنماط و سبل مكافحته، الموقع السابق.

العمل ، مما يحدث آثارا مادية و اقتصادية ، وسياسية و ثقافية خطيرة توقف الشبكة المعلوماتية والذي يعني توقف الحكومات الإلكترونية عن عملها ، وإلحاق الضرر بأعمال البنوك و أسواق المال العالمية.

و من الوسائل المستخدمة حاليا لتدمير المواقع ضخ مئات الآلاف من الرسائل الإلكترونية من جهاز الحاسبة الإلكترونية الخاصة بالمدمر إلى الموقع المستهدف للتأثير على السعة التخريبية للموقع ، فتشكل هذه الكمية الهائلة من الرسائل الإلكترونية ضغطا يؤدي في النهاية إلى تفجير الموقع العامل على الشبكة ، وتشتيت البيانات و المعلومات المخزنة في الموقع فتنتقل إلى جهاز المعتدي أو تمكنه من حرية التجول في الموقع المستهدف بسهولة و يسر و الحصول على كل ما يحتاجه من أرقام و معلومات و بيانات خاصة بالموقع المعتدى عليه[1].

وهناك أسباب لوقوع عملية تدمير المواقع ومن بينها ما يلي:

*ضعف الكلمات السرية فبعض مستخدمي الإنترنت يجد أن بعض الكلمات أو الأرقام أسهل في الحفظ فيستخدمها ، مما يسهل عملية كسر و تخمين الكلمات السرية في الإختراق.

*عدم وضع برامج حماية كافية لحماية الموقع من الإختراق أو التدمير وعدم التحديث المستمر لهذه البرامج و التي تعمل على الشبه عند وجود حالة إختراق للموقع.

*استضافة الموقع في شركات غير قادرة على تأمين الدعم الفني المستمر ، أو تستخدم برامج و أنظمة غير موثوقة أمنيا و لا يتم تحديثها باستمرار.

*عدم القيام بالتحديث المستمر لنظام التشغيل و الذي يتم في كثير من الحيان باكتشاف المزيد من الثغرات الفنية فيه ، ويستدعي ضرورة القيام بسد تلك الثغرات من خلال ملفات برمجية تصدرها الشركات المنتجة لها لمنع المخربين من الإستفادة منها.

*عدم القيام بالنسخ الإحتياطي للموقع للملفات و المجلدات الموجودة فيه ، وعدم القيام بنسخ قاعدة البيانات الموجودة بالموقع مما يعرض جميع المعلومات في الموقع للضياع وعدم إمكانية استرجاعها ، ولذلك تبرز أهمية وجود نسخة إحتياطية للموقع ومحتوياته خاصة مع تفاقم مشكلة الإختراقات في

[1]-عبد الله بن عبد العزيز بن فهد العجلان، الإرهاب الإلكتروني في عصر المعلومات ،بحث مقدم إلى المؤتمر الدولي الأول حول :حماية أمن المعلومات و الخصوصية في قانون الأنترنت ، و المنعقد بالقاهرة في المدة من 2-4يونيو 2008.

الآونة الأخيرة ، ويعد عام 2002 من أكثر الأعوام اختراقا فقد تضاعفت حالات الإختراق و التدمير بسبب إكتشاف المزيد من الثغرات الأمنية في أنظمة التشغيل و البرامج المستخدمة في مزودات الإنترنت و انتشار كثير من الفيروسات[1]، وتتصف الفيروسات بعد تكاثرها داخل الجهاز بقدرتها الفائقة على الإنتشار في أجهزة الحاسب المتصلة و الشبكات العامة و الخاصة المتعلقة بالإتصال بين الحواسيب ، الأمر الذي يؤدي إلى تدمير البرامج و المعلومات المخزنة داخل الجهاز و تعطيل الحاسب عن القيام بوظائفه الطبيعية و تضليل مستخدميه وضياع بياناته و تحويله إلى آلة صماء لا فائدة منها.

لذلك تعتبر الفيروسات من أخطر المشكلات التي تهدد أمن المعلومات ، لذلك يعد نشر فيروس جريمة من جرائم الحاسوب بتعريض من قام بها للعقوبة إذا تم اكتشافه.

و الفيروسات عبارة عن برامج حاسب مثل أي برنامج تطبيقي يتم تصميمه بواسطة أحد المبرمجين لتحقيق هدف معين ، يكون لإلحاق الضرر بنظام الحاسب ، ولذلك تتم برمجته بحيث يكتسب القدرة على ربط نفسه بالبرامج الأخرى وإعادة إنشاء نفسه للإنتشار بين برامج الحاسب المختلفة و مواقع الذاكرة بشكل يسمح له بتحقيق الأهداف التدميرية و الفيروسات ذات هدف تخريبي تنتشر ذاتيا و بسهولة من جانب لآخر و تستطيع أن تصيب و تفسد الأجهزة و البرامج و الشبكات المتصلة معها بشكل جزئي أو كلي ، وعادة ما يلجأ الإرهاب الإلكتروني إلى انتحال شخصية الفرد أو شخصية الموقع و ذلك بانتحال صفة من له الحق في الدخول إلى نظام معلوماتي معيين وذلك باستغلال بياناته كعنوان أو تاريخ ميلاده أو رقم ضمانه الإجتماعي إستغلالا سيئا من أجل الحصول على بطاقات الإئتمان ورخص القيادة أو بهدف تشويه سمعة صاحب الموقع، أما فيما يخص إنتحال شخصية الموقع فهي تعني أنه بإمكان الأشخاص الدخول على الموقع بغرض حجبه أو تغييره، ووضع الموقع الخاص به، و هذا ما يحدث غالبا في المواقع السياسية أو الدينية، ومن ذلك ما نجده في المواقع الفلسطينية و المواقع الإسرائيلية فكثير ما يدخل الفلسطينيون على المواقع الإسرائيلية ليقوموا بإلغاء الصفحة الرئيسية و يضعون بدلا منها العلم الفلسطيني و العكس صحيح.

وعموما هناك أنواع مختلفة من الفيروسات يستعملها الإرهاب الإلكتروني لتدمير أغلب المواقع و البيانات إن لم نقل كلها ، وتستخدم كلمة فيروس في مجال المعلوماتية للدلالة على كل البرامج الخبيثة

[1]- علي عدنان الفيل، الإجرام الإلكتروني، المرجع السابق، ص91.

التي تسبب إتلاف لأنظمة المعالجة الآلية للمعلومات و يوجد منها أنواع كثيرة ، وهي تتسبب في إتلاف المكونات المنطقية للحاسب الآلي أو تعطيل أجهزة الكمبيوتر أو الشبكات عن تأدية عملها[1].

وفيروس الحاسب الآلي عبارة عن معلومة خاطئة أو أمر مضلل يدخله الجاني إلى البرنامج من شأنها أو من شأنه كف منفعة البرامج فيما أعد له ومن خلال تكرار كتابة المعلومات ذاتها إلى آلية إدارة القرص مما يؤدي إلى إيقاف الحاسب الآلي عند حد معين،و يسبب أعباء إضافية على القرص و يزيد من حرارته نتيجة للتشغيل المستمر[2].

أو هو عبارة عن برنامج يتم زرعه على الأقراص و الأسطوانات الخاصة بالحاسب ، ويظل خاملا لفترة طويلة محددة ثم ينشط فجأة في توقيت معين ليدمر البرامج و البيانات المسجلة و يمتد أثره التخريبي ليشمل الإتلاف و الحذف و التعديل[3].

– **أنواع الفيروسات** :ومن بين هذه الفيروسات.

*** حصان طروادة :**

تختفي أغلب هذه الفيروسات ضمن برامج يبدو مظهرها بريئا ، وعندما يشغل المستخدم أحد هذه البرامج ينشط الجزء الماكر و يقوم بممارسة عمله في السيطرة على الجهاز، وإتلافه من خلال جمع معلومات عن إسم المستخدم وكلمة السر، وإرسالها لصاحب الفيروس أثناء إتصال المستخدم بالشبكة كما يسمح بتصفح الجهاز و التحكم بملفاته تحكما كاملا[4].

* **فيروس يوسف على إيه:** لقد رصد مركز عالمي لتحليل الفيروسات ورسائل البريد غير المرغوب فيها: "فيروسا إسلاميا" إنتشر في بعض أجهزة الحاسوب عبر الإنترنيت يمنع المتصفحين من الدخول إلى المواقع الإباحية.

وقال "جرهان كليولي" الخبير التكنولوجي بشركة "سوفوس" البريطانية لمكافحة الفيروسات: إن الشركة رصدت في إيران فيروسا إلكترونيا من نوع (حصان طروادة) يطلق عليه اسم "يوسف على إيه" حيث ينشر على المواقع الإباحية آيات قرآنية بالعربية وترجمة لمعانيها بالإنجليزية والفارسية، ويراقب

[1] -DAVID DAVIES.Computer.Virus-the Major Computer Abuse Threat of 1988.p02.

[2] -ماجد عمار ،المسؤولية القانونية الناشئة عن استخدام فيروس برامج الكمبيوتر و وسائل حمايتها ، دار النهضة العربية ،1989،ص82.

[3] -هدى حامد قشقوش،جرائم الحاسوب الألي في التشريع المقارن، المرجع السابق ،ص112

[4] - منصور بن سعيد القحطاني ، مهددات الأمن المعلومات و سبل مواجهتها ، جامعة نايف العربية للعلوم الأمنية ،2008،ص39

حركة المتصفحين والموقع الذي يطلبونه ويدقق النافذة النشيطة المفتوحة وأنه في حالة عثوره على كلمة لا تعجبه مثل "جنس" أو أي كلمة بذيئة فإنه يعمل على تصغير النافذة حتى لا يتمكن المتصفح من رؤية موادها ثم يعرض على الصفحة آيات قرآنية.

وإذا استمر المتصفح في البقاء على صفحة الموقع الإباحي يلجأ "يوسف علي إيه" إلى عرض زر على الصفحة يقول للخروج إضغط هنا، وما أن تتحرك فأرة الكمبيوتر نحو هذا الزر حتى يدخل المتصفح مع مؤشر الفأرة في قفص لا يمكن الخروج منه حيث تظهر صفحة كتب عليها بالإنجليزية "آه، لا إنني في قفص" وعليها ثلاثة أزرار كلها تعني إنهاء العمل على الموقع الإباحي.

والفيروس الإسلامي الجديد ينشر نفسه عبر الرسائل الإلكترونية لكنه لا يستنسخ نفسه مثل الفيروسات، وهو يصيب نظام التشغيل Windows وقد رصدته شركة سوفوس يوم 2005/9/4.*

ومن خلال ما سبق، نستنتج أن الفيروسات تستخدم في أحد غرضين: حمائي أو تخريبي.

الغرض الحمائي: ويكون ذلك لحماية البيانات والبرامج من خطر النسخ غير المشروع (المرخص به) إذ ينشط الفيروس بمجرد النسخ ويدمر نظام الحاسوب الذي يعمل عليه.

الغرض التخريبي: ويكون ذلك بهدف الدعاية أو الإبتزاز حيث يرمي واضع الفيروس للتخريب بهدف التخريب ذاته أو بهدف الحصول على منافع شخصية.

***الديدان:**

عبارة عن فيروسات تتميز بقدرة كبيرة على نسخ نفسها من وإلى الأقراص المرنة أو عبر الشبكة و يعتمد بعضها على بعض في إنجاز مهامها، وهي تنقسم إلى نوعين :النوع الأول الدودة المضيفة و التي تستخدم الشبكة لنسخ نفسها على أجهزة الحاسب الآلي المتصلة بالشبكة ، والنوع الثاني الدودة

---

* بالإضافة إلى الفيروسات السابقة الذكر، هناك عدة فيروسات:

فيروس مايكل أنجلو: أطلق هذا الفيروس يوم 6 مارس 1992 بمناسبة الإحتفال بذكرى ميلاد الرسام الإيطالي مايكل أنجلو الذي توفي عام 1964 وقد أصاب العديد من أجهزة الحاسوب.

فيروس ناسا أو نازا: عبارة عن برنامج يحمل رسالة مناهضة للأسلحة، وكان الهدف منه محاولة أختراق شبكة الحاسوب التابعة لوكالة الفضاء الأمريكية "ناسا"

الفيروس الإسرائيلي: وقد تم اكتشاف هذا الفيروس في الجامعة العبرية في القدس، وهو يقوم بإبطاء تشغيل النظام المعلوماتي إلى نص زمن التشغيل تقريبا بعد نصف ساعة فقط من تشغيل الجهاز.

عن موقع إسلام أن لاين. محمود سامي الشوا: "ثورة المعلومات وانعكاساتها على قانون العقوبات". دار النهضة 1995. ص: 108.

قال :كليولي: "إن بعض الناس قد يعتبره حميدا لأنه ينفذ مهمة جيدة ويحمي من المواقع الإباحية والدعارة الجنسية إلا أن الكثيرين يفضلون توظيف برامج إلكترونية قانونية وليس برامج يضعها أي متسلل إلكتروني وأن حصان طروادة هذا قد يحجز بعض الطلبات البريئة التي يطلبها الشبان المراهقون مثلا المواقع الطبية والإجتماعية.

الشبكية و التي تزرع أجزائها على عدة أجهزة حاسب آلي و تعتمد على الشبكة فيما بعد لتشغيل هذه الأجزاء ، و يمكن أن تظهر الدودة على أجهزة حواسيب منفصلة فتنسخ نفسها إلى أماكن متعددة على القرص الصلب ، وأهم أضرار الديدان هو إبطاء سرعة عمل الشبكة[1].

ومن أمثلة التخريب أو تعطيل المواقع على أنظمة المعالجة الآلية للمعطيات قضية مورس وهي أول الهجمات الكبيرة و الخطيرة في بيئة الشبكات ففي مارس 1988 تمكن طالب يبلغ من العمر 23 عاما ويدعى ROBER KORRIS من إطلاق فيروس عرف باسم دودة مورس عبر الإنترنت أدى إلى إصابة 6 آلاف جهاز يرتبط معها حوالي 60000 نظام عبر الإنترنت من ضمنها أجهزة العديد من المؤسسات و الدوائر الحكومية ، وقد قدرت الخسائر لإعادة تصليح الأنظمة وتشغيل المواقع المصابة بحوالي مائة مليون دولار إضافة إلى مبلغ أكثر من ذلك يمثل الخسائر غير المباشرة الناجمة عن تعطيل هذه الأنظمة.

***القنبلة الموقوتة:**

وهي فيروس ويعرف كذلك بالشيفرة ، وهو عبارة عن برنامج مصمم للنظام المعلوماتي يثبته بداخله و يكون ملتصق بملف أو برسالة بريد إلكتروني أو صورة أو إشعار ...ويبدأ عملها أو نشاطها في وقت لاحق محدد بزمن أو حدث معين ، وتكون الغاية منه تعطيل النظام المعلوماتي ، ويحدث نفس الأثر التخريبي لأحصنة طروادة من حذف و تعديل للبيانات....إلخ ، ولعل ما حدث في جامعة **مونموث** في الولايات المتحدة الأمريكية يعطينا صورة عن الأثر المدمر للقنابل الإلكترونية ، فبعد انفجار قنبلة إلكترونية استهدفت نظام البريد الإلكتروني للجامعة الذي ترتبط به أعمال و أنشطة على درجة عالية من الأهمية ، كالتسجيل و تبادل الأبحاث ودفع الرسوم ، انهار نظام البريد الإلكتروني ، وقدرت الخسائر بعشرات الآلاف من الدولارات ، غير أن فريق تحقيق فيدرالي تمكن من تحديد اليوم و الساعة وعنوان الكمبيوتر المستخدم في الجريمة ، و بعد مواجهة المتهم إعترف و حاول تدمير الكمبيوتر المستخدم في الجريمة ، و حاول تبرير فعله بأنه لم يقصد التخريب إلا أن ذلك لم يسعفه ، فاعتبرته المحكمة مذنبا وحكمت عليه بالسجن لمدة ثلاث سنوات و غرامة مالية مقدارها مائة ألف دولار[2].

[1]- منصور سعيد القحطاني، مهددات الأمن المعلوماتي، وسبل مواجهتها ، المرجع السابق، ص39.

[2]- فاطمة نعناع ، مقالة بعنوان قنبلة إلكترونية في بريد الجامعة ،منشور في مجلة إنترنت العالم العربي ، السنة الألى ، العدد السابع ، إبريل 1998،ص64-65.

***فيروسات الشبكة:** تنتشر عن طريق البريد الإلكتروني و خصوصا الرسائل التي تأتي لاحقا لعملية التخريب.

***باب المصيدة:**

عبارة عن رمز يتم توزيعه عند تركيب باب الحماية، ولكي يعطي المخزن حرية إختيار الوقت المناسب لعملية التخريب، حيث يسمح هذا الرمز بالنفاذ من خلال الشبكات في وجود نظم الحماية التي تعتاد على وجوده.

***فيروسات العتاد:**

تصمم لتصيب العتاد، حيث يبرمج الفيروس لتنفيذ ملايين العمليات الحسابية المثالية دون استخدام أوامر الإخراج أو الإدخال ، ومن ثم يلقي عبئا كبيرا على وحدة المعالجة المركزية ، فيؤدي إلى ارتفاع درجة حرارتها و احتراقها[1].

***القناة الخبيثة:**

وهي نوع خطير من الإعتداءات، و يقوم على مبدأ تهريب المعلومات عبر خرق سياسة الأمن و الحماية المعتادة في الأنظمة المعلوماتية، وهي في ذلك تتطلب ذكاءا فائقا من المعتدي، وقد تستخدم عبارات متعددة للإشارة إلى الإتلاف حيث تبين أن الإتلاف يمكن أن يحصل عن طريق التعطيل أو الإفساد أو الإدخال أو المحو أو التعديل، فإن الذي يبدو لنا أن تعطيل أو إفساد تشغيل برامج الحاسب الآلي لا يمكن أن يتم إلا من خلال إدخال معطيات أو معلومات أو بيانات جديدة أو محو أو تعديل المعطيات أو البرامج المخزنة بالجهاز لأن هذه الأفعال من شأنها تعطيل تشغيل النظام بصورة كلية أو بصورة جزئية، وهذا يتحقق من خلال إدخال الفيروسات التي سبق أن بينا أن أثرها لا ينصرف فقط على برامج التشغيل بل من الممكن أن يمتد أثرها إلى الأنظمة الأخرى[2]الملحقة بها، أي البرامج الخاصة بالمعالجة ، مما يؤدي إلى شغل ذاكرة الجهاز بصورة كاملة ، وبالتالي يصبح من غير الممكن التعامل مع هذه المعلومات أو المعطيات بمعالجتها أو باسترجاعها مطبوعة ، والسبب في ذلك أن الفيروس الذي يتم إدخاله ، أي البرنامج الدخيل محل برامج الحاسب الأصلية لا يستجيب

[1]- منصور بن سعيد القحطاني ، مهددات الأمن المعلوماتي و سبل مواجهتها ، المرجع السابق ،ص40

[2]- محمد حماد مرهج الهيتي ،جرائم الحاسوب ، المرجع السابق ، ص204.

للتعليمات و الأوامر التي توجه إليه، وذلك لامتلاء الذاكرة أو الأسطوانة بالمعلومات أو الأوار التي تصدر إليه مما ينشأ عنه عدم إشتغال الحاسب الآلي أو عدم قدرته على المعالجة، مما ينشأ عنه تعطيل البرنامج أو إتلافه.

لأن هناك من الفيروسات ما تؤدي إلى تكرار المعلومات المختزنة في الجهاز أو القرص أو الأسطوانة إلى الحد الذي يجعل الذاكرة مملوءة بالمعلومات ، وبسبب أن عمل الفيروس هو تكرار المعلومات فإن أي عملية حذف لأي جزء من هذه المعلومات التي تملأ الذاكرة ، من أجل أن تكون هناك سعة لإدخال معلومات جديدة أو لإصدار أوامر جديدة للتشغيل أو المعالجة سوف لن تكون ممكنة مما يتبع في النهاية إيقاف العمل بالبرامج أو عدم إمكان تشغيله أو استخدامه ، مما يحقق إتلاف البرنامج أو تعطيله[1].

[1]- محمد حماد مرهج الهيتي ،المرجع السابق ، ص205.

خلاصة الباب الأول:

يشهد العالم و بشكل كبير تطورا هائلا و متسارعا في تكنولوجيا عالم الإتصالات حتى أصبحت وسائل الإتصال الحديثة وعلى رأسها الإنترنت وسيلة لا يمكن الإستغناء عنها ، وهي تعد محرك الحضارة الجديدة التي تقوم عليها فكرة الإتصال لا الإنتقال ، وتعتبر هذه الشبكة هي إحدى ثمار الإندماج بين ثورة تكنولوجيا المعلومات و الإتصالات الرقمية فهذه الشبكة التي نشأت و تطورت بسرعة هائلة قد استطاعت أن تزيل الحدود و المسافات بين الدول و تجعل من العالم قرية صغيرة ، إلا أن هذه التقنية جلبت معها آثار سلبية خلفتها جرائم سميت بالجرائم الماسة بالمعطيات الرقمية لذلك تناولنا في الفصل الأول: تعريف المعطيات الرقمية و تبين بأنها : عبارة عن حقائق رقمية أو غير رقمية تتم بطريقة منهجية يمكن فهم دلالتها مباشرة دون الدخول في عمليات استنتاجيه استقرائية لدلالتها المعقدة من خلال أكثر من بيان.

ثم تطرقنا إلى خصائص هذه الجريمة ومن أبرز هذه الخصائص أن هذه الجرائم ترتكب بواسطة الحاسب الآلي باعتبارها الوسيلة الرئيسية الأكثر إستخداما في الجريمة و به يتم الإعتداء على الحواسيب الأخرى و الدخول إلى البرامج و سرقتها و إتلافها . وكانت شبكة الإنترنت مجالا خصبا للإعتداءات لذلك لجأ إليها البعض لتحقيق أهدافهم الإجرامية ، وباعتبار أن هذه الجرائم عابرة للحدود فقد ألغت كل الحدود الجغرافية ما جعلها تكتسب طبيعة دولية كاختراق الشيفرات البنكية و تبييض الأموال في دول مختلفة من العالم ، كذلك خاصية أخرى بأنها جريمة يصعب إكتشافها و إثباتها و السبب في ذلك أنها لا تترك آثارا خارجية مما يزيد الأمر تعقيدا ، وقد أعتبرت من الجرائم الناعمة لأنها لا تتطلب عنفا لسرقة المعلومات و البيانات أو نقلها من جانب لآخر أو معرفة الشيفرات الخاصة بالبنوك و السطو على أرصدتها ، رغم غياب العنف إلا أن النتيجة المراد تحقيقها تحققت وهنا تكمن نعومة هذه الجرائم ، كذلك تحتاج الجرائم الماسة بالمعطيات الرقمية إلى خبرة فنية عالية لاكتشافها و البحث عنها و ضبط الأدلة باحترافية لكن الواقع أثبت أن هناك نقص في الخبرة لدى الأجهزة الأمنية و القضائية لإثبات هذه الجرائم.

وفي الفصل الثاني : تناولنا صور التعدي على المعطيات الرقمية ومن أبرز صور التعدي على المعطيات الرقمية الجرائم التي ترتكب ضد الأشخاص و الأموال و الأمن ، فقد استخدمت هذه الجرائم في المساس بحرمة الحياة الخاصة للأشخاص ، وقد أصبح الأمر أكثر تعقيدا مع التطور العلمي و

التكنولوجي الحديث مما أدى إلى اختراع وسائل الإتصال الذكية فاستغلت في التنصت على المحادثات و اقتحام البريد الالكتروني وكسر الشيفرات الخاصة به و العبث بالملفات الخاصة بالأفراد مما زاد من إمكانية التطفل على أسرارهم و انتهاك حرمتها دون وجه حق.

أيضا تناولنا في هذا الفصل جرائم تقع على الأموال عبر الشبكة المعلوماتية و التي لم تقتصر على أساليب إساءة الثورة التقنية للأشخاص فحسب بل تعدى الأمر ليصل إلى الذمة المالية للغير عبر البنوك باختراقها بواسطة بطاقات الإئتمان و غيرها من أساليب الإحتيال ، حتى الأموال المعنوية كالمؤلفات و الإختراعات لم تسلم من هذه الإعتداءات الرقمية ، أما فيما يخص الجانب الخاص بالأمن الوطني ، فمن المعلوم أن التطور الذي شهده العالم اليوم على جميع الأصعدة كان نقطة تحول و قسم العالم إلى شق متطور جدا و الآخر متخلف ، وكان لتكنولوجيا الإتصالات مكانتها البارزة لكن البعض من هذه الدول إستغلتها استغلالا سلبيا ، و ارتكبت عددت جرائم مست أمن الدول كالتجسس الإلكتروني و القرصنة و اختراقات مواقع وزارة الدفاع لدى بعض الدول لذلك صنفت هذه الأعمال بأنها إرهاب إلكتروني واعتبر هذا الأخير من الظواهر الإجرامية التي تجاوزت آثارها حدود الدولة الواحدة فاكتسبت بذلك طابعا عالميا يهدد أمن و سلامة البشرية وحقوق الإنسان ، و حرياته الأساسية من جهة و مصالح الشعوب من جهة ثانية.

الباب الثاني:

الأحكـــام الإجرائيـة للحمـــاية الجنائية للمعطيات الرقميـة

الباب الثاني: الأحكام الإجرائية للحماية الجنائية للمعطيات الرقمية

بحكم تطور المجتمع و ظهور جوانب قانونية لقنوات الإتصال الحديثة أو ما يعرف بالتكنولوجيا الحديثة ، و مع التطور الكبير و المتسارع لأجهزة الحوسبة و الاتصالات تزايد الوعي لدى شعوب العالم ، و موازاة مع هذا التطور ظهرت مشكلة تتمثل في كيفية مواجهة هذا النوع الجديد من الإجرام غير المعهود به من قبل ، لذلك وجب مواجهة هذه الجرائم بإجراءات قانونية للحد منها فقد ظهر اتجاه في الفقه يدعو إلى تطويع النصوص الجنائية التي تتعلق بالجرائم التقليدية بتعديل هذه النصوص القانونية حتى تتلائم و طبيعة ما يسمى بالمال المعلوماتي أو بالمعطيات الرقمية ، و باعتبار هذه المعطيات الرقمية ذات قيمة مستحدثة ظهرت من خلال الإعتماد على الحاسب الآلي وشبكة الإنترنت من خلال مجموعة أوامر و تعليمات تمت معالجتها و أصبحت رموز و شفرات لا يمكن للإنسان العلم بها إلا من خلال الآلة و أثناء تشغيلها و هي تشبه المكالمات التلفونية و التيار الكهربائي ...إلخ وعليه فقد استقر الفكر القانوني لدى المشرعين على ضرورة و جود نصوص خاصة لتجريم الأفعال التي تمثل اعتداء أو إساءة استخدام للتكنولوجيا وأدى ذلك إلى إصدار تشريعات خاصة بهذه الجرائم كالولايات المتحدة الأمريكية استكملت بنيانها التشريعي مع نهاية القرن الماضي بشأن التشريعات التي تحكم المعاملات الإلكترونية و تواجه الجريمة الإلكترونية ، و كذلك فعل المشرع الفرنسي و الكندي و أكثر من 12 دولة في نطاق الاتحاد الأوربي ، وتعتبر هذه الدول سباقة في هذا المجال ، أما على الصعيد الوطني فإننا نلاحظ أن المشرع الجزائري بدأ ينتهج سياسة تشريعية خاصة فيما يتعلق بالجرائم الإلكترونية وذلك بداية من سنة2009 حيث أصدر المشرع الجزائري قانون خاص بالجرائم المعلوماتية ، وهو القانون رقم 09-15 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها.

لذلك فقد قسمنا هذا الباب الخاص بالأحكام الإجرائية للجرائم الماسة بالمعطيات الرقمية إلى فصلين تناولنا في الفصل الأول: التحقيق في الجرائم الماسة بالمعطيات الرقمية ، و في الفصل الثاني: إثبات الجرائم الماسة بالمعطيات الرقمية و الجزاءات المقررة لها.

الفصل الأول: التحقيق في الجرائم الماسة بالمعطيات الرقمية.

تطورت وسائل التحقيق الجنائي في عصر المعلوماتية تطورا ملموسا يواكب حركة الجريمة و تطور أساليب إرتكابها ، فبعد أن كان الطابع المميز لوسائل التحقيق العنف و التعذيب للوصول إلى الدليل ، أصبحت المرحلة العلمية الحديثة القائمة على الإستعانة بالأساليب العلمية و استخدام شبكة الإنترنت هي الصفة المميزة و الغالبة ، ومرد ذلك هو حدوث طفرة علمية في مجال تكنولوجيا المعلومات و الإتصالات و استخدام الوسائط الإلكترونية في شتى مجالات الحياة ، فكلما اكتشف العلم شيئا حديثا وجد الإكتشاف طريقه إلى مجال الإثبات الجنائي و التدليل.

و تبعا لذلك فإنه من البديهي أن تظهر أنماط جديدة من الجرائم لم تكن معهودة في السابق ، وهذا ليس قاصرا على أسباب التقدم التقني فقط بل يحدث دوما و بصفة مستمرة ، فالمجرم و الجريمة في تقدم و تجدد مستمر ، فمجرم الأمس ليس كمجرم اليوم.

ولا شك أن ظهور أنماط جديدة من الجرائم لم تكن مألوفة في السابق ونحن لا نزال في بداية عصر الإنفجار المعلوماتي ، يعنى توقع ظهور المزيد و المزيد من هذه الأنماط الجديدة ، والتي يتوجب معها تحديث الأنظمة و التعليمات و الجهات الأمنية المختصة لمعالجة القضايا الناتجة عن ظهور هذه الأنماط الجديدة ، وهو ما يستتبع تطوير أسلوب التحقيق فيها.

كما أن التحقيق عامة يعتمد على ذكاء المحقق و فطنته و قوة ملاحظته و سرعة البديهة لديه ، وأن يحاول بكل الجهد الممكن أن يقوم بالتحقيق في الجريمة و متابعتها و البحث فيها ، وفي الأدلة و التنقيب عنها وصولا لإظهار الحقيقة.

و نظرا لما يلعبه التحقيق في الجريمة من أهمية إرتأينا تقسيم هذا الفصل إلى مبحثين تناولنا في المبحث الأول: الأجهزة المكلفة بمكافحة الجرائم الماسة بالمعطيات الرقمية ، وفي المبحث الثاني : التفتيش في الجرائم الماسة بالمعطيات الرقمية.

المبحث الأول: الأجهزة المكلفة بمكافحة الجرائم الماسة بالمعطيات الرقمية.

منح القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و محافحتها دورا ايجابيا لمقدمي الخدمات من خلال مساعدة السلطات العمومية في مواجهة الجرائم وكشف مرتكبيها حيث تنص المادة الثالثة منه على وضع ترتيبات تقنية لمراقبة الإتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية.
ونص ذات القانون في مادته الرابعة على أربعة حالات يسمح فيها للسلطات الأمنية بممارسة الرقابة على المراسلات والإتصالات الإلكترونية ، منها الوقاية من الأفعال الموصوفة بجرائم الإرهاب والتخريب والجرائم التي تمس بأمن الدولة ، وكذلك في حال توفر معلومات عن احتمال إعتداء على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو النظام العام ، ولمقتضيات التحريات والتحقيقات القضائية ، عندما يصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية ، وفي إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.
ويحدد القانون طبيعة الترتيبات التقنية الموضوعة لتجميع وتسجيل معطيات ذات صلة بالوقاية من الإعتداء على أمن الدولة ومكافحة مثل هذه الجرائم ، وذلك تحت طائلة العقوبات المنصوص عليها في قانون العقوبات بالنسبة للمساس بالحياة الخاصة للغير.
وعلى هذا الأساس ، يجوز للجهات القضائية وضباط الشرطة القضائية الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها ، وكذا المعطيات المعلوماتية المخزنة فيها ، مع إمكانية اللجوء إلى مساعدة السلطات الأجنبية المختصة من أجل الحصول على المعطيات المبحوث عنها في منظومة معلوماتية تقع في بلد أجنبي ، ويسمح القانون للمحققين باستنساخ المعطيات محل البحث في حال تبين جدوى المعلومات المخزنة في الكشف عن الجرائم أو مرتكبيها لذلك ارتأينا تقسيم هذا المبحث إلى مطلبين: تناولنا في المطلب الأول: الأعوان المكلفون بالتحري وجمع الأدلة في الجرائم الماسة بالمعطيات الرقمية ، وفي المطلب الثاني: الوسائل المستخدمة في التحري و جمع الأدلة.

المطلب الأول: الأعوان المكلفون بالتحري وجمع الأدلة في الجرائم الماسة بالمعطيات الرقمية.

يعتبر جهاز الضبطية القضائية صاحب الولاية العامة في البحث والتحري عن الجرائم بمختلف أنواعها وأشكالها ، غير أن ذلك لا يمنع أن تعهد بعض القوانين الخاصة بهذا الدور على سبيل الإستثناء إلى بعض الجهات والهيئات الخاصة بحكم خبرتها في مجال معين وباعتبارها الأقدر من غيرها على

كشف الجرائم الواقعة ضمن حدود إختصاصها الفني أو التقني، والواقع أن ذلك لا يحول دون ضرورة تنسيق الجهود مع جهاز الضبطية القضائية التقليدي من أجل ضمان تحقيق أكبر قدر من الفعالية في مجال ضبط الجرائم والتحري بشأنها.

ومن أجل إشراك مزودي خدمات الإنترنت والإتصالات الثابتة والمتنقلة في محاربة الجرائم التكنولوجية، يلزم القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها هؤلاء بتقديم المساعدة للسلطات المختصة في مجال جمع وتسجيل المعطيات المتعلقة بمحتوى الإتصالات في حينها، وبوضع المعطيات الملزمين بحفظها ، وتشمل هذه المساعدة المعطيات التي تسمح بالتعرف على مستعملي الخدمة ، وتلك المتعلقة بالتجهيزات المستعملة في الإتصال ، والخصائص التقنية وتاريخ وزمن ومدة كل اتصال ، والمعطيات المتصلة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها ، بالإضافة إلى المعلومات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم وعناوين المواقع المطلع عليها.

ويتضمن القانون أيضا إجراءات عقابية حيث أنه ولتفادي أي تهرب من التزامات القانون 09-04 ، يسلّط هذا الأخير على الأشخاص الطبيعيين الذين يعرقلون سير التحريات القضائية عقوبة السجن من خمس إلى ستة سنوات وغرامة مالية تتراوح ما بين خمسة ملايين إلى خمسين مليون سنتيم ، مع معاقبة المؤسسات المخالفة بالغرامات المالية المنصوص عليها في قانون العقوبات.

من جهة أخرى يجبر القانون مقدمي خدمات الإنترنت على الإلتزام بالتدخل الفوري لسحب المحتويات التي بإمكانهم الإطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين، وتخزينها أو جعل الدخول إليها غير ممكن، إضافة إلى وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحتوي معلومات مخالفة للنظام العام أو الآداب العامة وإخطار المشتركين لديهم بوجودها، لذلك قسمنا هذا المطلب إلى فرعين تناولنا في الفرع الأول: الضبطية القضائية، وفي الفرع الثاني: دور مقدمي الخدمات في التحري والتحقيقات في الجرائم الماسة بالمعطيات الرقمية، وفي الفرع الثالث نتناول السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي.

الفرع الأول: الضبطية القضائية.

يعتبر أعضاء الشرطة القضائية موظفون منحهم القانون صفة الضبطية القضائية و خولهم بموجبها

حقوق و فرض عليهم واجبات في إطار البحث عن الجرائم و مرتكبيها وجمع الإستدلالات عنها فيبدأ دورهم بعد وقوع الجريمة و ينتهي عند فتح التحقيق القضائي أو إحالة المتهم إلى جهة الحكم و تتميز

الشرطة القضائية عن الشرطة الإدارية في أن المهمة الرئيسية لهذه الأخيرة تتمثل في تنفيذ تدابير الشرطة العامة ، الصادرة من السلطات المختصة و مراقبة نشاط الأفراد و الجماعات قبل وقوع الجريمة قصد المحافظة على الأمن العمومي ومنع أسباب الإضطرابات و إزالتها إذا وقعت فأعمال الشرطة الإدارية إجراءات وقائية ومانعة في حين أن أعمال الشرطة القضائية رادعة.

ـ مفهوم الضبط القضائي بصفة عامة:

1ـ أهمية وظيفة الضبط القضائي:

بالرغم من أن وظيفة الضبط لا تقل أهمية عن وظيفة التحقيق الذي يجريه قاضي التحقيق ، وبالرغم من أن أعماله تعتبر قانونية بالنسبة لإجراءات المحاكمة التي تقوم بها المحاكم إلا أن وظيفة الضبط بالرغم من أنها ليست وظيفة قضائية تماما إلا أنها وظيفة ضرورية لا يمكن الإستغناء عنها ، فهي ضرورية لفتح التحقيق بعد أن توجد دلائل كافية على وقوع الجريمة ، هذه الدلائل يبحثها الضبط القضائي ويقدمها لسلطة لتحقيق وهي ضرورية أيضا بالنسبة لقيام الدعوى العمومية فإن النيابة العامة لكي تباشر سلطتها في رفع الدعوى إلى قاضي التحقيق أو أمام قاضي الحكم أو حتى في حفظ الدعوى لا بد أن تقوم قبل ذلك بنفسها أو بواسطة ضباط الشرطة القضائية ببعض الإجراءات لكي تستخلص منها القرائن التي تستند إليها في رفع الدعوى أو في صرف النظر عنها بقرار الحفظ إذ رأت أنه لا فائدة من وراء بحث الدعوى أو أنه لا أهمية لرفعها ، إذن فمرحلة الضبط القضائي أو مرحلة الإجراءات الأولية ضرورية لقيام الدعوى العمومية ، فهي سابقة و حاسمة لها فإما أن تتقادم الدعوى بعد هذه المرحة أو تصرف النيابة النظر عنها و عن إقامتها على ضوء المعلومات التي جمعها الضبط القضائي، لأن مرحلة الضبط القضائي لا تعتبر مرحلة من مراحل الدعوى العمومية بالمعنى الصحيح لذلك فإن أعضاء هذا الجهاز لا يمكنهم أن يعاملوا الشخص كمتهم و لكن كمشتبه فيه و عند الانتهاء من هذه المرحة و تمكن الضبط القضائي من جمع الأدلة و العثور على مرتكب الجريمة تبدأ الدعوى العمومية بمعناها الصحيح عندما يبدأ قاضي التحقيق في إجراءات التحقيق بناءا على طلب من وكيل الجمهورية، وذلك لأن النيابة عندما طلبت من قاضي التحقيق الإختصاص بالتحقيق إنما

قصدت إقامة الدعوى على من اشتبه في أمره رجال الضبط القضائي ولقد حدد المشرع الجزائري فئات منحهم صفة الضبطية القضائية.

2ـ فئات الضبط القضائي:

نص قانون الإجراءات على أن الضبط القضائي يشتمل على ثلاثة فئات و هي ضباط الشرطة القضائية ، أعوان الضبط القضائي ، الموظفين و الأعوان المنوط بهم قانونا بعض مهام الضبط القضائي كما أوردت المادة 28 قانون الإجراءات الجزائية حكما خاصا في سلطات الولاة في مجال الضبط القضائي[1].

أولا: ضباط الشرطة القضائية.

أورد المشرع الجزائري الطوائف التي منحها صفة الضبط القضائي و قد جاء هذا البيان على سبيل الحصر وهي رؤساء المجالس الشعبية البلدية ، ضباط الدرك الوطني ، محافظوا الشرطة ، ضباط الشرطة ، ذوو الرتب في الدرك الذين أمضوا في سلك الدرك ثلاث سنوات على الأقل و الذين تم تعيينهم بموجب قرار مشترك صادر عن وزير العدل ووزير الداخلية بعد موافقة لجنة خاصة ، مفتشوا الأمن الوطني الذين قضوا في خدمتهم بهذه الصفة ثلاث سنوات على الأقل و عينوا بموجب قرار مشترك صادر عن وزير العدل ووزير الداخلية بعد موافقة لجنة خاصة ، ضباط و ضباط الصف التابعين للمصالح العسكرية للأمن الذين تم تعيينهم خصيصا بموجب قرار مشترك بين وزير الدفاع الوطني ووزير العدل[2].

ثانيا :أعوان الضبط القضائي

يعتبر من هؤلاء الأعوان طبقا بما جاء بالمادة 19 من قانون الإجراءات الجزائية ، موظفو مصالح الشرطة و ذوو الرتب في الدرك الوطني ورجال الدرك و مستخدمو مصالح الأمن العسكري الذين ليست هم صفة ضباط الشرطة القضائية.

ثالثا : الموظفون و الأعوان المكلفين ببعض مهام الضبط القضائي.

هي الفئة الثالثة من فئات الضبط القضائي التي أشارت إليها المادة 14 من قانون الإجراءات الجزائية

[1] ـ أنظر المادة 14 من الامر رقم 56 –155 المؤرخ في 18صفر1386 الموافق ل 8 جوان 1966 و المتضمن قانون الإجراءات الجزائية.
[2] ـ أنظر المادة 15 من قانون الإجراءات الجزائية القانون السابق.

و قد أوردت المادة 21 من نفس القانون بيانا عن هذه الفئة فهي تتكون من رؤساء الأقسام و الأعوان الفنيون و التقنيون المختصون في الغابات و حماية الأراضي و استصلاحها.

رابعا: الولاة.

نص المشرع على المشرع على حالة واحدة أجاز فيها لوالي الولاية القيام بأعمال الضبط القضائي و هي حالة وقوع جناية أو جنحة ضد أمن الدولة و وضعت لذلك شروط هي:

1. أن تكون الجريمة جناية أو جنحة.

2. أن يتطلب الأمر سرعة القيام بالإجراءات الضرورية لإثبات وقوع الجريمة.

3. ألاّ يكون قد وصل إلى علمه أن السلطات المختصة قد أخطرت بالحادث ، و في حالة توافر هذه الشروط يتولى والي الولاية إختصاصات الضبط القضائي فله أن يقوم بنفسه بكل الإجراءات الضرورية من تفتيش و حجز و إجراءات أولية خلال 48 ساعة يتخلى بعدها عن هذه المهمة ليسلمها إلى وكيل الجمهورية وله أيضا أن يكلف أحد ضباط الشرطة القضائية المختصين للقيام بهذه المهمة و الإجراءات حتى إنقضاء مدة 48 ساعة[1].

وما ينبغي الإشارة إليه فيما يتعلق بالضبطية القضائية أنها لم تسلم هي الأخرى من سلبيات التطور التكنولوجي و ما أفرزه من إجرام مستحدث إذ نتج عن ذلك نوع من التحدي الكبير لأجهزة العدالة الجنائية ، أجهزة التحقيق ، وأجهزة القضاء وأجهزة ضبط الجرائم و المتمثلة في رجال الضبطية القضائية ، إذ أصبح هؤلاء شبه عاجزين عن الكشف عن مثل هذه الجرائم ، نظرا لما تتميز به من خصائص راجعة إلى طبيعتها الخاصة و ما يكتنفها من تعقيد ، فضلا عن عجزهم عن ملاحقة مرتكبيها.

ولقد أثير في المؤتمر الدولي لجرائم الحاسوب المنعقد في أوسلو النرويج في الفترة ما بين 29، 05/31 /2000 موضوع عدم إمكانية البحث في البنية التحتية للإنترنت من أجل الوصول إلى تحديد شخصية مرتكب الجريمة أو المصدر الحقيقي لها و موقعه على وجه التحديد ، وإن كانت توفر إمكانية التعرف على عنوان رقم الحاسوب فقط المرتبط بالإنترنت و المستعمل كوسيلة لارتكاب

[1] ـ أنظر المادة 28 من قانون الإجراءات الجزائية، القانون السابق.

الجريمة ،أي ما يطلق عليه في النظام Internet Protocol (IP) و بالتالي تحديد الشخص صاحب ذلك الرقم بسهولة ، لتبدأ بعد ذلك سلسلة إثبات إرتكاب الجريمة من عدمه ، ولكن وفي المقابل ذلك فإن هذا الرقم ليس موحدا على المستوي العالمي إذ أن هناك أقلية من الدول التي تتبعه دون غيرها و خاصة الدول العربية.[1]

فمثلا في الولايات المتحدة الأمريكية و كندا يمكن للشخص فيها إقتناء " IP " خاص به يشير إلى كونه أحد أعضاء الإنترنت ، ومن ثم يمكن تحديد هذا الشخص بكل سهولة لتبدأ بعد ذلك عملية إثبات إرتكابه للجريمة من عدمه ، وما إذا كان غيره قد إستخدام هويته المذكورة أو حاسوبه لارتكاب جرائم ما ، و العكس في الدول العربية إذ أن مصداقية الهوية عبر الإنترنت IP تتقلص كثيرا ، ذلك لأن كل خط هوية على الإنترنت يصادفه عدد من الهويات التي يمكن أن تكون محلا للتغاير بين أعضاء الإنترنت المشتركين في مزود إنترنت واحد ، فمثلا بمجرد وجود شخص في أي دولة فإنه يملك فورا هوية رقمية محددة حقا حال وجوده على الإنترنت إلا أنه إذا حدث وانقطع الإرسال فإن الشخص إذا عاد من جديد إلى الإنترنت فإن الهوية السابقة لن تكون له و إنما لغيره ، وقد يتواجد حينها بهوية IP أخرى[2].

ولذلك كان من الضروري إعداد وتجهيز قوات خاصة لمواجهة هذا العدوان الإلكتروني عبر الإنترنت ، و الذي أصبح أحد الهواجس التي تعيشها المجتمعات القديمة و النامية ، وهذا ما توصلت إليه دول كثيرة وجاءت به توصية المجلس الأوروبي رقم (95) 13 في 1995/09/11 في شأن مشاكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات ، إذ دعت إلى ضرورة تشكيل وحدات خاصة

---

[1] ـ عمر محمد أبو بكر بن يونس ، الجرائم الناشئة عن استخدام الانترنت ، دار النهضة العربية ، القاهرة ، 2004، ص811.
يعرف (IP) وهو اختصار كلمة internet protacop أنه الوسيلة لنقل البيانات من مكان على الانترنت إلى مكان آخر أما (IP adresse) فهو عنوان مكون من أربعة أرقام و تستخدم لتحديد جهاز يتصل بالانترنت ، ذلك أنه عندما يتجول مستخدم الانترنت في حوار إنترنت ، فإنه يترك آثار أقدامه في كل مكان يزوره ، ذلك أن الموقع الذي يمر يفتح سجلا خاصا به يتضمن عنوان الموقع الذي جاء منه ،نوع الكمبيوتر و المتصفح الذي يستخدمه ، وعنوان رقم ip الدائم و المتغير للكمبيوتر الذي يتصل منه ، ويمكن تحت ظروف معينة ، أن يتمكن الموقع من الحصول على عنوان البريد الالكتروني ، و الاسم الحقيقي و يقول لعض الخبراء كمبيوتر أنه يمكن استخدام برمجيات جيقا أو جيقا سكريب معرفة عنوان البريد الالكتروني للمتصل و بعض المعلومات الأخرى عنه ، رغم عدم قانونية هذا العمل إلا إذا كان بتصريح خاص من النيابة أو القاضي المختص ، وذلك للبحث عن أدلة في نطاق عمل الضبطية القضائية لرجال القانون ، وأسهل طريقة لمعرفة ما تسجله المواقع التي= = يزورها مستخدم الانترنت هو التوجه لموقع www .consumer . net/ analyze و الانتظار قليلا قبل أن يكتشف هذا الموقع المعلومات و يعرضها أمام رجال الضبطية على الشاشة.
و يمكن الاستفادة عما يكشف عنه الرقم (IP) في البحث و التحقيق الجنائي ، ذلك أنه عندما يزور شخص ما موقعا على الشبكة ، يسجل الموقع (IP) العائد للكمبيوتر الذي اتصل به ، وعند إرسال بريد إلكتروني كذلك ، و يمكن لمتسلم الرسالة معرفة عنوان (IP)للكمبيوتر المرسل ، كذلك عند استخدام برنامج (الأوت لوك) فيكفي النفر على أوبشن option بعد أن يفتح الرسالة ، فيتم الاطلاع على عنوان المرسل.راجع خيرت علي محرز، التحقيق في جرائم الحاسب الآلي ، دار الكتاب الحديث ، 2012، ص63

[2] ـ عمر محمد أبو بكر بن يونس ، المرجع نفسه ،ص 811.

لمكافحة جرائم الحاسب الآلي و إعداد برامج خاصة لتأهيل العاملين في مجال العدالة الجنائية لتطوير معلوماتهم في مجال تكنولوجيا المعلومات ، وكذلك ما دعى إليه وزير الداخلية الفرنسي السابق Dominique de Villepin[1].

الفرع الثاني: دور مقدمي الخدمات في التحري والتحقيقات في الجرائم الماسة بالمعطيات الرقمية.

أولا: المقصود بمقدمي الخدمات.

إن تكنولوجيات الإعلام و الإتصال متنوعة حيث تتعلق بخدمات الإتصال السلكية واللاسلكية ، كالهواتف النقالة والشبكات الرقمية المتمثلة في الإنترنت ، وإن توصيل الخدمات المتنوعة لهذه التكنولوجيا المتنوعة إلى مستعمليها يتطلب توافر مجموعة من الفاعلين على رأسهم مقدمي الخدمات ، المنصوص عليهم في القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها الذي يعرفهم على أنهم "أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الإتصال بواسطة منظومة معلوماتية و/ أو نظام للإتصال ، وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الإتصال المذكورة أو لمستعمليها".[2]

وتجدر الإشارة إلى أن المشرع في تعريفه لمقدمي الخدمات قد جمع ثلاثة أنواع من الوسطاء يسمح تدخلهم بتوصيل خدمات تكنولوجيا المعلوماتية بأنواعها إلى مستعمليها وهم:

1 ـ مقدمي (متعهدي خدمة التوصيل).

2 ـ متعهدي الإيواء.

3 ـ مقدمي المضمون.

هؤلاء الوسطاء في تقديم الخدمات نص عليهم المشرع الفرنسي وأعطى لكل واحد منهم تعريفه الخاص ، ولكن المشرع الجزائري جمع هؤلاء المقدمين في إسم واحد وهم مقدمي الخدمات لأن جميعهم لديهم الإلتزامات نفسها ويتحملون نفس المسؤولية الجنائية على عاتقهم في حالة تقصيرهم أو مخالفتهم

[1] ـ نبيلة هبة هروال، المرجع السابق ، ص 99.

[2] ـ أنظر المادة 02 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها.القانون السابق.

للأنظمة المقررة قانونا.

أولا ـ مقدمي خدمة التوصيل (متعهدي التوصيل): يشارك متعهدي التوصيل بإرسال وتوجيه المعلومات

عن طريق الشبكات بتقديم الأجهزة والخدمات التقنية لمستعمليها من أجل الإتصال بالشبكات وهم كما سبق تعريفهم أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الإتصال بواسطة منظومة معلوماتية و/أو نظام للإتصالات.

جامعا بذلك نوعين من خدمات التوصيل ، خدمات التوصيل بالإنترنت وكذلك الأمر خدمات التوصيل بمنظومات الإتصال المختلفة ومنها شبكات الهاتف النقال ، وبالنسبة للمشرع الفرنسي فإنه قد عرفهم بأنهم " الأشخاص الذين يضمنون نشاط خدمة التوصيل بشبكة إتصالات إلكترونية".

2 ـ متعهدي (مقدمي) خدمة الإيواء:

عرف المشرع الجزائري مقدمي خدمة الإيواء في القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها على أنهم :أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الإتصال المذكورة أو لمستعمليها ، وعليه فإنه لا يستطيع أي شخص سواء أكان طبيعيا أو معنويا أن ينشأ موقعا خاصا إلا عن طريق متعهد إيواء المواقع ، وبعبارة أخرى فإن هؤلاء الأشخاص يقومون باستضافة أو بإيواء المواقع المختلفة لجعلها في متناول مستخدمي الإنترنت ، وذلك بالسماح للغير بالإطلاع على محتوياتها في أي وقت وكذلك عرفهم المشرع الفرنسي بأنهم" كل الأشخاص الطبيعية أو المعنوية الذين يقدمون خدمة للجمهور بواسطة وسائل الإتصال عبر الإنترنت للجمهور: تخزين الرموز والكتابات والصور والأصوات أو الرسائل أي كانت طبيعتها لفائدة مستعملي هذه الخدمات[1] .

3 ـ مقدمو المضمون(الناشرون):

مقدم المضمون أو الناشر هو الشخص الذي يحرر الرسالة ومن ثمة يضعها على الإنترنت أي ينشرها إلكترونيا ، فهو يستخدم خدمات الإتصالات المختلفة وخاصة منها الإنترنت لنشرها على الجمهور.

[1]- أحمد مسعود مريم ، آليات مكافحة جرائم تكنولوجيات الإعلام والاتصال في ضوء القانون رقم 09-04 ، مذكرة ماجستير في الحقوق تخصص قانون جنائي ، كلية الحقوق والعلوم السياسية ، قسم الحقوق ، جامعة قاصدي مرباح ، نوقشت بتاريخ 23 /2013/04 ، ص98.

وكما يوجد مقدمو خدمات المضمون المحترفون مثل الناشرين ، هناك آخرون غير محترفين مثل: منشئي المدونات لأنه الآن وبتطور الإنترنت أصبح لمشتركيها إنشاء مضامين خاصة بهم[1].

ثانيا: إلتزامات مقدمي الخدمات.

لقد أورد المشرع الجزائري كنظيره الفرنسي مجموعة من الإلتزامات على عاتق مقدمي الخدمات تكاد تكون متماثلة على الرغم من أن المشرع الجزائري قد أغفل الدور الذي يلعبه مقدمو خدمات المضمون وأهميته في البحث والتحري للكشف عن الجرائم الماسة بالمعطيات الرقمية ، وذلك لتحديد المسؤولية الجزائية المترتبة على نشر المضمون المجرم عبر مختلف المواقع الإجتماعية الإفتراضية ، وعليه سنتناول الإلتزامات المفروضة على نوعين من مقدمي الخدمات وهما مقدمي خدمة التوصيل ومقدمي خدمة الإيواء.

1 ـ الإلتزام بحفظ المعطيات المتعلقة بحركة السير ومساعدة السلطات القضائية:

عرف المشرع الجزائري المعطيات المتعلقة بحركة السير في المادة 02 فقرة هـ بأنها " أي معطيات متعلقة بالإتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا من حلقة اتصال ، توضح مصدر الإتصال ، والوجهة المرسل إليها والطريق الذي يسلكه ، ووقت وتاريخ وحجم ومدة الإتصال ونوع الخدمة ، إن الإلتزام بحفظ المعطيات المنصوص عليها في المادة 11 من القانون 09-04 المذكور أعلاه التي أوجبت على عاتق مقدمي الخدمات بنوعيهما – التي نص عليها المشرع دون تحديد صنفيهما وهما مقدمي خدمات التوصيل بالإنترنت أو منظومة الإتصال ومقدمي خدمة الإيواء الخاصة بالإنترنت – حفظ المعطيات بشكل يسمح بالتعرف على الأشخاص المساهمين في إنشاء المحتويات على الإنترنت (المدونات ، الصفحات الخاصة ، والإعلانات في مواقع البيع عن طريق المزاد....) وذلك من أجل التبليغات المحتملة للسلطات القضائية أو في حالة طلب هذه الأخيرة

[1]- المدونون (مقدمي خدمات خاصين): المدونة عبارة عن موقع على شبكة الإنترنت ينشئه شخص يطلق عليه إسم المدون يتناول فيه كل ما يخص الحياة في مجتمعه أو المجتمعات الأخرى ، إلا أن المدونة تختلف عن الموقع وتختلف عن المنتدى ، كون المدونة تكون مجهولة لدى الجهة الرسمية المسؤولة عن الموافقة على إنشاء المواقع على شبكة الانترنت في البلد الذي أنشأ فيه المدون مدونته ، وليس هذا فحسب وإنما يقوم المدون الذي يستخدم دائما إسما مستعارا وأيضا المشاركون معه في المواقع وبالتحدث بحرية مطلقة وانتقاد الأوضاع الموجودة في البلد الذي ينتمون إليه ، والبلاد الأخرى ، وفي قرار صادر عن الغرفة الجنائية بمحكمة النقض الفرنسية في 10 نوفمبر 2009 التي رأت أن عبارات القذف الموضوعة في مدونة تابعة لجريدة La république de centre-ouest سمحت بإقامة المسؤولية الجزائية للناشر ولمدير النشرية لأن المدونة تعد جزءا مكملا لكيان الجريدة ، والتبرئة التي استفاد منها كانت لسبب واحد هو أن الدليل لم يقم على الناشر للعبارات المجرمة كانت على علم بشرها ، فمحكمة النقض سوت بطريقة واضحة بين وضعية المدونة مع تلك المرتكزة على الإعلام التقليدي. أنظر أحمد مسعود مريم المرجع نفسه، ص100.

لأجل التحريات أو المعاينات وبحسب القانون فإن مقدمي الخدمات غير ملزمين بوضع ملفات إسمية لمستعملي الخدمات ، كما لا يمكنهم الإحتفاظ بالمعلومات المتعلقة بمضمون الإتصالات ، نصوص الرسائل القصيرة ، أو مواضيع البريد الالكتروني ، كذلك حدد المشرع مدة حفظ هذه المعطيات لمدة لا تزيد عن سنة واحدة إبتداءا من تاريخ التسجيل[1].

إلا أنه بالنظر لنص المادة 10 الفقرة الأولى من القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال ومكافحتها نجد أن المشرع قد سمح بتسجيل المعطيات المتعلقة بمحتويات الإتصال ولكن بشرط أن يكون في حينه[2] ، وهو إجراء تسخير من طرف السلطات القضائية لمقدمي الخدمات المعنيين لجمع وتسجيل المعطيات المتعلقة بمحتوى الإتصالات أيا كانت (مكالمات صوتية هاتفية أو مكالمات فيديو عبر مواقع الإنترنت SMS, Email, MMS) ولكن لم يحدد المشرع الجزائري على عكس المشرع الفرنسي مدة تسجيل هذه الإتصالات وتركها مفتوحة ، كما لم يحدد الأشخاص المكلفين بتسخير مقدمي الخدمات للقيام بهذا الإجراء الخطير ، بينما المشرع الفرنسي في نص المادة 60 الفقرة 2 من قانون الإجراءات الجزائية سمح لضباط الشرطة القضائية بتسخير من وكيل الجمهورية مع ترخيص مسبق من طرف قاضي الحريات والحبس ، بتسخير مقدمي الإتصالات للجمهور عبر الإنترنت للقيام بكل الإجراءات التي تؤمن الحفظ لمدة لا تزيد عن سنة واحدة لمحتويات معلوماتية التي تتم من طرف أشخاص مستعملين للخدمات التي يؤمنها مقدمو الخدمات المعنيون.

هذه الأحكام المختلفة بين القانونين والتي تهدف إلى نفس النتيجة وهي حفظ معطيات تتعلق بتسجيل وجمع محتوى إتصالات في حينها تختلف من حيث:

1-1 ـ الأشخاص الذين يحق لهم تقديم طلب المساعدة (والتي نص عليها المشرع الفرنسي بلفظ التسخير) يكون طلب المساعدة في التشريع الجزائري للسلطات المكلفة بالتحريات القضائية ، بما فيهم ضباط الشرطة القضائية ، فهل يستوجب على هؤلاء طلب إذن من وكيل الجمهورية أو قاضي التحقيق بحسب الحالة للقيام بطلب المساعدة من مقدمي الخدمات؟.

[1] ـ أحمد مسعود مريم ، المرجع السابق ، ص101.

[2] ـ أنظر المادة 10 من القانون رقم 09 ـ 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها ، المرجع السابق.

وذلك عكس المشرع الفرنسي الذي قدم ضمانات قانونية تكفل حماية الحياة الخاصة للأشخاص وذلك عندما نص على أن طلب المساعدة يكون بتسخير من وكيل الجمهورية والذي بدوره لا يمكنه منح هذا التسخير إلا بوجود ترخيص مسبق من قاضي الحريات والحبس ، هذه الإجراءات يرى البعض أنها تحد من التجاوزات التي يمكن لأعوان الضبط القضائي ممارستها في حالة التحريات عن الجرائم الرقمية.

1-2 ـ من حيث مدّة حفظ هذه المحتويات الخاصة بالإتصالات الآنية: إن تحديد مدة الحفظ يسمح بتعجيل إجراءات المتابعة الجزائية إن كان لها محل ، وهو ما قدره المشرع الفرنسي (بسنة واحدة لحفظ المكالمات) وهو ما يجب على المشرع الجزائري أن يأخذ به[1].

1-3 ـ أصناف المعطيات الواجب حفظها: لقد أوضح المشرع الجزائري أصناف المعطيات التي يجب على مقدمي الخدمات حفظها وهي:

أـ المعطيات التي تسمح بالتعرف على مستخدمي الخدمة (مثال ذلك عنوان IP ، رقم الهاتف ، عنوان البريد الالكتروني).

ب ـ المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للإتصال.

ج ـ الخصائص التقنية وكذلك تاريخ ووقت ومدة كل اتصال.

د ـ المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها.

هـ ـ المعطيات التي تسمح بالتعرف على المرسل إليه ، أو المرسل إليهم عند الإتصال وكذا عناوين المواقع المطلع عليها[2].

2 ـ الإلتزام بتصفية المواقع وبيان نوعها: نص القانون رقم 09-04 على أنه " زيادة على الإلتزامات المنصوص عليها في المادة 11 أعلاه يتعين على مقدمي خدمات الإنترنت ما يلي:

أ ـ التدخل الفوري لسحب المحتويات التي يتيحون الإطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن.

[1] ـ أحمد مسعود مريم ، المرجع السابق ، ص101.

[2] ـ المادة 11 من القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجات الإعلام والإتصال ومكافحتها ، القانون السابق.

ب ـ وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام والآداب العامة ، وإخبار المشتركين لديهم بوجودها".

ـ بالنسبة للتدخل الفوري لسحب المحتويات التي يتيحون الإطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن ، هذا الإلتزام الذي فرضه المشرع على مقدمي الخدمات ، لم يفرض فيه مسؤولية جزائية في حال عدم تنفيذه ، مما يؤدي إلى القول بأن هذا الإلتزام ، إلتزام أدبي من طرف مقدمي الخدمات ، لأن المشرع لم يفرض عقوبة رادعة في حالة مخالفة مقدمي الخدمات لهذا الإلتزام، وفي هذه الحالة لا يمكن مطالبة مقدمي الخدمات المتقاعسين عن أداء واجبهم في حذف المضامين المجرمة والمخالفة للقوانين بتعويضات مدنية في حالة حدوث أضرار نتيجة عرض المضامين المجرمة عبر الإنترنت دون رقيب في انتظار تحريك الدعوى العمومية التي يمكن من خلالها وبطلب من السلطة القضائية وقف هذه المضامين المجرمة، بينما المشرع الفرنسي فرض المسؤولية المدنية والجزائية على مقدمي خدمة الإيواء الذين يرفضون أو يتقاعسون عن القيام بالتزامهم المتمثل في سحب المحتويات المخالفة للقوانين أو جعل الدخول إليها غير ممكن ، وهو ما نصت عليه المادة 06 الفقرة 1 و 2 من القانون رقم 2004/575 الصادر في 21 جوان 2004 من أجل الثقة في الإقتصاد الرقمي ، حيث نص على أن المسئولية المدنية أو الجزائية لمقدم خدمة الإيواء لا يمكن أن تقوم إلا في حالة العلم الحقيقي بالوقائع أو الظروف التي بموجبها يكون النشاط أو المعلومة مجرمة ، وفيما يتعلق بالمطالبة بالتعويضات فلا تقوم إلا على وجود العلم بأن الوقائع أو الظروف بحسب النشاط أو المعلومة تكون مجرمة ولم يتصرف مقدم خدمة الإيواء فورا لسحب المعلومات أو بجعل الوصول إليها مستحيلا.

ـ أما بالنسبة لبيان نوع المواقع التي تحوي معلومات مخالفة للنظام العام والآداب العامة فإن المشرع ألزم مقدمي الخدمات بوضع ترتيبات تقنية تسمح لمستعملي الإنترنت بالتعرف وبسهولة على نوع هذه المواقع[1] وبالطبع يجب أن تكون واضحة و يمكن لمن أراد أن يدخل لمواقع معينة معروفة أنها مواقع مخالفة للنظام العام والآداب العامة معرفة ذلك قبل الدخول إليها.

كما يجب لهذه التقنيات أن تعلم لمن يستعملها بوجود وسائل تقنية تسمح بحصر الدخول إلى هذه

[1] - المادة 12 من القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجات الإعلام والإتصال ومكافحتها ، القانون السابق

المواقع كالمراقبة الأبوية التي تمنع القصر من الدخول إلى هذه المواقع باستعمال برامج وقائية تتطلب كلمة سر معينة[1].

الفرع الثالث: السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي

بموجب القانون المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، يتم إنشاء سلطة إدارية مستقلة لحماية المعطيات ذات الطابع الشخصي من طرف رئيس الجمهورية[2] ، تسمى اختصارا "السلطة الوطنية" يكون مقرها الجزائر العاصمة وتكون لها الشخصية المعنوية والإستقلال المالي والإداري وتقيد ميزانية السلطة الوطنية في ميزانية الدولة ، وتعد السلطة الوطنية نظامها الداخلي الذي يحدد لا سيما كيفيات تنظيمها وسيرها وتصادق عليه وتتشكل من[3]:

- ثلاثة شخصيات يختارهم رئيس الجمهورية بما فيهم الرئيس، على أن يكونوا ذوي الإختصاص في المجال.
- ثلاثة قضاة يقترحهم المجلس الأعلى للقضاء من بين قضاة المحكمة العليا ومجلس الدولة
- عضو عن كل غرفة من البرلمان يتم اختيارهم من قبل رئيس كل غرفة مع التشاور مع رؤساء المجموعات البرلمانية.
- ممثل عن المجلس الوطني لحقوق الإنسان.
- ممثل عن وزير الدفاع الوطني.
- ممثل عن وزير الشؤون الخارجية.
- ممثل عن الوزير المكلف بالداخلية.
- ممثل عن وزير العدل حافظ الأختام.
- ممثل عن الوزير المكلف بالمواصلات السلكية واللاسلكية والتكنولوجيات والرقمنة.
- ممثل عن الوزير المكلف بالصحة.
- ممثل عن الوزير المكلف بالعمل والضمان الإجتماعي.

يتم اختيار أعضاء السلطة الوطنية حسب اختصاصهم القانوني أو التقني في مجال معالجة المعطيات ذات الطابع الشخصي ويمكن السلطة الوطنية أن تستعين بأي شخص مؤهل من شأنه مساعدتها في

[1] - أحمد مسعود مريم ، المرجع السابق ، ص103.
[2]- المادة 22 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي ، القانون السابق.
[3]- المادة 23 من القانون رقم 18-07 من القانون نفسه.

مهامها، ويعين الرئيس وباقي أعضاء السلطة الوطنية بموجب مرسوم رئاسي لعهدة مدتها خمس سنوات قابلة للتجديد.

وقبل التنصيب في الوظيفة يؤدي أعضاء السلطة الوطنية اليمين أمام مجلس قضاء الجزائر العاصمة[1].

وتعمل السلطة الوطنية على السهر على مطابقة معالجة المعطيات ذات الطابع الشخصي لأحكام القانون ، وضمان عدم وجود أي أخطار تجاه حقوق الأشخاص والحريات العامة وحرمة الحياة الخاصة عند استعمال تكنولوجيات الإعلام والإتصال[2].

وتتمثل مهامها على وجه الخصوص في:

- منح التراخيص وتلقي التصريحات المتعلقة بمعالجة المعطيات ذات الطابع الشخصي
- إعلام الأشخاص المعنيين بالمعالجة بحقوقهم وواجباتهم.
- تقديم الإستشارات للأشخاص والكيانات التي تلجأ لمعالجة المعطيات ذات الطابع الشخصي أو التي تقوم بتجارب أو خبرات من شأنها أن تؤدي إلى مثل هذه المعالجة
- تلقي الإحتجاجات والطعون والشكاوى بخصوص تنفيذ معالجة المعطيات ذات الطابع الشخصي وإعلام أصحابها بمآلها.
- الترخيص بنقل المعطيات ذات الطابع الشخصي نحو الخارج وفقا للشروط المنصوص علها في هذا القانون.
- الأمر بالتغييرات اللازمة لحماية المعطيات ذات الطابع الشخصي المعالجة.
- الأمر بإغلاق معطيات أو سحبها أو إتلافها.

ويقع على عاتق الرئيس وأعضاء السلطة الوطنية واجب المحافظة على الطابع السري للمعطيات ذات الطابع الشخصي والمعلومات التي يطلعون عليها بمناسبة أدائهم لمهامهم ، ما لم يوجد نص قانوني يقضي بخلاف ذلك[3].

وإضافة إلى ضباط وأعوان الشرطة القضائية ، فإن أعوان الرقابة الآخرون الذين تلجأ إليهم السلطة الوطنية يكونون مؤهلين للقيام ببحث ومعاينة الجرائم المتعلقة بالمعطيات الشخصية، تحت إشراف وكيل الجمهورية[4].

[1] ـ المادة 24 من القانون رقم 18-07. المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.القانون السابق

[2] ـ المادة 25 من القانون رقم 18-07 من القانون نفسه

[3] ـ المادة 26 من القانون رقم 18-07 من القانون نفسه.

[4] ـ ونصت المادة 50 من القانون رقم 18-07 من القانون نفسه.

وتتم معاينة هذه الجرائم بواسطة محاضر، يجب أن توجه فورا إلى وكيل الجمهورية المختص إقليميا، ويمكن لكل شخص يدعي أنه تم المساس بحق من حقوقه المتعلقة بمعالجة المعطيات الشخصية، أن يطلب من الجهة القضائية المختصة اتخاذ أي إجراءات تحفظية لوضع حد لهذا التعدي أو للحصول على تعويض.

وتختص الجهات القضائية الجزائرية بمتابعة الجرائم، التي ترتكب خارج إقليم الجمهورية، من طرف جزائري أو شخص أجنبي مقيم في الجزائر أو شخص معنوي خاضع للقانون الجزائري، يكون موضوعها المساس بالمعطيات ذات الطابع الشخصي المعالجة آليا .

كما تختص الجهات القضائية الجزائرية بمتابعة هذه الجرائم وفقا لقواعد الإختصاص المنصوص عليها في المادة 588 من الإجراءات الجزائية[1].

المطلب الثاني: الوسائل المستخدمة في التحري وجمع الأدلة.

عند القيام بالتحقيق في جريمة ما ، فإنه يجب على المحقق الإلتزام بقوانين و تشريعات و لوائح مفسرة ، و قواعد فنية تحقق الشرعية ، و سهولة الوصول إلى الجاني ، وحيث أن للجرائم المعلوماتية طابعها الخاص المميز لها ، فإن التحقيق فيها يحتاج إلى معرفة تامة و إدراك لوسائل وقوع الجريمة و بالتالي حل لغزها و الوصول إلى الجاني لذلك تناولنا هذا المطلب في فرعين ، الفرع الأول: الوسائل القانونية ، و الفرع الأول: الوسائل المادية.

الفرع الأول: الوسائل القانونية.

ويقصد بها الإجراءات التي باستخدامها يتم تنفيذ طرق التحقيق الثابتة والمحددة والمتغيرة والغير محددة التي تثبت وقوع الجريمة وتحدد شخصية مرتكبها ومنها:

أولا ـ إقتفاء الأثر: من أخطر ما يخشاه مجرم نظم المعلومات تقصي أثره أثناء ارتكابه للجريمة ، فهناك الكثير من الوثائق التي يتم نشرها في المواقع الخاصة بالمخترقين تحمل بين جنباتها العديد من النصائح أولاها نصيحة قم بمسح آثارك ، فلو لم يقم المخترق بمسح آثاره فمن المؤكد أنه سوف يتم القبض عليه ، حتى وإن كانت عملية الإختراق قد تمت بشكل سليم ، ويمكن تقصي الأثر بطرق عدة

[1] ـ أنظر المادة 53 من القانون رقم 18-07. المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي ، القانون السابق.

سواء عن طريق بريد الكتروني تم استقباله ، أو عن طريق تتبع أثر الجهاز الذي تم استخدامه للقيام بعملية الإختراق.

ثانيا: الإطلاع على عمليات النظام المعلوماتي وأسلوب حمايته.

ينبغي على المحقق وهو بصدد التحقيق في إحدى الجرائم الماسة بالمعطيات الرقمية، أن يطلع على النظام المعلوماتي ومكوناته من شبكات وتطبيقات وخدمات تقدم للعملاء ، كما ينبغي عليه الإطلاع على عمليات النظام المعلوماتي ، كقاعدة البيانات وإدارتها وخطة تأمينها ومعرفة مواد النظام والمستفيدين والملفات والإجراءات وتصنيف الموارد العامة ، ومدى مزامنة الأجهزة ، ومدى تخصيص وقت معين في اليوم يسمح باستخدام كلمات المرور ، ومدى توزيع الصلاحيات للمستخدمين ، وإجراءات أمن العاملين ، وأسلوب النسخ الإحتياطي والإستعانة ببرامج الحماية ، كمراقبة المستفيدين والموارد والبرامج التي تعالج البيانات وتسجيل الوقائع وحالات فشل الدخول إلى النظام ، بالإضافة إلى معرفة نوعية برامج الحماية وأسلوب عملها ، والإستفادة من التقارير التي تنتجها نظم أمن البيانات وتقارير جدران الحماية ، ويراعى هنا ضرورة أن يتأكد قائد فريق التحقيق من حرص جميع أعضاء فريق التحقيق على الأمور التالية أثناء تعاملهم مع الأدلة الرقمية على وجه الخصوص:

1 ـ عدم القيام بأي عمل من شأنه إحداث تعديل أو تغيير أي دليل.

2 ـ عدم تنفيذ أية برامج على الحواسيب الموجودة في موقع الجريمة ، خصوصا البرامج ذات الصلة بأنظمة التشغيل.

3 ـ ضرورة عمل نسخة مطابقة للأقراص الصلبة ، ومن ثمة عمل الفحوصات الجنائية على هذه النسخة فقط ، سواء تم ذلك داخل مسرح الجريمة أو خارجه ، وهنا يجب التأكيد على أنه لا تكفي نسخة إحتياطية في البيانات المراد فحصها ، وإنما يجب عمل نسخة مطابقة تماما لكامل القرص الصلب وعلى مستوى **البت** (BIT) وهي أصغر وحدة لقياس كم البيانات الرقمية ، وهذه الطريقة تعرف باسم (Bit Stream Back-UP) ، بل إنه من الأفضل عمل نسخة إحتياطية ثانية من النسخة الإحتياطية الأولى وعلى مستوى **البت** أيضا ومن ثم إجراء الفحوصات الجنائية على النسخة الثانية ، بحيث تظل النسخة الأولى دون أن تطالها أية تعديلات.

ثالثا: الإستعانة بالذكاء الإصطناعي.

أثبتت تقنيات الحاسبة الإلكترونية نجاحها في جمع الأدلة الجنائية وتحليلها واستنتاج الحقائق منها ، كما يمكن الإستعانة بالذكاء الإصطناعي في حصر الحقائق والإحتمالات والأسباب والفرضيات ومن ثمة استنتاج النتائج على ضوء معاملات حسابية يتم تحليلها بالحاسبة الإلكترونية ، وفق برامج صممت خصيصا لهذا الغرض.

رابعا: مراقبة الإتصالات الإلكترونية.

عرف المشرع الجزائري الإتصالات الإلكترونية بأنها أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية ، الإتصالات الإلكترونية تشمل هنا الإتصالات السلكية أو الخلوية ، البريد الإلكتروني ، مواقع الدردشة على الإنترنت ، وحتى المنتديات المختلفة وساحات الرأي والنقاش التي تسمح بنقل وتبادل الأفكار[1] والمعلومات لذلك سنتطرق إلى مفهوم مراقبة الإتصالات الإلكترونية.

ولم يعرف المشرع الجزائري على غرار العديد من المشرعين عملية مراقبة الإتصالات الإلكترونية ، على عكس بعض التشريعات التي عرفتها مثل التشريع الأمريكي والكندي[2].

وقد وضع الفقه العديد من التعريفات لمراقبة الإتصالات الإلكترونية منها " أنها تعمد الإتصالات والتسجيل ومحلها المحادثات الخاصة سواء أكانت مباشرة أو غير مباشرة أي سواء كانت مما يتبادله الناس في مواجهة بعضهم البعض أو عن طريق وسائل الإتصال السلكية واللاسلكية[3] ".

الفرع الثاني: الوسائل المادية.

هي الأدوات الفنية التي غالبا ما تستخدم في بنية نظم المعلومات والتي يمكن باستخدامها تنفيذ إجراءات وأساليب التحقيق المختلفة والتي تثبت وقوع الجريمة وتساعد على تحديد شخصية مرتكبها ومن أهمها:

[1] - أنظر المادة 02 من القانون رقم 09-04 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي. القانون السابق.

[2] - فقد عرف المشرع الأمريكي مراقبة الإتصالات الإلكترونية بأنها: عملية الإستماع لمحتويات أسلاك أو أي إتصالات شفوية عن طريق إستخدام جهاز إلكتروني أو جهاز آخر ، المادة 2510 الفقرة الرابعة من قانون الإتصلات الفدرالي الأمريكي لسنة 1968 ، وطبقا لقانون الإتصالات الإلكترونية لسنة 1986 أصبح التعريف المذكور يتسع ليشمل الإتصالات الإلكترونية الأخرى.

[3] - أحمد مسعود مريم ، المرجع السابق ، ص79.

أولا: عناوين IP، والبريد الإلكتروني، وبرامج المحادثة.

عنوان الإنترنت هو المسئول عن تراسل حزم البيانات عبر شبكة الإنترنت وتوجيهها إلى أهدافها ، وهو يشبه إلى حد كبير عنوان البريد العادي ، حيث يتيح للموجهات والشبكات المعنية نقل الرسالة ، وهو يوجد بكل جهاز مرتبط بالإنترنت ، ويتكون من أربعة أجزاء ، كل جزء يتكون من أربع خانات ، فيكوّن إثنا عشر خانة كحد أقصى ، حيث يشير الجزء الأول من اليسار إلى المنطقة الجغرافية ، والجزء الثاني لمزود الخدمة ، والثالث لمجموعة الحاسبات الآلية المرتبطة ، والرابع يحدد جهاز الحاسبة الإلكترونية الذي تم الإتصال منه.

وفي حالة وجود أي مشكلة أو أية أعمال تخريبية فإن أول ما يجب أن يقوم به المحقق هو البحث عن رقم الجهاز و تحديد موقعه لمعرفة الجاني الذي قام بتلك الأعمال غير القانونية ، ويمكن لمزود خدمة الإنترنت أن يراقب المشترك ، كما يمكن للشبكة التي تقدم خدمة الإتصال الهاتفي أن تراقبه أيضا إذا ما توافرت لديها أجهزة وبرامج خاصة بذلك.

هذا وتوجد أكثر من طريقة يمكن من خلالها معرفة هذا العنوان الخاص بجهاز الحاسبة الإلكترونية في حالة الإتصال المباشر ، منها على سبيل المثال ما يستخدم في حالة العمل على نظام تشغيل (WINDOWS) حيث يتم كتابة (WINPCFG) في أمر التشغيل ليظهر مربع حوار يبين فيه عنوان (IP) ، مع ملاحظة أن عنوان الإنترنت قد يتغير مع كل اتصال بشبكة الإنترنت.

أما في حالة إستخدام أحد البرامج التحادثية كأداة للجريمة فإنه يتطلب تحديد هوية المتصل، كما تحدد رسالة البريد الإلكتروني عنوان شخصية مرسلها حتى ولو لم يدون معلوماته في خانة المرسل شريطة أن تكون تلك المعلومات التي وضعت في مرحلة إعدادات البريد الإلكتروني معلومات صحيحة.

ثانيا: البروكسي(proxy).

يعمل البروكسي كوسيط بين الشبكة ومستخدميها بحيث تضمن الشركات الكبرى المقدمة لخدمة الإتصال بالشبكات قدرتها لإدارة الشبكة ، وضمان الأمن وتوفير خدمات الذاكرة الجاهزة (CasheMemory) ، وتقوم فكرة البروكسي على تلقي مزود البروكسي طلبا من المستخدم للبحث عن صفحة ما ضمن ذاكرة (Cashe) المحلية المتوفرة فيتحقق البروكسي فيما إذا كانت هذه الصفحة قد جرى تنزيلها من قبل فيقوم بإعادة إرسالها إلى المستخدم دون الحاجة إلى إرسال الطلب إلى الشبكة

العالمية ، أم أنه تم تنزيلها من قبل فيتم إرسال الطلب إلى الشبكة العالمية ، وفي هذه الأخيرة يعمل البروكسي كمزود زبون ويستخدم أحد العناوين (IP) ، ومن أهم مزايا مزود البروكسي أن ذاكرة (Cashe) المتوفرة لديه يمكن أن تحتفظ بتلك العمليات التي تمت عليها مما يجعل دوره قوي في الإثبات عن طريق فحص تلك العمليات المحفوظة بها والتي تخص المتهم والموجودة عند مزود الخدمة.

ثالثا: برامج التتبع.

تقوم هذه البرامج بالتعرف على محاولات الإختراق التي تتم مع تقديم بيان شامل بها إلى المستخدم الذي تم اختراق جهازه ، ويحتوي هذا البيان على إسم الحدث وتاريخ حدوثه وعنوان (IP) الذي تمت من خلاله عملية الإختراق ، واسم الشركة المزودة لخدمة الإنترنت المستضيفة للمخترق ، وأرقام مداخلها ومخارجها على شبكة الإنترنت ومعلومات أخرى ، ومن الأمثلة على هذه البرامج برنامج (Hack Tracer vl,2) وهو يتكون من شاشة رئيسية تقدم للمستخدم بيان شامل بعمليات الإختراق التي تعرض لها جهازه ، يحتوي على اسم وتاريخ الواقعة وعنوان (IP) الذي تمت من خلاله عملية الإختراق ، واسم الدولة التي تمت منها محاولة الإختراق واسم الشركة المزودة لخدمة الإنترنت المستضيفة للمخترق بما فيها أرقام هواتفها والفاكسات الخاصة بها وآخر تحديث قامت به في أجهزة الخدمة الخاصة بها ، وغيرها من المعلومات.

رابعا: نظام كشف الإختراق (Intrusion Détection System).

ويرمز له اختصارا بالأحرف (IDS) وهذه الفئة من البرنامج تتولى مراقبة بعض العمليات التي يجري حدوثها على أجهزة الحاسبة الإلكترونية أو الشبكة مع تحليلها بحثا عن أية إشارة قد تدل على وجود مشكلة قد تهدد أمن الحاسبة الإلكترونية أو الشبكة.

ويتم ذلك من خلال تحليل رموز البيانات أثناء انتقالها عبر الشبكة ومراقبة بعض ملفات نظام التشغيل الخاص بتسجيل الأحداث فور وقوعها في جهاز الحاسبة الالكترونية أو الشبكة ، ومقارنة نتائج التحليل بمجموعة من الصفات المشتركة للإعتداءات على الأنظمة الحاسوبية والتي يطلق عليها أهل الإختصاص مصطلح التوقيع ، وفي حال إكتشف النظام وجود أحد هذه التواقيع يقوم بإنذار مدير النظام بشكل فوري وبطرق عدة ويسجل البيانات الخاصة بهذا الإعتداء في سجلات حاسوبية خاصة ،

والتي يمكن أن تقدم معلومات قيمة لفريق التحقيق تساعدهم على معرفة طريقة إرتكاب الجريمة وأسلوبها وربما مصدرها.

خامسا: نظام جرة العسل Honey Pot.

هو نظام حاسوبي مصمم خصيصا لكي يتعرض لأنواع مختلفة من الهجمات عبر الشبكة دون أن يكون عليه أية بيانات ذات أهمية ويعتمد على خداع من يقوم بالهجوم وإعطائه انطباعا خاطئا بسهولة الإعتداء على هذا النظام بهدف إغرائه بمهاجمته ليتم منعه من الإعتداء على أي جهاز آخر في الشبكة ، في الوقت الذي يتم فيه جمع أكبر قدر ممكن المعلومات عن الأساليب التي يتبعها المهاجم في محاولة الإعتداء وتحليلها وبالتالي اتخاذ إجراء وقائي فعال ، وهذه المعلومات التي تم جمعها تفيد في تحليل أبعاد الجريمة في حال وقوعها وتعطي فريق التحقيق العديد من البيانات التي توضح معالم الجريمة.

سادسا: أدوات تدقيق ومراجعة العمليات الحاسوبية.

هي أدوات خاصة تقوم بمراقبة العمليات المختلفة التي تجري على ملفات ونظام تشغيل حاسبة إلكترونية معينة وتسجيلها في ملفات خاصة يطلق عليها (logs) والكثير من هذه الأدوات تأتي مضمنة في أنظمة التشغيل المختلفة وبعضها يأتي كبرامج مستقلة يتم تركيبها على أنظمة التشغيل بعد إعدادها للعمل ، وكل ما يحتاجه الأمر هو قيام مدير الشبكة أو النظام بتفعيلها وإعدادها للعمل في وقت مبكر وسابق لارتكاب الجريمة حتى يمكن أن تقوم بتسجيل المعلومات التي قد يكون لها علاقة بالحادثة وربما ساعدت في كشف أسلوب الجريمة وشخصية مرتكبها.

سابعا: أدوات الضبط.

هي أدوات تعتبر من الوسائل المادية التي تساعد في ضبط الجريمة المعلوماتية ، منها على سبيل المثال برامج الحماية وأدوات المراجعة ، وأدوات مراقبة المستخدمين للشبكة ، وبرامج التنصت على الشبكة ، والتقارير التي تنتجها نظم أمن البيانات ، ومراجعة قاعدة البيانات ، وبرامج النسخ الإحتياطي التي تستخدم لعمل نسخ مطابقة تماما للأقراص الصلبة الموجودة في الحاسبات الإلكترونية محل التحقيق ، وبغرض عمل الفحوصات الجنائية عليها دون تعريض الأقراص الأصلية لأي تغيير في البيانات الموجودة.

ثامنا: الوسائل المساعدة للتحقيق.

من هذه الوسائل الأدوات المستخدمة في استرجاع المعلومات من الأقراص التالفة ، وبرامج كسر كلمات المرور وبرامج الضغط وفك الضغط ، وبرامج البحث عن الملفات العادية المخفية وبرامج تشغيل الحاسبة وبرامج نسخ البيانات ، أيضا من الأدوات المهمة التي تساعد في عملية التحقيق برامج منع الكتابة وذلك بعد ارتكاب الجريمة مما يساعد في المحافظة على مسرح الجريمة ، وهناك البرامج التي تساعد على استرجاع الملفات والمعلومات التي قد يلجأ الجاني إلى حذفها نهائيا من الحاسبة الإلكترونية.

وهناك أيضا برمجيات تحرير الملفات الستة عشر وهي برامج تمكن المحقق من الإطلاع على محتوى كل ملف حاسوبي بشكله الثنائي متيحة له المزيد من القدرة على تحليل الملف والتعرف على طبيعة البيانات التي يحتويها ، خاصة وأن بعض الأنظمة قد لا تستطيع تحديد أية فئة من الملفات التي ينتمي إليها هذا الملف ، وقد يتطلب الأمر إستخدام هذا النوع من برامج التحرير التي تعتمد على أن الكثير من الملفات تحتوي على مجموعة من الرموز ذات الدلالة تتواجد في بداية الملف ، ويستطيع الخبير الحاسوبي من خلالها تحديد نوع الملف بدقة ، كذلك توجد برمجيات إستعراض الصور والتي تستخدم في عرض الصور الرقمية على شاشة الجهاز وبالتالي فهي تقدم خدمة جديدة للمحقق من خلال تمكينه من مشاهدة واستعراض الصور الرقمية المخزنة داخل أجهزة الحاسبة الإلكترونية أو وسائط التخزين الخارجية حيث تبرز الحاجة لهذه البرمجيات في الجرائم الإباحية ونشر مواد ذات طابع إباحي.

تاسعا: أدوات فحص ومراقبة الشبكات.

هذه الأدوات تستخدم في فحص بروتوكول وذلك لمعرفة ما قد يصيب الشبكة من مشاكل ، ومعرفة العمليات التي تتعرض لها ومن هذه الأدوات:

1 ـ أدوات (ARP) وظيفتها تحديد مكان الحاسبة الإلكترونية فيزيائيا على الشبكة.

2 ـ برنامج (Visual Route S.2a): هو عبارة عن برنامج يلتقط أي عملية فحص عملت ضد الشبكة ، فيقوم بتقديم أجوبة تبين المعلومات التي حدث فيها مسح ، والمناطق التي مر فيها الهجوم ،

وبعد معرفة عنوان (IP) أو إسم الجهة يرسم البرنامج خط يوضح من خلاله مسار الهجوم بين مصدره والجهة التي استهدفها الهجوم.

3 ـ أداة (TRACER): تقوم هذه الأداة برسم مسار بين جهازين تظهر فيه كل التفاصيل عن مسار الرزم والعناوين التي زارها الجاني وتوجه من خلالها والوقت والفترات التي قضاها ، وهي تسمح برؤية المسار الذي اتخذه (IP) من مضيف إلى آخر وتستخدم هذه الأدوات (TTl) Time To live التي

تكون ضمن (IP) لكي تستقبل من كل موجه رسالة وبذلك يكون هو العدد الحقيقي للوثبات ، ويتم بذلك تحديد وبشكل دقيق المسار الذي تسلكه الرزمة ، وهذه الأدوات تستخدم في الأساس للمسح الميداني للشبكات المراد التخطيط للهجوم عليها ، إذ أنه يبين الشبكة وتخطيطها والجدران النارية المستخدمة ونظام الترشيد ، ونقاط الضعف ، ولكن يمكن أيضا من خلالها معرفة مكان الخلل والمشاكل التي تعرضت لها الشبكة والإختراقات التي وقعت عليها.

4 ـ (Net Stat): هي أدوات لفحص حالة الإتصال الحالي للبروتوكول ، ولها عدد من المهام من أهمها عرض جميع الإتصالات الحالة ، ومنافذ التنصت ، وعرض المنافذ والعناوين بصورة رقمية ، عرض كامل لجدول التوجيه.

ـ صعوبات ومعوقات جمع الأدلة.

الجريمة الماسة بالمعطيات الرقمية مثلها مثل أنواع الجرائم الأخرى ، تمر بذات مرحلتي الإستدلال والتحقيق الجنائي المتكامل وما يترتب على ذلك من إجراءات قانونية فنية وشكلية ، وإجراءات التحقيق الجنائي العام هي الأساس في التحقيق في جرائم الحاسب الآلي وذلك من سماع للشهود ومعاينة وقبض وتفتيش واستجواب ، لكن إجراءات التحقيق الأخرى الفنية والنفسية يتوقف استخدامها على ظروف كل جريمة على حدة مع مراعات الخصوصية التي تتسم بها الجريمة الماسة بالمعطيات الرقمية ، وهناك صعوبات كثيرة فيما يتعلق بعمل سلطات الإستدلال والتحقيق منها[1]:

أولا: المعوقات المتعلقة بالجريمة.

ـ خفاء الجريمة وغياب الدليل المرئي الممكن للقراءة فهمه.

[1] ـ خيرت علي محرز ، المرجع السابق ، ص67.

ـ صعوبة الوصول إلى الدليل لإحاطته بوسائل الحماية الفنية كاستخدام كلمات السر حول مواقعهم تمنع الوصول إليها أو ترميزها أو تشفيرها لإعاقة المحاولات الرامية للوصول إليها والإطلاع عليها أو استنساخها[1].

ـ سهولة محو الدليل أو تدميره في زمن قصير جدا فالجاني يمكنه محو الأدلة التي تكون قائمة ضده أو تدميرها في زمن قصير جدا ، بحيث لا تتمكن السلطات من كشف الجريمة إذا ما علمت بها ، وفي هذه الحالة التي قد تعلم بها فإنه يستهدف بالمحو السريع عدم إستطاعة هذه السلطات إقامة الدليل ضده ، وبالتالي تنصله من مسئولية هذا الفعل وإرجاعه إلى خطأ في نظام الحاسبة الإلكترونية أو الشبكة أو في الأجهزة ، ومن الأمثلة على ذلك قيام أحد مهربي الأسلحة في النمسا بإدخال تعديلات على الأوامر العادية لنظام تشغيل جهاز الحاسبة الإلكترونية الذي يستخدمه في تخزين عناوين عملائه والمتعاملين معه بحيث يترتب على إدخال أمر النسخ أو الطباعة إلى هذه الحاسبة من خلال لوحة مفاتيحه محو وتدمير كافة البيانات كاملة.

ـ الضخامة البالغة لكم المعلومات والبيانات المتعين فحصها ، وإمكانية خروجها عن نطاق إقليم الدولة ، والبعد الجغرافي بين مرتكبي الجريمة والضحية ، بالإضافة إلى عدم المعرفة بمكونات الجريمة المتعلقة بالإنترنت من قبل بعض الأطراف المعنية[2].

ـ عدم المعرفة بمكونات الجريمة المتعلقة بشبكة الإنترنت من قبل بعض الأطراف المعنية.

ثانيا: المعوقات المتعلقة بالجهات المتضررة.

- الإحجام عن الإبلاغ: تظل الجريمة الجريمة الماسة بالمعطيات الرقمية مستمرة ما لم يتم الإبلاغ عنها ، ومن ثمة عمل الإستدلالات أو تحريك الدعوى العمومية حسب القانون السائد ، والصعوبة التي تواجه أجهزة الأمن والمحققين ، هي أن هذه الجرائم لاتصل إلى علم السلطات المعنية بالصورة العادية ـ كما هو الحال في الجرائم التقليدية ـ وذلك لصعوبة إكتشافها من قبل الأشخاص العاديين أو حتى الشركات والمؤسسات التي وقعت مجنيا عليها في هذه الجرائم ، أو لأن هذه الجهات تحاول درء الأثر السلبي للإبلاغ عما وقع لها وحرصا على ثقة العملاء فلا تبلغ عن تلك الجرائم التي ارتكبت ضدها

[1] ـ علي عدنان الفيل ، المرجع السابق، ص 80

[2] ـ علي عدنان الفيل ، المرجع نفسه، ص 81.

وتدخل هذه المؤسسات في اعتباراتها أن الإبلاغ عن الجرائم الماسة بالمعطيات الرقمية التي وقعت ضدها ربما يؤدي إلى إحاطة المجرمين علما بنقاط الضعف في أنظمة الجهات المجني عليها ، لاسيما البنوك الكبرى.

ولذلك يكون من الملائم لدى سلطات الأمن في الجرائم الماسة بالمعطيات واكتشافها أن ترصد ميدانيا حركة المعاملات التجارية داخل المؤسسات المالية وحولها ، وذلك عن طريق جمع المعلومات السرية عن حركة السوق وتداول الأموال والممتلكات والتغيرات الإجتماعية والسلوكية للموظفين وصغار رجال الأعمال الذين يرتبطون بمؤسسات الجريمة المنظمة ، سيما وأن جرائم الحاسب الآلي هي من أدوات وأسلحة هذه الجريمة حيث يجري استقطاب صغار الموظفين وذوي القدرات الفنية والذين هم على مقربة من أسرار برامج الحاسب الآلي للمؤسسات المالية والشركات التجارية ، ويرتبط ذلك بضرورة تطوير ثقافة الحاسب الآلي في وسط رجال الأمن وربط تلك الثقافة بالثقافة الأمنية في صورها التقليدية ، وهو ما يضمن نجاحا للأجهزة الأمنية في مواكبة ظاهرة جرائم الحاسب الآلي[1].

والجريمة في صورتها التقليدية تصل إلى علم سلطات الضبط عن طريق الشكوى أو الإبلاغ والتي يجب على ضابط الشرطة القضائية أن يقيدها متى وردت في شأن جريمة ويحرر بها محضر يرسله فورا إلى النيابة العامة ، حتى يتسنى للنيابة العامة مراقبة مشروعية أعمال الإستدلال ، والشكوى كالبلاغ إلا أنها توجه ضد شخص معين ، وتقدم من المجني عليه أو المضرور من الجريمة ، بينما البلاغ يقدم من غيرهما أو يخلو من تعيين إسم من تنسب إليه الجريمة.

وفيما يتعلق بالإبلاغ عن الجرائم الماسة بالمعطيات الرقمية فإن الواقع أن البعض يحجم عن إبلاغ السلطات المختصة عن الجرائم المرتكبة في حقهم ، خاصة المؤسسات والشركات التجارية حتى في الدول المتقدمة من الناحية التقنية والتي ترتفع فيها معدلات هذا النوع من الجرائم ، ففي دراسة للمعهد الوطني للعدالة التابع لوزارة العدل الأمريكية شملت (127) من العاملين في مجال التحقيق في جرائم الحاسبة الإلكترونية والإنترنت يمثلون (11) وكالة رسمية ، كان غالبية المشاركين في الدراسة يعتقدون أن معظم جرائم الحاسبة الإلكترونية والإنترنت التي يتم اكتشافها لا يبلغ عنها للشرطة ، كما توصلت دراسة أخرى أجراها معهد أمن الحاسبة الإلكترونية بالإشتراك مع مكتب التحقيق الفدرالي في الولايات

[1] - خيرت علي محرز، المرجع السابق، ص69.

المتحدة الأمريكية إلى أن حوالي 70% من الجرائم التي يتم اكتشافها لا يتم الإبلاغ عنها للسلطات المعنية ، ويمكن أن يكون السبب في إحجام البعض عن الإبلاغ لعدة أسباب منها:

1 ـ عدم إدراك الأفراد أو مدراء الأنظمة الحاسوبية ومسئولي الشركات أن مثل هذه الأفعال و الهجمات تعتبر جرائم يمكن معاقبة مرتكبيها بموجب التشريعات والأنظمة المطبقة ضمن إقليم الدولة المطبقة دوليا.

2 ـ خوف الجهات التي وقعت عليها الجرائم ، خاصة المؤسسات والشركات المالية من أن يؤثر انتشار خبر الحادث على سمعتها ومصداقيتها وظهورها بمظهر مشين أمام الآخرين لأن تلك الجرائم أرتكبت ضدها مما قد يترك إنطباعا بإهمالها أو قلة خبرتها أو عدم وعيها الأمني ولم تتخذ الإحتياطات الأمنية اللازمة لحماية معلوماتها ، الأمر الذي قد ينعكس سلبا على أرباحها وقيمة أسهمها.

3 ـ خوف المؤسسات والشركات التجارية من أن تؤدي أعمال التحقيق إلى احتجاز حاسباتها أو تعطيل شبكاتها فترة طويلة ، مما قد يتسبب في زيادة خسائرها المالية جراء التحقيق ، عطفا على ما قد تسببه الجريمة في خسارتها أصلا.

4 ـ بعض الضحايا قد تساوره الشكوك حول مقدرة رجال إنفاذ القانون على التعامل مع هذا النوع المستحدث من الجرائم.

5 ـ الرغبة في إخفاء الأسلوب الذي ارتكبت به الجريمة لكي لا يتم تقليده من الآخرين مستقبلا.

6 ـ قد تكون بعض الجرائم محدودة الأثر ، مما يدفع بعدم الإبلاغ عنها ، فقد يقوم مخترق ما للنظام بإظهار رسالة تفيد بقيامه بهذه العملية ، أو يقوم مجرم آخر بإرسال فيروس حاسبة إلكترونية إلى جهاز المستفيد و يكون هذا الفيروس محدود الأثر ، أو تقوم برامج الحماية من الفيروسات بالقضاء عليه.

7 ـ قد يكون الإفصاح عن التعرض لجريمة معلوماتية من شأنه حرمان شخص من خدمات معينة تتعلق بالنظام المعلوماتي ، وقد يحرم الموظف في الجهة من خدمات معينة على الإنترنت أو قد يحرم

من خدمات الإنترنت عموما حين يتعرض لجريمة معلوماتية ناتجة عن الإختراق أو زيارته لأماكن غير مأمونة أو غير مسموح بزيارتها.

8 ـ عدم معرفة الضحية بوجود جريمة أصلا، وعدم القناعة أنها ممكن أن تحدث في مؤسسته[1].

في حين قد يتم الإبلاغ عن الجرائم الماسة بالمعطيات الرقمية أو تصل أخبارها إلى سلطات الضبط بإحدى الطرق الآتية:

1 ـ تلقي سلطات الضبط أو أجهزة التحقيق معلومات عن أن أشخاصا معروفين أو غير معروفين يمارسون أنشطة تندرج تحت تعريف الجريمة المعلوماتية، وذلك في مكان معروف وعلى أجهزة محددة ووفق لغات برمجية معلومة.

2 ـ ضبط شخص معين و بحوزته أموال مشبوهة أو بطاقات مزورة أو بطاقات تعريف مشبوهة "حالة تلبس".

3 ـ بلاغ إلى سلطات الضبط أو التحقيق من أحد المجني عليهم يفيد بتلاعب أو ممارسات خاطئة في حقه أو حقوق الآخرين سواء تمثل ذلك في صورة عجز مالي في حاسبات مؤسسة مالية أو ضياع حقوق أو تغييرات في الودائع ، وذلك دون بيان ما إن كانت هذه جريمة معلوماتية من عدمه ، لأن عملية تكييف السلوك الإجرامي هي مسالة أخرى لا دخل للمبلغ بها.

4 ـ توافر معلومات عن نشر فيروسات تخريبية عبر شبكة الإنترنت ، سيما و أن تطبيق القانون في مجال مكافحة الفيروسات المعلوماتية ، تواجه عدة صعوبات و موانع كثيرة هي:

ـ عدم معرفة المجني عليه بالمخرب الذي صمم الفيروس الذي هاجمه.
ـ عدم رغبة المجني عليه في الإبلاغ عن وجود فيروس بنظامه المعلوماتي ، حفاظا على الثقة بينه و بين الذين يستخدمون هذا النظام.
ـ عدم دراية المجني عليه بإصابة نظامه بفيروس معلوماتي لفترة غير محدودة من الزمن ، وبالتالي يصعب تحديد وقت الإصابة.
ـ عدم القدرة على قياس الخسائر التي يحدثها هذا الفيروس.

[1] ـ على عدنان الفيل ، المرجع السابق ، ص 84

5 ـ توافر معلومات عن وقوع عمليات إعتراض فضائية للمعلومات ، ذلك أن الظاهرة ـ الإختراقية ـ للمعلومات تتجاوز حدود الجغرافيا ، وقد جعلت شبكة الإنترنت هذا النوع من الجرائم ساحة للمعارك بين الدول ، وصارت الحركة التجارية و التعاملات المصرفية هدفا لهذه الإختراقات الإلكترونية.

ومن أجل تفعيل عملية الإبلاغ عن الجريمة المعلوماتية ، ومن ثم المساهمة بطريقة إيجابية في منع وقوع الجريمة أو سرعة تحصيل الدليل المتعلق بها ، ما طالب البعض به في الولايات المتحدة الأمريكية و ذلك بأن تتضمن القوانين المتعلقة بجرائم الحاسب و المعلومات ، نصوصا تلزم موظفي الجهة المجني عليها ـ أيا كانت ـ بضرورة الإبلاغ عما يصل إلى علمهم من جرائم تتعلق بهذا المجال ، وضرورة وضع تقرير من الخبراء يتضمن أوجه الإخلال بالإلتزامات المفروضة للحفاظ على المعطيات.

إلا أنه ولدى عرض هذا الاقتراح على " لجنة خبراء مجلس أوربا" قوبل بالرفض لسبب قانوني مؤداه أن المجني عليه ـ وهو الشركة التي أرتكبت في حقها جريمة معلوماتية ـ سوف تصبح متهمة أو جانيه بعد أن كانت مجنيا عليها ولذلك وردت إقتراحات بديلة قد تكون مقبولة منها الإلتزام بإبلاغ جهة خاصة ، أو إبلاغ سلطات إشرافية ، و تشكيل أجهزة خاصة لتبادل المعلومات ، و كذلك إصدار شهادة " أمن خاصة " تمنح بعد عمل مراجعة و تدقيق من قبل هيئة خاصة من المراجعين ، و يتعين على هذه الهيئة إبلاغ الشرطة بما تكتشفه من جرائم.

و لذلك فإن من صعوبات الإبلاغ عن هذه الجرائم على النطاق الدولي ، عدم وجود شبكة دولية لتبادل المعلومات الأمنية كما هو الحال في شبكة (يورب بول) التي تعمل حاليا في إطار الشرطة الدولية بمعزل عن الشبكة العامة المستخدمة حاليا كما هو الحال لشبكة إنترنت (2) التي تمثل إتحاد شركات عالمية تعمل بمعزل عما تواجهه شبكة الإنترنت الحالية من مشاكل وثغرات وفي هذا الإطار إستحدثت الصين شرطة متخصصة بملاحقة الإختراقات الإلكترونية حيث أسس أحد الأقاليم الصينية أول وحدة بوليسية متخصصة لمراقبة إستخدام شبكة الإنترنت[1].

- عدم إدراك خطورة الجرائم الماسة بالمعطيات الرقمية من قبل المسؤولين بالمؤسسات تعد إحدى معوقات التحقيق.

[1] ـ خيرت علي محرز، المرجع السابق، ص76.

- إغفال الجانب التوعوي لإرشاد المستخدمين إلى خطورة الجرائم المتعلقة بشبكة الإنترنت.
- تسابق الشركات في تبسيط الإجراءات وتسهيل إستخدام البرامج والأجهزة وملحقاتها، وزيادة

المنتوجات واقتصار تركيزها على تقديم الخدمة وعدم التركيز على الجانب الأمني على سبيل المثال مستخدمي شبكة الإنترنت عبر مزودي الخدمة أو بطاقات الإنترنت المدفوعة ليسوا مطالبين بتحديد هويتهم " عملية ربط رقم المستخدم مع هويته " عند الإشتراك في خدمة الإنترنت أي أن مزود الخدمة لا يعرف هوية مستخدمي الخدمة.

ثالثا: الصعوبات المتعلقة بجهات التحقيق.

من الصعوبات التي تواجه عملية إستخلاص الدليل في الجريمة الماسة بالمعطيات كذلك نقص الخبرة لدى رجل الضبط القضائي أو أجهزة الأمن بصفة عامة ، وكذلك لدى أجهزة العدالة الجنائية متمثلة في سلطات الإتهام والتحقيق الجنائي ، وذلك فيما يتعلق بثقافة الحاسب الآلي والإلمام بعناصر الجرائم المعلوماتية وكيفية التعامل معها وذلك على الأقل في البلدان العربية ، نظرا لأن تجربة الإعتماد على الحاسب الآلي وتقنياته وانتشارها في هذه البلدان جاء متأخرا عن أوروبا وكندا والولايات المتحدة ، وأن أجهزة العدالة المقاومة للجرائم المرتبطة بهذه التقنية تبدأ في التكون والتشكل عقب ظهور الجرائم ، وهو أمر يستغرق وقتا أبطأ من وقت إنشار الجريمة ، لأن الجريمة الماسة بالمعطيات – كما سبق– تتقدم بسرعة هائلة توازي سرعة تقدم التقنية ذاتها ، وحتى الآن فإن الحركة التشريعية أو الثقافة الأمنية أو القانونية بخصوص هذه الجرائم لا تسير بذات المعدل ، وهذا الفارق في التقدم أو التطور ينعكس سلبا على فئة إجراء الإستدلالات والتحقيقات في الدعوى الجنائية عن الجريمة الماسة بالمعطيات الرقمية ، ومن هنا تأتي الدعوة إلى وجوب تأهيل سلطات الأمن وجهات التحقيق والإدعاء والحكم في شأن هذه الجرائم[1].

1 ـ معوقات ترجع إلى شخصية المحقق ، منها عدم الحرص على متابعة المستجدات في مجال الجرائم المعلوماتية بشكل دوري.

[1]- خيرت علي محرز، المرجع السابق، ص81.

2 ـ صعوبات تتعلق بالنواحي الفنية، كنقص المهارة الفنية المطلوبة للتحقيق في هذا النوع من الجرائم ، و نقص المهارة في استخدام الحاسبة الإلكترونية و الإنترنت ، وعدم توفر المعرفة بأساليب إرتكاب جرائم الحاسبة الإلكترونية و الإنترنت و قلة الخبرة في مجال التحقيق في جرائم الحاسبة الإلكترونية و الإنترنت و المعرفة باللغة الإنجليزية.

لاسيما و أن للعاملين في مجال الحاسبة الإلكترونية مصطلحات علمية خاصة ، أصبحت تشكل الطابع المميز لمحادثاتهم و أساليب التفاهم معهم ، و ليس هذا فحسب بل إختصر العاملون في هذا المجال تلك المصطلحات و العبارات بالحروف اللاتينية الأولى لتكون لديهم لغة غريبة تعرف بلغة المختصرات وهي لغة متطورة ومتجددة، ومن أجل ذلك فإنه لابد من إيجاد أسلوب خاص للتحقيق في هذه الجرائم وهو أسلوب يجمع بين الخبرة الفنية و الكفاءة المهنية ومن الممكن حيال ذلك إتباع الخطوات التالية[1]:

1 ـ تبادل المعلومات بين المحقق و خبير الحاسبة الإلكترونية وذلك قبل البدء في التحقيق و أخذ أقوال الشهود و المشتبه فيهم أو استجواب المتهمين ، بحيث يشرح المحقق للخبير أهمية ترتيب المتهمين و الشهود و طريقة توجيه الأسئلة إليهم ، ومن جهة أخرى يقوم الخبير بشرح الأبعاد الفنية و النقاط التي ينبغي استجلابها من الأشخاص ، وكافة المصطلحات الحاسوبية التي يمكن استخدامها مع بيان معاينتها ليتم الإستفادة منها عند الضرورة.

2 ـ يتم حصر النقاط المطلوب استجلابها من قبل الخبير و المحقق قبل البدء في التحقيق ليتولى المحقق بعد ذلك ترتيب تلك النقاط.

3 ـ يتم أخذ أقوال الشهود و استجواب المتهمين من قبل المحقق و بحضور الخبير الذي يجوز له توجيه الأسئلة الفرعية أثناء الإستجواب وفق الكيفية التي يتم الإتفاق عليها مسبقا قبل بدء التحقيق.

4 ـ التنسيق بين المحقق و الخبير في الحصول على البيانات المخزنة في الحاسبة الإلكترونية و ملحقاته الخاصة بالشاهد أو المتهم الذي تم التحقيق معه مع مراعاة أن هذا الأخير لا يجوز إجباره على تقديم دليل يدينه ، و لضمان نجاح التحقيق في الجرائم الماسة بالمعطيات الرقمية فهناك بعض القواعد التي ينبغي مراعاتها أهمها:

[1] ـ خيرت علي محرز، المرجع السابق، ص84

أ ـ تفادي ضياع الوقت في التحقيق حول جرائم لا يمكن إكتشافها أو أن الأدلة اللازمة لاكتشافها و إثبات التهمة ، غير كافية.

ب ـ ضرورة مراعاة وجود نوع من التعامل بين المحققين و خبراء الحاسبة الإلكترونية العاملين في المؤسسة المجني عليها.

ج ـ مراعاة القوانين السارية بشأن الحقوق الفردية و سرية البريد الإلكتروني و غيرها من الحقوق.

د ـ العناية بإصدار الأوامر القضائية الخاصة بالتفتيش و ضبط أجهزة الحاسبة الإلكترونية وملحقاتها و برامجها.

هـ ـ مراعاة حفظ الأدلة الجنائية بالطرق المناسبة كل حالة على حدة ، وذلك حتى يتم تقديمها للمحكمة وهي على حالتها التي ضبطت عليها.

و ـ الإستعانة بالتقنيات المتطورة في المجال المعلوماتي في مواجهة الجرائم المعلوماتية ، سيما و أن هذه التقنيات أثبتت جدارتها و نجاحها في جمع الأدلة الجنائية و صناعة البنية الإتهامية و تحليل القرائن و استنتاج الحقائق[1].

[1] ـ خيرت علي محرز، المرجع السابق، ص86

المبحث الثاني: التفتيش في الجرائم الماسة بالمعطيات الرقمية.

مع بزوغ فجر الثورة المعلوماتية و توسع إستخدام شبكة الإنترنت و بدء إستخدامها في جل المعاملات ودخول جميع فئات المجتمع على قائمة المستخدمين ، بدأت تظهر جرائم على الشبكة ازدادت مع الوقت و تعددت صورها و أشكالها ، أي تلك الأعمال و الأفعال المجرمة التي تتم عن طريق الإنترنت ، ولعل التطور المستمر وتوفر السرية التامة جعلا من الإنترنت جهازا مثاليا للإعتداء على المعطيات الرقمية بعيدا عن أعين الجهات الأمنية ، فقد مكنت شبكة الإنترنت مافيا الجرائم الإلكترونية من نقل المعلومات و البيانات الخطرة و المحظورة[1] .

إن للجرائم الماسة بالمعطيات الرقمية طبيعة خاصة ، إذ أن أدلتها غير محسوسة أو تحتاج إلى خبرات فنية و تقنية عالية و عليه قسمنا هذا المطلب إلى فرعين تناولنا في الفرع الأول: التحقيق في الجرائم الماسة بالمعطيات الرقمية ، وفي الفرع الثاني: الإثبات في الجرائم الماسة بالمعطيات الرقمية[2].

يعتبر التفتيش من أخطر الحقوق التي منحت للمحقق و ذلك لمساسه بالحريات التي تكفلها الدساتير عادة ، ولذا نجد المشرع يضع لها ضوابط عديدة سواء فيما يتعلق بالسلطة التي تباشره أو تأذن بمباشرته و الأحوال التي تجوز فيها مباشرته و شروط إتخاذ هذا الإجراء بما يمثل ضمانات الحرية الفردية أو حرمة المسكن.

إن الأنظمة الجنائية عرفت في مرحلة تطورها أنواعا من الإجراءات تنطوي على انتهاك لحقوق الفرد الأولية في سبيل تتبع الجناة و محاكمهم ومنها القبض و التفتيش فإذا ما تخلت يد العدالة عن التعرض لحقوق الأفراد لأصبحنا إزاء فوضى إجرامية ، ومن ثم يجب أن يتاح للقائمين على تنفيذ القانون نوع من السلطة في إنكار الحريات الشخصية بالقدر الذي يحول دون تسليط الإجرام على مقدرات الناس و إنما لا ينبغي أن يتجاوز هذا القدر ، إذ لا فارق بين أن تنتهك حريات الأفراد بمعرفة أشخاص يعملون تحت ستار القانون أو بمعرفة مجرمين يرتكبون آثامهم بمنأى عن سطوة القانون ومن هذه الإجراءات التفتيش[3].

[1] ـ خالد ممدوح إبراهيم ، الجرائم المعلوماتية، ص05

[2] ـ علي عدنان الفيل ، المرجع السابق ، ص11.

[3] ـ خالد ممدوح إبراهيم ، المرجع نفسه ،ص 180.

لذلك قسمنا هذا المبحث إلى مطلبين تناولنا في المطلب الأول: شروط التفتيش في الجرائم الماسة بالمعطيات الرقمية و في المطلب الثاني: إجراءات التفتيش في الجرائم الماسة بالمعطيات الرقمية.

المطلب الأول: شروط التفتيش في الجرائم الماسة بالمعطيات الرقمية.

لم تتضمن التشريعات العربية تعريفا للتفتيش و اكتفت بالنص على أنه من إجراءات التحقيق ، ورغم ذلك فقد أورد الفقه عدة تعريفات للتفتيش كإجراء للتحقيق[1] ومن بين هذه التعريفات : عرف التفتيش بأنه إجراء تقوم به السلطة القضائية للإطلاع على محل يتمتع بحرمة خاصة للبحث عن الأدلة اللازمة للتحقيق الجنائي[2]، أيضا عرف على أنه إجراء من إجراءات التحقيق التي تهدف إلى البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة المسكن أو الشخص ، وذلك بهدف إثبات إرتكابها أو نسبتها إلى المتهم وفقا لإجراءات قانونية محددة[3].

إن التعاريف السالفة الذكر ومثلها تعاريف أخرى تتفق مع طبيعة المحل في الجرائم الماسة بالمعطيات الرقمية ، وهي البيانات أو المعلومات إذا اتفقت تلك التعاريف على اعتبار التفتيش إجراءا قضائيا بموجبه يتم الإطلاع على مكان له حرمة خاصة و الهدف من التفتيش هو الحصول عل الأدلة.

ومن خلال ما تقدم من تعاريف مختلفة للتفتيش نستنتج أن التفتيش إجراء قضائي يهدف إلى الحصول على أدلة تساعد في كشف الحقيقة ، كما أن هذا الإجراء يتميز بعدة خصائص و هي الجبر و الإكراه أي أن الإنسان يخضع له جبرا هذا إذا لم يوافق على إجراء التفتيش برضائه ، و كذلك يتضمن هذا الإجراء مساسا بممتلكات الإنسان بما فيها الحاسب الآلي هذا من جهة ومن جهة أخرى يهدف هذا الإجراء إلى جمع الأدلة التي تساهم في كشف الحقيقة ومن هنا يطرح السؤال نفسه حول مدى جوازية إجبار المتهم من قبل القائم بالتفتيش على تقديم الرقم السري الخاص بالدخول إلى جهاز الحاسوب المراد تفتيشه؟ وفي هذا الصدد هناك اتجاهات:

ـ الإتجاه الأول: يرى أن مالك الحاسوب أو مستعمله ملزم بتزويد القائم بالتفتيش بالكود السري أو كراك الدخول إلى الحاسوب ، و يقاس ذلك على أساس إعتبار مفتاح الدخول إلى الحاسوب كمفتاح باب البيت تماما ، فإذا امتنع صاحب الحاسوب عن الإدلاء بكلمة السر أو كلمة المرور إلى الحاسوب

[1] ـ علي حسن محمد الطولية ، على نظم الحاسوب و الانترنت ، دراسة مقارنة ، عالم الكتاب الحديث ، الأردن ، 2004، ص10

[2] ـ سامي جلال فقي ، التفتيش في الجرائم المعلوماتية ،دراسة تحليلية ، دار الكتب القانونية ، مصر ، 2011،ص51.

[3] ـ على عدنان الفيل ، إجراءات التحري وجمع الأدلة و التحقيق الإبتدائي في الجريمة المعلوماتية دراسة مقارنة ، المكتب الجامعي الحديث، 2011،ص38 ، أنظر هبة هروال ، المرجع السابق، ص232.

أمكن إجباره من قبل القائم بالتفتيش ، حيث إنتقد البعض هذا الرأي على أنه غير منطقي و غير مقبول إذ لا يمكن قياس كلمة السر الخاصة بدخول الحاسوب على مفتاح الدخول إلى البيت لأن هناك فرقا شاسعا بينهما ، لأنه إذا امتنع المتهم أو صاحب المكان عن تقديم مفتاح الباب للدخول و إجراء عملية التفتيش أمكن للقائم بالتفتيش إستخدام القوة للدخول عن طريق كسر الباب ، ولكن إذ إمتنع المتهم أو حائز الحاسوب عن تقديم رمز الدخول إلى الحاسوب كان إجباره على تقديم هذا الرمز غير ممكن من قبل القائم بالتحقيق لأن الرمز محفوظ في ذاكرته و لا يمكن الحصول عليه إلا إذا قدمه طواعية.

الاتجاه الثاني: و هذا الإتجاه هو عكس الإتجاه الأول إذ يرى أنه لا يجوز إجبار المتهم على تقديم دليل إدانته أو أن يدلي بأية معلومات قد تؤدي إلى إدانته فللمتهم حق الصمت و الإمتناع عن الإجابة عن الأسئلة التي توجه إليه ومن ضمن الأسئلة سؤاله عن رمز الدخول إلى جهاز الحاسوب محل التفتيش فالصمت هو أحد مظاهر حرية المتهم في الدفاع عن نفسه حتى لو كان سلبي عن طريق الإمتناع عن الإجابة على الأسئلة الموجهة إليه[1].

و لما كان التفتيش من الإجراءات الخطيرة التي تمس الحرية الشخصية و تنتهك حرمة الأشخاص و راحتهم و هدوئهم كان لا بد من أن يتم وضع قيود و ضوابط لتنظيم التفتيش لكي يكون هذا الإنتهاك لحرية الإنسان قانونيا و وفقا ضوابط محددة ، و لضمان عدم التجاوز على حرية الأشخاص إلا وفقا لما هو ضروري لمصلحة التحقيق إذ أن التفتيش إجراء من إجراءات التحقيق يمثل تغليبا لمصلحة المجتمع على مصلحة الأفراد إلا أن تغليب مصلحة المجتمع لا يعني التعسف في انتهاك حرية الأشخاص و انتهاك أسرارهم ، وعلى هذا الأساس وضع المشرع قيودا أو ضوابط تضمن عدم التجاوز على حرية الأشخاص و حرية ممتلكاتهم إلا في إطار حاجة التحقيق ، ومن الشروط و الضمانات التي يجب توافرها لإجراء التفتيش ما هو موضوعي و منها ما هو شكلي لذلك سنتطرق في الفرع الأول : للشروط الشكلية ، وفي الفرع الثاني: للشروط الموضوعية.

---

[1] ـ سامي جلال فقي ،المرجع السابق، ص64،65.

ولقد نصت أغلب التشريعات حق المتهم في الصمت و قد أشار إلى ذلك التعديل الخامس للدستور الأمريكي على أنه (لا يجوز إكراه أي شخص في أية دعوى جنائية على أن يكون شاهدا ضد نفسه ....) كما نصت المادة 01/274 من قانون الإجراءات الجنائية المصري رقم 150 لسنة 1950 على أنه (لا يجوز استجواب المتهم إلا إذا قبل) كذلك الشأن نص قانون الإجراءات الجزائية الجزائري على أنه (يتحقق القاضي حين مثول المتهم لديه لأول مرة من هويته و يحيطه علما بكل واقعة من الوقائع المنسوبة إليه و ينوه بأنه حر في عدم الإدلاء بأي قرار و ينوه في ذلك التنبيه في المحضر...) و كذلك المشرع الإجرائي الفرنسي في المادة 1145/ 01 (... قاضي التحقيق بضرورة تنبيه المتهم عند حضوره لأول مرة أمامه إلي أنه حر في عدم الإدلاء بأي قرار و يثبت ذلك التنبيه في محضر التحقيق).

الفرع الأول: الشروط الشكلية.

المقصود بالشروط الشكلية تلك الإجراءات التي أوجب المشرع مراعاتها عند إجراء عملية التفتيش و الهدف من وضع هذه الشروط من قبل المشرع هو إحاطة عملية التفتيش بإجراءات و شكليات تضمن صحة ودقة النتائج التي يصل إليها القائم بالتفتيش و إحاطة المتهم بضمانات كافية للحفاظ على حريته الفردية فالشكلية في الإجراءات الجنائية هي ضمانة لعدم تعسف الجهات القائمة بالتفتيش لذلك سنتطرق إلى القواعد الشكلية لإجراء التفتيش:

1 ـ وقت إجراء التفتيش:

يعد الميقات الزمني لإجراء التفتيش من الأمور المهمة جدا و التي تساعد في الحصول على الدليل المعلوماتي في الجرائم الماسة بالمعطيات الرقمية من عدمه ، وذلك لأنه من السهل جدا إتلاف الدليل المعلوماتي ومحوه من قبل المتهم قبل وصول سلطات التحقيق المتخصصة إليه ، لذلك كلما كان إجراء التفتيش في وقت قريب من ارتكاب الجريمة كانت فرصة الحصول على الأدلة أكبر ، وفي هذا الإطار إختلفت التشريعات الإجرائية في تنظيمها لوقت إجراء التفتيش ، و ذلك حرصا على تضييق نطاق الإعتداء على الحرية الفردية و حرمة المساكن في حين تترك تشريعات أخرى تحديد ذلك الوقت للقائم بالتفتيش[1] ، كما هو الحال بالنسبة لقانون الإجراءات الجنائية المصري ، و الذي لم يحدد وقتا معينا يتم فيه ذلك الإجراء ، و إنما تركه لسلطة القائم به أي أن التفتيش يجوز في كل الأوقات سواء ليلا أو نهارا بغض النظر عن الإعتبارات المتعلقة بالمحل المراد تفتيشه ، بينما في القانون الجزائري و الفرنسي يحظر كلاهما القيام بتفتيش المنازل و ما في حكمها في وقت معين ، فالمشرع الجزائري حدد الوقت من الساعة الخامسة صباحا إلى الساعة الثامنة مساءا و قد نص على ذلك " لا يجوز البدء في تفتيش المساكن أو معاينتها قبل الساعة الخامسة صباحا و لا بعد الساعة الثامنة مساء...."[2]. أما المشرع الفرنسي فيحدده من الساعة السادسة صباحا إلى الساعة التاسعة مساءا و قد نص على ذلك في المادة 59 من قانون الإجراءات الجنائية بأنه لا يجوز البدء في تفتيش و دخول المساكن قبل الساعة السادسة و بعد الساعة التاسعة.

[1] ـ هلالي عبد اللاه أحمد، المرجع السابق، ص75.
[2] ـ أنظر المادة 47 من قانون الإجراءات الجزائية الجزائري، القانون السابق.

إلا أنه و في حالات إستثنائية يجوز الخروج عن تلك القاعدة فعندما يتعلق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و جرائم الأموال و الإرهاب و كذلك الجرائم المتعلقة بالتشريع الخاص بالصرف فإنه يجوز إجراء التفتيش و المعاينة و الحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل و ذلك بناء على إذن مسبق من وكيل الجمهورية المختص[1].

و يتبين من النص أعلاه أن المشرع الجزائري أجاز إجراء التفتيش في أي وقت من أوقات النهار و الليل في جرائم معينة ، ومن بين هذه الجرائم الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات.

ومن خلال ما تقدم يمكن القول أنه نظرا لما تتميز به الجرائم الماسة بالمعطيات الرقمية من خصوصية مميزة من حيث أنها ذات صفة عالمية ، ويمكن ارتكابها في أي وقت و أن أدلة الإدانة فيها سهلة المحو و التدمير و أنها مرئية ، كان حظر القيام بإجراء التفتيش عنها في المنازل و ما في حكمها يتعارض مع تلك الخصوصية و يعرقل السير الطبيعي لمجريات التحقيق و بناء على ذلك فإنه من الأحسن عدم تحديد وقت معين في تفتيش الحواسيب المتصلة بالإنترنت التي ارتكبت من خلالها الجريمة الموجودة في مثل تلك الأماكن و الأفضل أن تتم في أي وقت سواء ليلا أو نهارا[2].

2 ـ حضور الأشخاص المعنيين أثناء التفتيش:

يعتبر هذا الشرط من أهم الشروط الشكلية التي يتطلبها القانون في الجرائم التقليدية و ذلك لضمان الإطمئنان إلى سلامة الإجراء و صحة الضبط و الأصل أن الشخص الذي يستوجب القانون حضوره هو المتهم ، وهذا الشرط يكون قائما حتما في تفتيش الأشخاص طالما أن التفتيش يقع عليهم ، غير أنه لا يتصور تفتيش المسكن في غياب صاحبه ، وبذلك قضت التشريعات بأن يكون التفتيش في حضور المتهم أو من ينوبه فمثلا نجد التشريع المصري نص من خلال المادة 51 من إجراءات جنائية مصري بأنه يشترط تفتيش المنازل و ما في حكمها من قبل مأمور الضبط القضائي وأن يتم ذلك بحضور المتهم أو من ينوبه و في حالة غيابه يجب أن يكون ذلك الإجراء بحضور شاهدين يكونان بقدر الإمكان من أقارب البالغين أو من القاطنين معه بالمنزل أو من الجيران.

[1] ـ أنظر المادة 47 الفقرة الأولى و الثانية من قانون الإجراءات الجزائية ، القانون السابق.
[2] ـ نبيلة هبة هروال ، المرجع السابق، ص 262

كذلك المشرع الجزائري هو الآخر إشترط أن يتم تفتيش المنزل في حضور المتهم ، و في حالة إذا ما تعذر عليه الحضور وقت الإجراء ، كان على ضابط الشرطة القضائية أن يكلفه بتعيين ممثل له و إذا امتنع عن ذلك أو كان هاربا كان من الواجب أن ينوب عنه شاهدين من غير الموظفين الخاضعين له لذلك نص على أنه تتم عمليات التفتيش التي على الوجه الآتي:

ـ إذا وقع التفتيش في مسكن شخص يشتبه في أنه ساهم في ارتكاب الجناية فإنه يجب أن يجري التفتيش بحضوره فإذا تعذر عليه الحضور وقت إجراء التفتيش فإن ضابط الشرطة القضائية ملزم بأن يكلفه بتعيين ممثل له ، و إذا امتنع عن ذلك أو كان هاربا إستدعى ضابط الشرطة القضائية لحضور تلك العملية شاهدين من غير الموظفين الخاضعين لسلطته ، و إذا جرى التفتيش في مسكن يشتبه بأنه يحوز أوراق أو أشياء لها علاقة بالأفعال الإجرامية فإنه يتعين حضوره وقت إجراء التفتيش ، وإن تعذر ذلك أتبع الأجراء المنصوص عليه في الفقرة السابقة[1].

وخلاصة الأمر فإن حضور الأشخاص في أثناء إجراء عملية التفتيش سواء أكان ذلك الحضور بخصوص إجراء التفتيش بحثا عن الأدلة في الجرائم العادية أو في الجرائم المعلوماتية إجراء ضروري و ضمانة لكل من المتهم و القائم بالتفتيش ، لذلك يجب عدم إغفاله و إذا تم التفتيش بدونهم عد هذا التفتيش باطلا بطلانا نسبيا[2].

3 ـ محضر التفتيش في الجرائم الماسة بالمعطيات الرقمية:

تسمى محاضر الشرطة القضائية بمحاضر البحث الإبتدائي و تكمن أهميتها في قيمتها الممنوحة لها كوسيلة إثبات على وقوع الجريمة و نسبتها إلى فاعلها من جهة ، ومن خطورة الصلاحيات الواسعة الممنوحة بموجبها لضابط الشرطة القضائية لذلك عرف المشرع الجزائري محضر الشرطة القضائية بأنه الوثيقة المكتوبة التي يحررها ضابط الشرطة القضائية أثناء ممارسته مهامه و يضمنها ما عاينه أو تلقاه من صلاحيات أو ما قام به من عمليات تدخل في اختصاصه[3] ، و أما الأشخاص الذين خول لهم القانون فتح المحضر هم حسب القانون الإجراءات الجزائية:

ـ المدعون العامون لدى محاكم الاستئناف و نوابهم.

---

[1] ـ أنظر المادة 45 من قانون الإجراءات الجزائية الجزائري ، القانون السابق.

[2] ـ سامي جلال فقي حسين، المرجع السابق، 169

[3] ـ أنظر المادة 23 من قانون الإجراءات الجزائية الجزائري ، القانون نفسه.

ـ وكلاء الجمهورية ونوابهم.

ـ قضاة التحقيق.

وقد وسع المشرع من دائرة من يمكنهم فتح المحضر وهم:

ـ ولاة الولايات و مساعدوهم.

ـ حكام المقاطعات و رؤساء المراكز الإدارية.

ـ مدير الأمن الوطني .....[1] ، ويجب أن يحتوي المحضر على البيانات الآتية:

ـ لغة المحضر: الأصل أن يتم تحرير المحضر باللغة العربية لأنها هي اللغة الرسمية للبلاد بموجب الدستور.

ـ بيانات فتح المحضر: و من أهم هذه البيانات الرقم التسلسلي للمحضر و تاريخه ، الجهة المحررة للمحضر نوع الجريمة أو الحادث.

ـ بيانات غلق المحضر: يجب على ضابط الشرطة القضائية أن يبين تاريخ و ساعة إقفال المحضر ثم يوقع على ذلك و يعمل على أن يوقع الأشخاص المستمع إليهم عند نهاية أقوالهم ، و بصفة عامة فإنه يجب أن يكتب المحضر بخط واضح أو أن يطبع طباعة واضحة و بترتيب و تنظيم يسهل معه تتبعه و فهمه كما يلزم إبراز كل تصريح على حدة مع تفادي الكشط و الشطب أو التحشير أو التخريج كما يجب ترقيم الصفحات و ذكر عدد المرفقات و صفاتها ، كما تلزم الإشارة إلى المحجوزات و تفصيلها بذكر وصفها و نوعها و عددها و أحجامها.

كما نص قانون الإجراءات الجزائية على البيانات الواجب أن تتضمنها هذه المحاضر و هي:

ـ إسم محرر المحضر: إذ لا قيمة لمحضر محرر من مجهول.

ـ صفة محرر المحضر: فالصفة هي التي تمكن من التأكد من أن لمحرر المحضر صفة ضابط شرطة قضائية.

[1] ـ المادة 12،19 من قانون الإجراءات الجزائية، من القانون السابق.

ـ مكان عمل محرر المحضر: أي الفرقة أو المفوضية و دائرتها الإدارية ، و فيها يحدد الإختصاص المكاني.

ـ توقيع محرر المحضر: و تتمثل أهمية التوقيع في تسهيل تحديد المسؤوليات فيما يتعلق باختصاص محرر المحضر[1].

بالإضافة إلى ذلك على محرر المحضر أن يحدد طبيعة المحضر من طرفه فيذكر بأن المحضر للتفتيش و الحال ذاته بالنسبة لمحضر التفتيش في الجرائم الماسة بالمعطيات الرقمية لذلك يتضمن لتحريره نفس الإجراءات و البيانات المخصصة للمحاضر بصفة عامة[2] ، وجدير بالذكر أنه ينبغي أن يكون هناك شخص متخصص في أمور الحوسبة و الإنترنت يرافق ضابط الشرطة القضائية القائم بالتفتيش للإستعانة به في مجال الخبرة الفنية الضرورية و في صياغة مسودة محضر التفتيش.

الفرع الثاني: الشروط الموضوعية.

يقصد بالشروط الموضوعية للتفتيش بصفة عامة في الجرائم التقليدية و بصفة خاصة في الجرائم الماسة بالمعطيات الرقمية الشروط اللازمة لإجراء تفتيش صحيح ، و يمكن حصرها في الشروط الأساسية وهي سبب التفتيش ، محل التفتيش ، السلطة المختصة بالقيام بالتفتيش.

أـ سبب التفتيش في الجرائم الماسة بالمعطيات الرقمية:

من المتفق عليه في الحالات التقليدية أن سبب التفتيش إنما يعني السعي نحو الحصول على الدليل في تحقيق قائم من أجل الوصول إلى حقيقة الحدث و يمكن القول بصورة مختصرة في وقوع جريمة ما جناية أو جنحة ، و اتهام شخص أو أشخاص معينين بارتكابها أو المشاركة فيها ، وفي قيام قرائن و دلائل على وجود أشياء تفيد كشف الحقيقة سواء بشخصه أو مسكنه أو شخص غيره أو مسكنه[3] ، وبتطبيق ما تقدم على سبب التفتيش في العالم الإفتراضي ، فلا بد إذن أن نكون بصدد جريمة ماسة بالمعطيات الرقمية قد وقعت بالفعل سواء أكانت جناية أو جنحة ، و إتهام أشخاص أو شخص معين بارتكابها أو المشاركة فيها ، و بتوفر دلائل على وجود أجهزة معلوماتية تفيد في كشف الحقيقة سواء بشخص المتهم أو مسكنه أو بشخص غيره أو مسكنه ومن بين شروط سبب التفتيش.

[1] ـ أنظر المادة 23 من قانون الإجراءات الجزائية الجزائري ، القانون السابق.
[2] ـ قدري عبد الفتاح الشهاوي ، المرجع السابق، ص160.
[3] ـ نبيلة هبة هروال ، المرجع السابق ، ص229، 230

1ـ وقوع جريمة مست بالمعطيات: طالما كان هدف التفتيش و غايته هو جمع الأدلة التي تثبت وقوع الجريمة و تكشف عن هوية فاعلها ، فإن المنطق يقتضي للقيام بإجراءاته ضرورة وقوع جريمة بصورة فعلية سواء أكانت جناية أو جنحة ، و يشترط لإجراء التفتيش أن تكون الجريمة قد وقعت بالفعل فلا يجوز إجراء التفتيش بحثا عن أدلة جريمة مستقبلية و لو كان هناك إحتمال في أنها سوف تقع[1] ، والجريمة هنا التي وقعت هي جريمة ماسة بالمعطيات و التي تحاول معظم تشريعات العالم مكافحتها و تسخير أجهزة لذلك.

2ـ نسبة جريمة ماسة بالمعطيات لشخص أو أشخاص معينين إما بصفتهم فاعلين أصلين أو شركاء في ارتكاب الجريمة: الأصل أن مجرد وقوع جريمة ما سواء أكانت جناية أو جنحة ، لا يكفي لقيام سبب التفتيش بل لا بد أن تتوفر في حق الشخص المراد تفتيشه شخصه أو مسكنه دلائل كافية تدعو إلى الإعتقاد بأنه ساهم في ارتكاب الجريمة بوصفه فاعلا أو شريكا ، مما يستوجب إتهامه بها ، وفي حالة العكس ، كان على قاضي التحقيق أن يصدر أمر بأن لا وجه لإقامة الدعوى ، والحال ذاته بالنسبة للتفتيش في بيئة الإنترنت ، إذ لا يكفي وقوع جريمة قد مست المعطيات فقط بل يجب أن يكون ذلك الوقوع مقترنا بنسبتها إلى شخص أو أشخاص معنيين إما بصفتهم فاعلين أصليين أو شركاء ، أو بصفة أخرى، يجب توفر دلائل كافية تدعو للإعتقاد بأن ذلك المشتبه فيه قد ساهم في إرتكاب تلك الجريمة سواء كفاعل أصلي أو شريك[2].

3ـ وجود أدلة تثبت وجود محل للجريمة: لا يكفي لحث سلطة التحقيق على إصدار قرارها بالتفتيش و مباشرته مجرد وقوع جناية أو جنحة ، كما لا يكفي إتهام شخص معين بإرتكابها أو المشاركة فيها ، بل يجب أن يتوافر إلى جانب ذلك دليل قوي على وجود أشياء أو أجهزة أو معدات معلوماتية تفيد في كشف الحقيقة لدى المتهم المعلوماتي أو غيره ، أي أن التفتيش لا يجري إلا إذا توافرت لدى المحقق أسباب كافية على أنه يوجد في المنزل أو لدى الشخص المراد تفتيشه أو لدى غيره أدوات أستعملت في ارتكاب جريمة الإنترنت أو ناتجة عنها[3].

4ـ غاية التفتيش: إن الغاية الأساسية من إجراء التفتيش هي الحصول على الأدلة التي تسهم في كشف الحقيقة ، ففي الجرائم التقليدية يكون غاية التفتيش هي ضبط الأدلة المادية التي تفيد في كشف

[1] ـ علي حسن محمد الطولية ، المرجع السابق، 62.
[2] ـ نبيلة هبة هروال ، المرجع السابق، ص232.
[3] ـ نبيلة هبة هروال ، المرجع نفسه، ص 233.

الحقيقة ، أما في الجرائم الماسة بالمعطيات الرقمية فتكون غاية التفتيش هي الحصول على أدلة معلوماتية تساعد في الوصول إلى الحقيقة في جريمة معلوماتية وقعت وجاري التحقيق فيها ، إن الهدف من البحث هو الحصول على أدلة تكشف الحقيقة سواء أكانت أدلة إثبات الجريمة على المتهم أو أدلة تنفي التهمة عنه فمهمة القائم بالتفتيش حيادية ، تتركز في جمع أدلة كشف الحقيقة ، أدلة إثبات كانت أم نفي[1].

ب . محل التفتيش في الجرائم الماسة بالمعطيات الرقمية:

يقصد بمحل التفتيش مستودع سر الإنسان ، و هذا المستودع إما أن يكون في محل له حرمة خاصة كالمسكن أو قد يكون الشخص أو رسائله ، هذا بالنسبة للجرائم التقليدية[2]، أما بالنسبة للجرائم الماسة بالمعطيات الرقمية فإن محل التفتيش هو الحاسب الآلي الذي يعتبر النافذة التي تطل بها الإنترنت على العالم ، و الشبكة التي تشمل في مكوناتها الخادم و المزود الآلي و المضيف و الملحقات التقنية ، وتجدر الإشارة هنا إلى أن مثل هذا المحل لا يكون قائما بذاته لذلك وجب على الضبطية القضائية عند استصدارها لإذن التفتيش أن تتأكد بأنه تم تحدد محل ذلك الإجراء تحديدا دقيقا وكذلك الغرض منه و أن يتأكد من أنه مما يجوز تفتيشه ، و إلا كان ذلك الأخير باطلا ، و بالتالي ففي إطار الجرائم الماسة بالمعطيات الرقمية يقع التفتيش على المكونات المادية و المعنوية (المنطقية) للحاسب الآلي لذلك سنتطرق إلى:

1ـ مدى قابلية المكونات المادية للحاسب الآلي للتفتيش: يعتبر اللجوء إلى المكونات المادية للحاسب الآلي بحثا عن شيء ما يتصل بجريمة مست بالمعطيات وقعت يفيد في كشف الحقيقة عنها و عن مرتكبها يخضع للإجراءات القانونية الخاصة بالتفتيش بمعنى أن حكم تفتيش تلك المكونات المادية يتوقف على طبيعة المكان الموجودة فيه تلك المكونات ، مع مراعاة التمييز بين ما إذا كانت الحاسبة المراد تفتيشها منعزلة عن غيرها من الحاسبات الأخرى أو أنها متصلة بحاسبة إلكترونية أخرى أو بنهاية طرفية في مكان أخر كمسكن غير المتهم مثلا ، فإذا كانت كذلك و كانت هناك بيانات مخزنة في أوعية هذا النظام ، وأن هذا الأخير من شأنه كشف الحقيقة تعين مراعاة القيود و الضمانات التي

[1] ـ سامي جلال فقي حسين ، المرجع السابق ، ص 127

[2] ـ قدري عبد الفتاح الشهاوي ، ضوابط التفتيش في التشريع المصري و المقارن ، منشأة المعارف ، الإسكندرية ، 2005، ص111

يستلزمها المشرع لتفتيش هذه الأماكن[1].

إما لوجود شخص يحمل مكونات الحاسبة الإلكترونية المادية أو كان مسيطرا عليها أو حائزا لها في مكان ما من الأماكن العامة سواء أكان عامة بطبيعتها كالطرق العامة و الميادين و الشوارع ، أو كانت من الأماكن العامة بالتخصيص كالمقاهي و المطاعم و السيارات العامة ، فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص و بنفس الضمانات و القيود المنصوص عليها في هذا المجال.

2ـ مدى قابلية المكونات المعنوية (المنطقية) للحاسب الآلي للتفتيش: أثار تفتيش المكونات المعنوية للحاسب الآلي جدلا كبيرا في الفقه بشأن تفتيشها وذلك كمايلي:

ـ الرأي الأول: يرى بجواز ضبط البيانات الإلكترونية بمختلفة أشكالها ، و يستند هذا الرأي في ذلك أن القوانين الإجرائية عندما تنص على إصدار الإذن بضبط أي شيء فإن ذلك يجب تفسيره بحيث يشمل بيانات الحاسبة المحسوسة وغير المحسوسة ، لأن الغاية من التفتيش هي ضبط الأدلة المادية التي

تفيد في كشف الحقيقة فإن المفهوم يمتد ليشمل البيانات الالكترونية بمختلف أشكالها[2].

ـ الرأي الثاني : على نقيض الرأي الأول يرى عدم إنطباق المفهوم المادي على بيانات الحاسبة غير المرئية أو غير الملموسة ، ولذلك فإنه يقترح مواجهة هذا القصور التشريعي بالنص صراحة على أن تفتيش الحاسبة الإلكترونية لا بد أن يشمل المواد المعالجة عن طريق الحاسبة الإلكترونية أو بيانات الحاسبة الإلكترونية بحيث تصبح الغاية الجديدة من التفتيش بعد التطور التقني الذي حدث بسبب ثورة الإتصالات عن بعد تتركز في البحث عن الأدلة المادية أو أية مادة معالجة بواسطة الحاسبة.

ـ الرأي الثالث: في مقابل الرأيين أعلاه، فإن هذا الرأي نأى بنفسه عن البحث عما إذا كانت كلمة شيء تشمل البيانات المعنوية لمكونات للحاسبة الإلكترونية أو لا، فذهب إلى أن النظرة في ذلك يجب أن تستند إلى الواقع العملي و الذي يتطلب أن يقع الضبط على بيانات الحاسبة الإلكترونية إذا اتخذت

شكلا ماديا[1].

[1] ـ علي عدنان الفيل ، المرجع السابق ، ص42 . و لمزيد من التفصيل أنظر هلالي عبد اللاه أحمد ، تفتيش نظم الحاسب الآلي و ضمانات المتهم المعلوماتي ، الطبعة الأولى ، دار النهضة العربية ، القاهرة ، 1997، ص47

[2] -vassilaki(Irini) computer crimes and other crimes against information technology in Greece .Rev . Intern .De.Dr.Pen.P371

ج ـ السلطة المختصة بالتفتيش في الجرائم الماسة بالمعطيات الرقمية:

يعد التفتيش إجراء من إجراءات التحقيق الإبتدائي التي تمس حقوق و حريات الأفراد ، لذا حرص المشرع على إسنادها لجهة قضائية تكفل تلك الحقوق و الحريات ، وتتمل هذه الجهة القضائية في قاضي التحقيق أو النيابة العامة بإختلاف التشريعات كسلطة أصلية ، أو استثناءا في رجال الضبط القضائي:

1ـ إجراء التفتيش بإذن سلطة التحقيق:

لا يختلف الأمر في حالة جرائم الإنترنت عما هو عليه في الجرائم التقليدية في كون أن سلطة التحقيق الأصلية المختصة بتفتيش الجرائم التقليدية هي ذاتها المختصة في الجرائم الماسة بالمعطيات ، وهي بإختلاف التشريعات المقارنة تتمثل إما في قاضي التحقيق كسلطة أصلية و النيابة العامة استثناءا أو العكس و لابد أن تكون هذه السلطة وفقا للقواعد العامة مختصة أصلا بالتحقيق في هذه الجريمة سواء كان إختصاصا مكانيا أو نوعيا، ولما كانت مهام السلطة الأصلية في التحقيق كثيرة ومتنوعة، وخصوصا إذا ما تعددت الأمكنة أو الأشخاص المراد تفتيشهم، كان من الجائز لتلك الأخيرة أن تفوض سلطاتها في التفتيش إلى الضبطية القضائية عن طريق الإذن بذلك متى توافرت دلائل كافية قِبَل المتهم[2].

إن إناطة سلطة إصدار إذن التفتيش بالسلطة المختصة بإجراء التحقيق في الجريمة ترد عليها استثناءات فقد يحدث أن قاضي التحقيق المختص يكون غير موجود لسبب ما ، فلا يجوز ترك القضية دون إجراءات لحين حضور القاضي المختص ، ولذلك فقد منح قانون الإجراءات الجزائية صلاحية إصدار إذن استثناء إلى سلطات أخرى غير السلطات المختصة أصلا ففي حالة وقوع جريمة من نوع الجنايات أو الجنح و لم يكن قاضي التحقيق المختص موجودا فإن على المسؤول عن التحقيق عندما تقتضي الضرورة إصدار قرار أو إجراء فوري في التحقيق وعرض الأمر على أن قاضي في منطقة إختصاص قاضي التحقيق أو أي منطقة قريبة لإتخاذ ما يلزم على أن تعرض الأوراق على قاضي التحقيق المختص في أقرب وقت[3].

---

[1] ـ علي عدنان الفيل ، المرجع السابق ،ص43

[2] ـ نبيلة هبة هروال ، المرجع السابق، ص 242.

[3] ـ سعيد حسب الله عبد الله، شرح قانون أصول المحاكمات الجزائية، دار بن الأثير للطباعة، الموصل، 1998، ص177.

2 ـ تسبيب إذن التفتيش:

يحب أن يكون إذن التفتيش مسببا أي يجب أن يكون إصداره مبنيا على أسباب تبرر ذلك ، وتكمن علة التسبيب في بيان الغاية من التفتيش و غايتها هنا هي ضبط الأدلة التي تفيد كشف الحقيقة.

3 ـ شكل الإذن:

لم يشترط المشرع الجزائري شكلا معينا لأمر التفتيش ، ولكن بالرجوع إلى القواعد الأساسية للتحقيق الإبتدائي ، فإنه يحب أن تكون الإجراءات مدونة في محاضر وموقع عليها من القاضي ، ومن هذه الإجراءات أمر التفتيش الذي يصدره قاضي التحقيق على أوراق الدعوى الجزائية ، ويكون موقعا منه و مؤرخ ، ويعني ذلك أنه لا توجد ورقة معينة لأمر التفتيش إنما يكون إصدار الأمر على أوراق الدعوى ، ويعين قاضي التحقيق في الأمر الصادر بالتفتيش المكان المراد تفتيشه و الهدف من إجرائه ، وينتهي الأمر بتنفيذ الإجراء أو إلغائه ، و قد يشترط القانون أن يكون إذن التفتيش مكتوبا و لا يجوز أن يصدر شفهيا و لا يعني ذلك إقرار المحقق أمام المحكمة بأنه إذن شفوي بالتفتيش لصحة هذا الإذن ، ومتى ما كان الإذن مكتوبا جاز تبليغه للقائم بصورة شفوية في حالة الإستعجال سواء بطريق الهاتف أو البرقية ، ويجب أن يكون موقعا و مؤرخا و فيه وقت صدوره و اسم من أصدره.

4 ـ التفتيش في بيئة الإنترنت بناءا على القبض على الأشخاص:

من الآثار المترتبة على القبض الصحيح ، تفتيش المتهم عموما ، و يشترط لصحة هذا التفتيش أن تكون الواقعة محل ذلك الإجراء معقولة و أن يكون ذلك القبض بناء على توفر دلائل كافية على ارتكاب تلك الجريمة ، وغالبا ما يلجأ رجال الضبطية القضائية في الجرائم الماسة بالمعطيات الرقمية إلى تفتيش شخص المتهم المعلوماتي الذي تم القبض عليه و بسبب الإستخدام المتزايد للحاسوب المحمول و أجهزة التخزين الإلكتروني و الهواتف النقالة فإنهم وفي الغالب يفاجئون بوجود تلك الأخيرة في حوزته.

5 ـ التفتيش في بيئة الإنترنت بناءا على حالة التلبس بالجريمة:

من المتعارف عليه في معظم التشريعات الإجرائية أن حالة التلبس تعتبر إحدى الحالات التي تتسع فيها سلطات الضبطية القضائية ، حيث تصبح تباشر إختصاصات هي أصلا من اختصاص سلطة

التحقيق ومنها تحديدا التفتيش بحثا عن أدلة الجريمة و تحديد فاعلها ، سواء تعلق الأمر بتفتيش المساكن أو الأشخاص ، ولما كانت الجرائم الماسة بالمعطيات الرقمية كغيرها من الجرائم التي يمكن أن تتوفر فيها شروط الجريمة المتلبس بها كان من الجائز إجراء تفتيش شخص المشتبه به وما قد يحمله من حاسوب نقال أو هاتف نقال أو حاسوب صغير أو مسكنه وما يتضمنه من موجودات ومن بينها الحاسوب ومن مظاهر التفتيش في حالة التلبس أن يكون رجل الضبط القضائي في إحدى مقاهي الإنترنت يمارس هوايته في الإبحار عبر شبكة الإنترنت ، و يلاحظ وجود شخص آخر يقوم بالإبحار عبر تلك الشبكة في المواقع الإباحية ، ويقوم بطباعة الصور المتواجدة فيها بواسطة طابعة ففي هذه الحالة تتحقق شروط التلبس[1].

المطلب الثاني: وسائل التفتيش في الجرائم الماسة بالمعطيات الرقمية.

تعد إجراءات التفتيش و الضبط من إجراءات التحقيق التي تختص بها سلطة التحقيق ويناط لضابط الشرط القضائية القيام بهما في حالات استثنائية و يعتبر التفتيش وسيلة للحصول من خلاله على أدلة في بيان و ظهور الحقيقة ، و لا يكفي في التفتيش مجرد توافر شروطه سواء الموضوعية أو الشكلية ، بل يلزم أيضا ضرورة مراعاة حدوده الداخلية و التي يتمثل أهمها في ضرورة التقيد بالغرض من التفتيش أثناء تنفيذه وفقا لما نص عليه قانون إجراءات الجزائية و الذي يقضي بأن الأصل في التفتيش هو البحث عن الأشياء المتعلقة بالجريمة موضوع التحقيق ، و يلاحظ أنه في الحالات التي يجوز فيها لضابط الشرط القضائية القيام بإجراء التفتيش و الضبط فإن مشروعية هذا الإجراء تتوقف على محل ارتكاب الجريمة ومدى تبعيته للمجني عليه[2] لذلك قسمنا هذا المطلب إلى فرعين تناولنا في الفرع الأول: دور الإنابة في التفتيش في الجرائم الماسة بالمعطيات الرقمية ، وفي الفرع الثاني إجراءات التفتيش في الجرائم الماسة بالمعطيات الرقمية.

ـ الفرع الأول: دور الإنابة في التفتيش في الجرائم الماسة بالمعطيات الرقمية.

الأصل في تنفيذ أمر التفتيش أن يباشره من خصه القانون بالنيابة العامة أو قاضي التحقيق ، و لم يعطي القانون هذا الحق لغيرهم إلا استثناءا ، وذلك في بعض الحالات التي يخشى فيها من عدم الإسراع بالتحقيق فوات تطبيق العدالة ، أو ضياع أدلة الجريمة ، والذي يؤدي كشفها في لحظتها إلى

[1] ـ نبيلة هبة هروال ، المرجع السابق، ص 248.
[2] ـ خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية المرجع السابق، ص 228.

بيان الحقيقة ، و الإنابة التي تصدر من صاحب السلطة بالتفتيش إلى أحد ضباط الشرطة القضائية هي الصورة الإستثنائية في التحقيق الجنائي ، وفي التطبيق العملي نجد أن الصورة الأولى قليلة الحدوث ، بينما الصورة الثانية ـ الإستثنائية ـ كثيرة الوقوع في الحياة اليومية ، ولأهمية الإنابة في موضوع التفتيش سنتطرق إلى:

1ـ تعريف الإنابة بإجراء التفتيش:

الإنابة أو الإذن أو الندب للتحقيق عموما يراد به الإنابة الصادرة ممن له سلطة التحقيق إلى أحد أعضاء الضبطية القضائية يفوضه بموجبها إجراء عمل أو أكثر من أعمال التحقيق ، و يعرفها جانب من الفقه بأنها تصرف إجرائي يصدر ممن له سلطة التحقيق بمقتضاه يفوض أحد ضباط الشرطة القضائية ليقوم به بدل منه وفي الشروط التي يجب أن يتقيد بها بمباشرة إجراء معين أو أكثر من إجراءات التحقيق التي تدخل في سلطته ويعرفه جانب آخر من الفقه بأنه أمر إنابة أو ندب في مباشرة التفتيش ويصدر هذا الأمر أو الإذن من الجهة صاحبة الإختصاص الأصيل في مباشرة إجراء التحقيق لغيرها من مأموري الضبط القضائي ، عندما تدعو لذلك ضرورة عملية كلزوم سرعة إتخاذ إجراء أو أكثر أو كثرة أعمال التحقيق في القضية ذاتها أو كون الإجراء يلزم القيام به والخروج من دائرة الإختصاص[1].

ومن التعاريف السابقة يتضح أن الإنابة تقوم على أساس صدور تفويض ممن يملك إختصاص مباشرة التحقيق ، إلى مفوض إليه لا يملك مباشرته من حيث الأصل لكونه خارجا عن نطاق إختصاصه الوظيفي لذلك فإن الإنابة تتمثل في الحقيقة في مخالفة مؤقتة لقواعد الإختصاص الوظيفي.

ويعلل هذا الرأي بأن الحاجة إليه ضرورية لتلبية دواعي الإسراع في إنجاز إجراءات التحقيق ، أو الرغبة في التخفيف من أعباء المحقق وتوفير الوقت الكافي له ليقوم بمباشرة باقي إجراءات التحقيق ، وغيرها مما يستدعي تلك الإنابة ونجد في نطاق التفتيش في الجرائم الماسة بالمعطيات الرقمية الإنابة أو الإذن ضرورية جدا ، وتبريره أن المحقق قد لا يستطيع تنفيذه بنفسه لوجود عدة جرائم في الوقت نفسه أو أن الجريمة المرتكبة عبر الإنترنت ومن عدة مناطق فيحتاج المحقق لمساعدين لإجراء التفتيش في جميع هذه المناطق و في نفس الوقت.

[1] ـ على حسن الطوالبة، المرجع السابق، ص103.

2 ـ الطبيعة القانونية للإنابة بالتفتيش:

إن الإنابة في التفتيش تستمد سندها القانوني بوضوح من النصوص الصريحة التي ترد على تلك القوانين إلى الحد الذي يمكن القول معه إن ذلك النوع من الإنابة أصبحت في وقتنا الحاضر من المبادئ التي استقرت على الأخذ بها جميع القوانين الحديثة.

لذلك نصت بعض التشريعات على الإنابة القضائية في التفتيش ، وقد نص المشرع الجزائري على "يجوز لقاضي التحقيق أن يكلف بطريق الإنابة القضائية أي قاض من قضاة محكمة أو أي ضابط من ضباط الشرطة القضائية المختصة للقيام بما يراه لازما من إجراءات التحقيق في الأماكن الخاضعة للجهة القضائية التي يتبعها كل منهم[1]".

أما المشرع الفرنسي فيأخذ بنظام الفصل بين سلطة التحقيق و سلطة الإتهام ، فيجعل سلطة التحقيق من اختصاص قاضي التحقيق ، أما سلطة الإتهام فهي من اختصاص وكيل النيابة ، فيكون لقاضي التحقيق ، دون غيره سلطة التحقيق بصفة أصلية ، أما وكيل النيابة فليس له سلطة التحقيق إلا على سبيل الإستثناء ، كما في حالة التلبس بالجريمة ، مثله في ذلك مثل ضابط الشرطة القضائية الذي له حق مباشرة إجراءات التحقيق في حالة ضبط الجريمة في حالة تلبس ، و يحق لقاضي التحقيق أن ينيب عضو من ضباط الشرطة القضائية للتفتيش[2].

على عكس بعض التشريعات التي جمعت بين سلطتي الإتهام و التحقيق كما في القانون الأردني و المصري.

ومن خلال ما تقدم نجد أن أغلب التشريعات متفقة على الأخذ بمبدأ إنابة عضو من ضباط الشرطة القضائية ، وإن اختلفت من حيث التشديد أو التخفيف في صفة من له سلطة التحقيق في كل منها ، إلا أنها متفقة على مبدأ واحد وهو أن من يملك سلطة التحقيق يملك سلطة الإنابة ، وأن السند القانوني لهذه الإنابة يستمده المحقق من خلال النص على جواز الأخذ بها صراحة في هذه القوانين.

أما الطبيعة القانونية للإنابة بالتفتيش فهناك آراء متعددة و هناك من يعتبر الإنابة إجراء من إجراءات التحقيق باعتبارها صادرة من السلطة المختصة بالتحقيق و هي سلطة قضائية ، ومن طبيعة محل

[1] ـ أنظر المادة 138 من قانون الإجراءات الجزائية الجزائري ، القانون السابق.
[2] ـ على حسن الطوالبة، المرجع السابق،ص106.

التفويض ، وهو طلب القيام بمباشرة إجراء أو أكثر من إجراءات التحقيق ، و القيمة القانونية للإجراءات التي يقوم بها ضابط الشرطة القضائية ومنها التفتيش في الجرائم الرقمية على نظم الحاسب الآلي ، تكون لها نفس القيمة القانونية التي تكون للإجراءات التي قام بها قاضي التحقيق ، ومن هنا تعتبر جميع الإجراءات التي يتخذها ضابط الشرطة القضائية بناءا على أمر الإنابة الصادرة من المحقق أعمال تحقيق و ليس أعمال الإستدلال ، كما تعتبر المحاضر التي يعدها حال قيامه بهذه الإجراءات محاضر تحقيق و ليس محاضر استدلال ، وهي تعد من الناحية القانونية أدلة ناتجة عن

إجراءات التحقيق تصلح لأن يؤخذ بها كسند للحكم بالبراءة أو الإدانة على حد سواء[1].

الفرع الثاني : إجراءات التفتيش في الجرائم الماسة بالمعطيات الرقمية.

يعد حضور أشخاص معينين أثناء إجراء التفتيش من قبل الشخص المكلف بذلك قانونا من الضمانات المهمة التي تكفل إجراءه بشكل صحيح ، و يبعد الشك حول إمكانية إخفاء الدليل من قبل القائمين به ، ويعد ضمانة للقائم بالتفتيش ، و يقوم المفتش بمجموعة من الإجراءات منها:

1 ـ إجراءات تفتيش النظام المعلوماتي الخاص بالمتهم:

إذا كان محل ارتكاب الجريمة ينصب على نظام المعلومات الخاص بالمتهم دون تطلب التدخل في نظام معلوماتي لشخص آخر، و في هذا الفرض إذا كانت الشروط الإجرائية للتفتيش صحيحة وفقا لما نص عليه القانون فإن التفتيش و ما يسفر عنه من ضبط أي من الأدلة ، سواء أكانت هذه الأدلة هي أجهزة الكمبيوتر أم أحد الوسائط المتعددة ، يكون مشروعا ، وهذا الحال يكثر في جرائم التزوير و التزييف حيث يتم التفتيش و ملحقاته من طباعات ملونة أو أجهزة ماسح ضوئي ، و يتم نقل البرنامج الداخلي الذي يوجد عن طريق إتمام عملية التزوير أو التزييف في أي من الوسائط المتعددة و بذلك يتم الحصول على دليل إرتكاب الجريمة ، وهذا ما يتم أيضا في جرائم النسخ و التقليد حيث يتم ضبط الوسائط المتعددة المحملة بالبرنامج المنسوخة و الأجهزة المستخدمة في ذلك[2].

2 ـ إجراءات التفتيش في نظام معلوماتي غير خاص بالمتهم:

يظهر هذا الفرض في الجرائم التي ترتكب باستخدام الشبكات بحيث يتم ارتكاب الجريمة من أي جهاز

[1] ـ على حسن الطوالبة، المرجع السابق، ص108.
[2] ـ خالد ممدوح إبراهيم ، المرجع السابق ، ص 229.

من أجهزة الحاسبات الآلية الأخرى و المتصلة بالحاسب الذي ارتكبت في نظامه المعلوماتي الجريمة و في هذا الفرض فإن إجراءات التفتيش و الضبط تتطلب الدخول في نظام معلوماتي لشخص آخر، ويلاحظ أن قانون الإجراءات الجزائية نص على أنه لا يجوز لرجال الشرطة القضائية الدخول في أي محل مسكون إلا في الأحوال المبينة في القانون ، أو في حالة طلب المساعدة من الداخل .....وهو ما دعا المشرع إلى مد تلك الحماية إلى المحل الخاص بحيث أقر له ذات الحماية الخاصة بالمسكن و كذلك السيارة الخاصة إذا كانت توجد في مسكن المتهم ، أما إذا وجدت في الطريق العام فلها نفس حرمة الشخص بحيث لا يجوز تفتيشها إلا إذا جاز تفتيش الشخص قانونا.

3 ـ تطبيقات في إجراءات تفتيش نظم الحاسبات الآلية الخاصة بالأشخاص:

طبقا لمعيار الخصوصية التي يحميها المشرع يتبين أنه قد تناول المسكن و السيارة و المحل و كل ما تعلق بالشخص و يمثل خصوصياته ، و لذلك فإن نضام المعلومات وما يحويه من خصوصيات للأشخاص تخضع أيضا و بالتبعية لمعيار الخصوصية من حيث عدم جواز التدخل فيه بدون إذن من وكيل الجمهورية[1].

رغم أن المشرع و في جل القوانين التي نصها حاول حماية الخصوصية للأفراد بما فيها البيانات و المعلومات الشخصية و كذلك السجلات و الدفاتر أو الحاسبات الآلية و الملحقات السرية بعدم جوازية الإطلاع عليها أو الحصول على بياناتها إلا في الأحوال التي نص عليها القانون ، وهذا ما أكده أيضا بامتداد الحق في التفتيش إلى سجلات البيانات التي تكون في موقع إلكتروني آخر عندما يكون التخزين الفعلي خارج المكان الذي يتم فيه التفتيش.

و كذلك ذهب جانب آخر من الفقه بأن البيانات لها طابع مادي على أساس أنها نبضات أو ذبذبات إلكترونية و إرشادات أو موجات كهرومغناطيسية قابلة لأن تسجل و تخزن على وسائط متعددة و يمكن قياسها[2].

و لأن البحث عن الدليل على ارتكاب الجريمة ، من حيث كونه وسيلة للإثبات ومحلا للإقتناع وفقا لنظرية الإثبات الجنائي يتطلب الإتجاه السابق من أراء الفقهاء من حيث الإقرار بإمكانية أن تكون المعلومات محلا للتفتيش و ضبط الأدلة المتحصل عليها ، ويلاحظ أن الأمر يختلف من حيث صدور

[1] ـ خالد ممدوح إبراهيم ، المرجع السابق ، ص 230.
[2] ـ خالد ممدوح إبراهيم ، المرجع نفسه ، ص331.

إذن بالتفتيش في النظام المعلوماتي لأحد الأشخاص عنه في الإذن بالتفتيش في الجرائم التقليدية الأخرى ، لأن الإذن قد يصدر في حق شخص قد ارتكب جناية أو جنحة و قامت قرائن قوية على ارتكابه للجريمة و عند القيام بتنفيذ إذن التفتيش ، فإن الأمر قد يقتضي امتداد حق التفتيش إلى نظام معلوماتي آخر إما تابع للمتهم ، أو أن للمتهم أكثر من جهاز في أماكن مختلفة كأن يكون المتهم مالكا لجهاز في منزله و جهاز آخر في عمله ، أو أن يكون الشخص له شريك في الأجهزة مما يتطلب الحصول على إذن آخر من وكيل الجهورية.

وذلك عن طريق تحديد مجال هذا التفتيش وما يستتبعه بالضرورة من تتبع لشبكات المعلومات و يخضع ذلك للسلطة التقديرية للقاضي من حيث توافر حالة الضرورة أو عدم توافرها ، و هذا النظام إتبعته بعض الدول مثل الولايات المتحدة الأمريكية و كندا ، حيث نصتا على أن يكون إذن التفتيش متضمنا ما يلي:

ـ البحث عن أدلة محصلة من كيان الحساب المنطقي و التي يدخل فيها برامج التطبيق و نظم التشغيل.

ـ البيانات المستخدمة بواسطة برنامج الكمبيوتر أو كيانه المنطقي.

ـ السجلات التي تثبت استخدام الأنظمة الآلية لمعالجة البيانات[1].

ـ السجلات المستخدمة في عملية الولوج في النظام الآلي لمعالجة البيانات.

4 ـ التعاون الدولي في مجال تمديد إجراءات التفتيش و الضبط خارج حدود الدولة:

يعد التفتيش بوصفه إجراء تحقيقيا تنص عليه التشريعات مساسا بحرية الأفراد و حرية أماكنهم و التي تكفل القانون بحمايتها من أي انتهاك ، فالتفتيش يشكل انتهاكا قانونيا لهذه الحرية و الجريمة التي كفلها المشرع و ذلك بهدف تحقيق مصلحة أهم و أعم من مصلحة الأفراد و هي المصلحة العليا للمجتمع ، التي تتمثل في كشف الحقيقة في جريمة وقعت ، بهدف إيصال الجاني إلى العدالة حيث قد تستدعي مصلحة التحقيق إتخاذ هذا الإجراء للحصول على الأدلة التي تفيد في كشف الجريمة[2].

[1] ـ خالد ممدوح إبراهيم، المرجع السابق، ص232.
[2] ـ سامي جلال فقي حسين، المرجع السابق، ص09.

ولكون الجرائم الماسة بالمعطيات الرقمية ظاهرة مستحدثة على الساحة الإجرامية داخل الجزائر لم ينص قانون العقوبات عليها صراحة بل ذكر في القسم السابع مكرر03 عنوان المساس بأنظمة المعالجة الآلية للمعطيات ، و بين كذلك أن تعقب مرتكب الجريمة و تتبع آثاره و ضبط الأدلة المعلوماتية الدالة على ارتكابه للجريمة قد لا يتقد بحدود الدولة وإنما يمتد إلى خارجها و هذا مرجعه إلى قوة شبكات الإنترنت التي ربطت جميع الدول ببعضها البعض و أصبح لا يحدها فاصل.

و أمام هذا التطور التكنولوجي بات ارتكاب الجرائم من دولة إلى أخرى من السهولة بمكان ، و لذلك أصبح من ضروري البحث في مشروعية القيام بإجراء التفتيش و الضبط من قبل من الضبطية القضائية لمتهم في دولة أخرى ، و تعرف الجريمة بهذا الوصف بالجريمة المنظمة نتيجة مزاولة الأنشطة الإجرامية عبر حدود الدول ، مما دعا الدول لإقرار أن الجريمة المنظمة هي في حقيقتها جريمة داخلية مضافا إليها البعد الدولي ، أي بارتكابها خارج حدود الدولة و حدوث النتيجة داخلية[1].

و إذا كان الإختصاص بنظر تلك الجرائم ينعقد وفق للإختصاص المكاني للدولة التي حدث ارتكاب الجريمة على أرضها تبعا لمبدأ السيادة الدولة ، فإن للضبطية القضائية القيام بإجراء التفتيش و الضبط على أرضها ، ومن هنا يثور البحث في حالة إمتداد إجراءات التفتيش و الضبط خارج حدود الدولة و الدخول في سيادة دولة أخرى.

ومن هنا يثور البحث في حالة إمتداد إجراءات التفتيش و الضبط خارج حدود الدولة و الدخول في سيادة دولة أخرى ، لذلك فإن الدولة حرصا منها على مراعاة مصلحتين هامتين هما احترام الخصوصية للأشخاص ومواجهة الجرائم المرتكبة لتحقيق الصالح العام أبرمت العديد من الإتفاقيات الدولية لمكافحة هذه الظاهرة ، هذا بجانب الضامنات التي أقرتها المواثيق الدولية[2].

[1] ـ خالد ممدوح إبراهيم، المرجع السابق، ص 234.
[2] ـ خالد ممدوح إبراهيم ، المرجع نفسه ، ص 235

الفصل الثاني: إثبات الجرائم الماسة بالمعطيات الرقمية والجزاءات المقررة لها.

لما كان الإرتكان إلى القضاء يعتبر من حيث الترتيب الزمني آخر مرحلة يمكن اللجوء إليها ، فإن ذلك يجب أن يكون ممن كانت مصالحه مهددة سواء أكانت تلك المصالح محمية بمقتضيات زجرية أو غير زجرية كما يجب أن يكون ذلك اللجوء مقرونا بوسائل مثبتة للإعتداء على تلك المصالح أو مهددة للمراكز.

و كما هو معلوم فإن فكرة الإثبات بصفة عامة يمكن أن تندرج في سياق الصراع القائم بين كل من مدرسة الإثبات الحر و مدرسة الإثبات المقيد و مدرسة الإثبات المختلط ، و لذلك يبدو من المفيد جدا أن نقف عند نطاق الأخذ باتجاهات تلك المدارس في المجال الجنائي عموما و مجال إثبات الجريمة الماسة بالمعطيات الرقمية على وجه الدقة على اعتبار أن حداثة ظهور هذا النوع من الجرائم يطرح العديد من الإشكالات التي تنبع من صميم طبيعة الجريمة الرقمية ذاتها، و هكذا يمكن القول بأن الطبيعة المادية للجريمة الإلكترونية تفرض على الجهات المكلفة بإنفاذ القانون ضرورة التعامل مع الوسائل الجديدة و الكفيلة بالكشف عن تلك الجرائم من جهة و تحديد مرتكبيها من جهة أخرى.

و في ظل الصعوبات التي تطرحها الجريمة الإلكترونية سواء على المستوى الواقعي أو القانوني ، يبدو البحث في نظام إثبات هذا النوع من الجرائم مجازفة نظرا لوجود هوة فارقة بين مستوى التنظيم التشريعي للجريمة الماسة بالمعطيات الرقمية و التطور الذي يشهده هذا النوع من الجرائم ، و هي الهوة التي يمكن و صفها بالمتطورة وفق متتالية هندسية تجعل من المستحيل على المشرعين الإحاطة بجميع حيثياتها و جوانبها ، لذلك فإن البطء التشريعي في هذا المجال و ضعف التعاطي الواقعي مع مختلف مظاهر الجريمة الماسة بالمعطيات الرقمية يعتبران من الدوافع الأساسية التي تؤثر سلبا في بلورة تصور ملائم لنظام إثبات ملائم من شأنه المساهمة في محاربة الجريمة الماسة بالمعطيات الرقمية ، وقد قسمنا هذا الفصل إلى مبحثين تناولنا في المبحث الأول :إثبات الجرائم الماسة بالمعطيات الرقمية ، وفي المبحث الثاني الجزاءات المقررة للجرائم الماسة بالمعطيات الرقمية.

المبحث الأول: إثبات الجرائم الماسة بالمعطيات الرقمية.

إذا كان البحث في مسألة إثبات الجريمة الماسة بالمعطيات الرقمية أمرا صعبا ، فإن الصعوبة تبدأ انطلاقا من تعريف الجريمة الإلكترونية ذاتها على اعتبار أن التعريف يعتبر مدخلا أساسيا لتحديد نطاق إعتماد وسائل إثبات معينة دون غيرها و مدى السلطات التي يتمتع بها القاضي في تقدير القيمة القانونية لتلك الوسائل أو ما يملكه الأطراف من حرية في التعامل مع نفس وسائل الإثبات ، لذلك يذهب معظم المهتمين إلى القول بأن الجريمة الإلكترونية باعتبارها مظهرا جديدا من مظاهر السلوك الإجرامي لا يمكن تصورها إلا من خلال ثلاث مظاهر ، إما أن تتجسد في شكل جريمة تقليدية يتم اقترافها بوسائل إلكترونية أو معلوماتية ، أو في شكل إستهداف للوسائل المعلوماتية ذاتها و على رأسها قاعدة المعطيات و البيانات أو البرامج المعلوماتية ، أو أن يتم اقتراف الجرائم العادية في بيئة إلكترونية كما هو الأمر مثلا بالنسبة لجرائم الصحافة.

وقد قسمنا هذا المبحث إلى مطلبين تناولنا في المطلب الأول: دور المعاينة في إثبات الجرائم الماسة بالمعطيات الرقمية، في حين تناولنا في المطلب الثاني: دور الشهادة و الخبرة في إثبات الجرائم الماسة بالمعطيات الرقمية.

المطلب الأول: دور المعاينة في إثبات الجرائم الماسة بالمعطيات الرقمية.

مع تزايد إستخدام الكمبيوتر و الإنترنت و الشبكات الداخلية و الخارجية تزايدت نسبة الإعتداء على المعطيات بشكل كبير باستخدام تقنيات جديدة و متطورة يعمد إليها مرتكبو الجرائم ، سواء أكانت جريمة تمت عبر الكمبيوتر أم جريمة تمت على الكمبيوتر و لذلك كان من الواجب على ضابط الشرطة القضائية الإنتقال على ذلك المكان ، لمعاينة و إثبات الآثار المادية للجريمة والمحافظة عليها و إثبات حالة الأماكن و الأشخاص و كل ما يفيد في كشف الحقيقة ، وكذا إخطار وكيل الجمهورية فورا لكي ينتقل بدوره إلى محل الجريمة في حالة الجناية المتلبس بها[1].

[1]- نصت المادة 42 من قانون الإجراءات الجزائية " يجب على ضابط الشرطة القضائية الذي بلغ بجناية في حالة تلبس أن يخطر بها وكيل الجمهورية على الفور ثم ينتقل بدون تمهل على مكان الجناية و يتخذ جميع التحريات اللازمة.
وعليه أن يسهر على المحافظة على الآثار التي يخشى أن تختفي ، و أن يضبط كل ما يمكن أن يؤدي إلى إظهار الحقيقة .
و أن يعرض الأشياء المضبوطة على الأشخاص المشتبه في مساهمتهم في الجناية للتعرف عليها.

و تعتبر المعاينة أهم إجراء من إجراءات التحقيق قاطبة و يجوز لوكيل الجمهورية أن يقوم بها في غياب المتهم إذا لم يتيسر حضوره ، والمعاينة لها أهمية قصوى في إثبات الواقعة ، وقد قسمنا هذا المطلب إلى فرعين تناولنا في الفرع الأول: تعريف معاينة الدليل الإلكتروني في الجرائم الماسة بالمعطيات الرقمية ، وفي الفرع الثاني الدليل الإلكتروني في الجرائم الماسة بالمعطيات الرقمية.

الفرع الأول: تعريف معاينة الدليل الإلكتروني في الجرائم الماسة بالمعطيات الرقمية.

يقصد بالمعاينة: مشاهدة و إثبات الآثار المادية التي خلفها ارتكاب الجريمة ، بهدف المحافظة عليها خوفا من إتلافها أو محوها أو تعديلها.

والمعاينة من إجراءات التحقيق الإبتدائي ، و يجوز للمحقق اللجوء إليها متى رأى لذلك ضرورة تتعلق بالتحقيق ، و الأصل أن يحضر أطراف الدعوى الجزائية المعاينة ، وقد يقرر المحقق أن يجربها في غيابهم ، و لا يلتزم المحقق بدعوة محامي المتهم للحضور[1].

كذلك عرفت المعاينة بأنها إجراء بمقتضاه ينتقل المحقق إلى مكان وقوع الجريمة ليشاهد بنفسه و يجمع الآثار المتعلقة بالجريمة و كيفية وقوعها و كذلك جمع الأشياء الأخرى التي تفيد في كشف الحقيقة[2].

و المعاينة و إن كانت إجراء يجوز اللجوء إليه في كافة الجرائم ، إلا أنها ليست إجراء مجدي أو صالح لكشف الحقيقة في الجرائم كلها ، فهي ليست إجراء تلقائي في مباشرتها بل إجراء هادف ، غايته الكشف عن العناصر المادية التي تتعلق بالجريمة و تفيد في التحقيق الجاري بشأنها ، فإذا إنعدم ذلك الهدف كما هو الحال في جريمة التزوير المعنوي و جريمة السب التي تقع بالقول في غير علانية و غيرهما ، لم يكن ثمة مجال أو مقتضى لإجرائها[3].

ـ المعاينة في الجرائم الخاصة بالمعطيات:

يقصد بها معاينة الآثار التي يتركها مستخدم شبكة الإنترنت و تشمل الرسائل المرسلة منه أو التي يستقبلها و كافة الإتصالات التي تمت من خلال الكمبيوتر و الشبكة العالمية ، فمستخدم الإنترنت

[1] ـ محمود نجيب حسني، شرح قانون الإجراءات الجنائية، ط3 ، دار النهضة العربية، القاهرة ، 1998،ص 529
[2] ـ مأمون سلامة، قانون الإجراءات الجنائية، دار الفكر العربي، الطبعة الأولى،1980، ص347
[3] ـ هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، أسيوط، 1994، ص 58

عندما يتجول في حوار إنترنت يترك آثار أقدامه في كل مكان يزوره فالموقع الذي يمر به يفتح سجلا خاصا به يتضمن عنوان الموقع الذي جاء منه ، و نوع الكمبيوتر و المتصفح الذي يستخدمه و عنوان رقم (IP) الدائم و المتغير للكمبيوتر الذي يتصل منه ، ويمكن تحت ظروف معينة أن يتمكن الموقع من الحصول على عنوان البريد الإلكتروني و الإسم الحقيقي للمستخدم.

ويلاحظ أن الآثار الرقمية المستخلصة من أجهزة الكمبيوتر من الممكن أن تكون ثرية جدا فيما تحتويه من معلومات مثل صفحات المواقع المختلفة ، البريد الإكتروني ، الفيديو الرقمي والصوت الرقمي ، غرف الدردشة والمحادثات ، الملفات المخزنة في الكمبيوتر الشخصي ، الصور المرئية ، الدخول إلى الخدمة و الإتصال بالإنترنت والشبكة عن طريق مزود الخدمات وفي كل الأحوال عند تلقي البلاغ عن موقع إحدى جرائم الإنترنت ، وبعد التأكد من البيانات الضرورية في البلاغ يتم الإنتقال إلى مسرح الجريمة للمعاينة[1].

ـ مدى أهمية المعاينة في الجرائم الماسة بالمعطيات الرقمية:

مع التسليم بأهمية المعاينة في كشف غموض الكثير من الجرائم التقليدية و جدارتها إلا أن دورها في مجال كشف غموض الجرائم الماسة بالمعطيات الرقمية و ضبط الأشياء التي تفيد في إثبات وقوعها و نسبتها إلى مرتكبها لا ترقى إلى نفس الدرجة من الأهمية ، ومرد ذلك إلى اعتبارين هما:

1ـ أن الجرائم التي تقع على نظم المعلومات و الشبكات قلّما يتخلف عن ارتكابها آثارا مادية.

2ـ أن عددا كبيرا من الأشخاص قد يتردد في المكان أو مسرح الجريمة خلال الفترة الزمنية الطويلة نسبيا و التي تتوسط عادة بين زمن إرتكاب الجريمة و بين اكتشافها مما يفسح المجال لحدوث تغير أو إتلاف أو عبث بالآثار المادية أو زوال بعضها وهو ما يلقي ظلالا من الشك على الدليل المستمد من المعاينة.

أولا ـ إجراءات معاينة مسرح الجريمة الماسة بالمعطيات الرقمية:

تكون معاينة مسرح الجريمة أول إجراء يقوم به المحقق بعد تلقي البلاغ أو إخطاره به و ذلك في

[1]- هدى طلب علي، الإثبات الجنائي في جرائم الانترنت و الإختصاص القضائي بها، مذكرة ماجستير، تخصص قانون عام، كلية الحقوق، جامعة النهرين، 2012 ، ص 81.

ظروف قد لا يكون فيها عنصر الخصوم أو المتهمين قد ظهر بعد بهذه الصفة على ساحة التحقيق ، لذلك عرف مسرح الجريمة بأنه: هو كل محل أو وحدة من منشأة أو رقعة من الأرض تضم بؤرة الجريمة ومركزها بحيث تكون ميدانا لأنشطة الجاني أو الجناة من الفاعلين الأصليين عند ارتكاب الأفعال المؤثمة جنائيا و التي تدخل في إعداد الأعمال التنفيذية المكونة للجريمة أو الشروع فيها.

و حتى تكون للمعاينة في الجرائم الماسة بالمعطيات الرقمية فائدة في كشف الحقيقة عنها وعن مرتكبها ينبغي مراعاة عدة قواعد و إرشادات فنية أهمها ما يلي:

ـ تصوير الحاسبة الإلكترونية و الأجهزة الطرفية المتصلة بها و المحتويات و الأوضاع العامة بمكانه ، مع التركيز بوجه خاص على تصوير الأجزاء الخلفية للحاسبة و ملحقاتها و مراعاة تسجيل وقت و تاريخ ومكان التقاط كل صورة.

ـ العناية البالغة بملاحظة الطريقة التي تم بها إعداد النظام و الآثار الإلكترونية الخاصة بالتسجيلات الإلكترونية التي تتزود بها شبكات المعلومات بموافقة موقع الإتصال و نوع الجهاز الذي تم عن طريق الولوج إلى النظام أو الموقع[1].

ـ ملاحظة و إثبات التوصيلات و الكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عملية المقارنة و التحليل عند عرض الأمر فيها على القضاء.

ـ وضع مخطط تفصيلي للمنشأة التي وقعت بها الجريمة مع كشف تفصيلي للمسؤولين بها ودور كل واحد منهم.

ـ فصل الكهرباء عن موقع المعاينة لشل فاعلية الجاني في القيام بأي فعل من شأنه التأثير على آثار الجريمة.

ـ إبعاد الموظفين عن أجهزة الحاسبة الإلكترونية ، وكذلك عن الأماكن الأخرى التي توجد بها أجهزة للحاسبة الإلكترونية[2].

[1] ـ على عدنان الفيل، المرجع السابق،ص 32، 33
[2] ـ على عدنان الفيل، المرجع نفسه، ص34

ـ عدم نقل أي معلومة من مسرح الجريمة إلا بعد التأكد من خلو المحيط الخارجي لموقع الحاسبة الإلكترونية من أي مجال مغناطيسي يمكن أن يتسبب في محو البيانات المسجلة.

ـ التحفظ عما قد يوجد بسلة المهملات ، من الأوراق الملقاة أو الممزقة أو أوراق الكربون المستعلمة و الأشرطة و الأقراص الممغنطة غير السليمة و فحصها و رفع البصمات التي قد تكون لها صلة بالجريمة المرتكبة.

ـ التحفظ على مستندات الإدخال و المخرجات الورقية للحاسبة ذات الصلة بالجريمة لرفع و مضاهاة ما قد يوجد بها من بصمات.

ـ قصر مباشرة المعاينة على فئة معينة من الباحثين و المحققين الذين تتوافر لديهم الكفاءة العلمية و الخبرة الفنية في مجال الحاسبة الإلكترونية و الشبكات و نظم المعلومات و استخراج المعلومات الذين تلقوا تدريبا كافيا على التعامل مع نوعية الآثار و الأدلة التي يحويها مسرح الجريمة المعلوماتية[1].

ويعد الإثبات الجنائي بالأدلة الرقمية من أبرز تطورات العصر الحديث في كافة النظم القانونية ، وذلك بفعل التطورات التي جاءت لتلاءم الثورة العلمية و التكنولوجية و التقنية في عصرنا الحالي ، و التي تطور معها الفكر الإجرامي ، فظهر نوع جديد من الجرائم هو ما يعرف بالجرائم الرقمية ، مما ألقى على عاتق القائمين على مكافحة الجريمة في الدول عبئا شديدا ومهما يفوق القدرات المتاحة لهم وفق أسس و قواعد إجراءات البحث الجنائي و الإثبات الجنائي التقليدي ، نظرا لعدم كفاية وعدم ملائمة هذه النظم التقليدية ، و إثبات تلك الجرائم ـ سواء من الناحيتين القانونية أو الفنية ـ وكان حتما على المشرع أن يستحدث من التشريعات ما يلائم هذا النوع من الجرائم ، فضلا عن إنشاء أجهزة فنية متخصصة يناط بها عملية الإثبات العلمي الفني لهذه الجرائم.

و عملية الإثبات في الجرائم الرقمية هي مجموعة القواعد المتعلقة بالبحث عن الأدلة و إقامتها أمام القضاء و تقديرها من جانبه ، فالإثبات هو مجموعة الأسباب المنتجة لليقين ، و بالتالي فإن الإثبات في المواد الجنائية ما هو إلا كافة الأدلة التي تؤكد وقوع الجريمة ، و تحقق حالة اليقين لدى القاضي

[1] ـ على عدنان الفيل، المرجع السابق، ص35
ففي فرنسا مثلا يقوم فريق مكون من 13 شرطي بالإشراف على تنفيذ المهمات التي يعهد بها إليه وكلاء النيابة و المحقيقن ، وجميعهم تلقوا تدريب متخصص إلى جانب اختصاصهم الأساسي في مجال التكنولوجيا الحديثة و هم يقومون بمرافقة المحققين أثناء التفتيش حيث يقومون بفحص كل جهاز وينقلون نسخة من الأسطوانة الصلبة وبيانات البريد الإكتروني ثم يقومون بعمل تقرير يرسل إلى القاضي الذي يتولى التحقيق أما عن المعدات والبرامج ، فهم يستخدمون برامج تستطيع إستعادة المعلومات من على الأسطوانة الصلبة كما يمكنها قراءة الأسطوانات المرنة والصلبة التالفة ، كما يوجد تحت تصرفهم برامج تمكنهم من قراءة الحاسبات المحمولة.

لإدانة المتهم ، أو ترجح حالة الشك لديه فيقضي بالبراءة أو هو ما يؤدي إلى إظهار الحقيقة ، و لأجل الحكم على المتهم في المسائل الجنائية يجب ثبوت وقوع الجريمة في ذاتها و أن المتهم هو المرتكب لها ، و بعبارة أخرى وقوع الجريمة بوجه عام و نسبتها للمتهم بوجه خاص و تعد كل من الدليل الرقمي و الشهادة و الخبرة أحد وسائل جمع الأدلة لإثبات الجرائم الماسة بالمعطيات الرقمية و لذلك سنتطرق إلى:

ثانيا: شروط معاينة مسرح الجريمة الماسة بالمعطيات الرقمية.

بعد تلقي بلاغ بوقوع إحدى الجرائم الماسة بالمعطيات الرقمية والتأكد من البيانات الضرورية في البلاغ ، يتم الإنتقال إلى مسرح الجريمة لمعاينته ، ومسرح الجريمة المعلوماتية يختلف عن مسرح الجريمة التقليدية كالقتل والسرقة ، والجريمة المعلوماتية قد تكون جريمة مستقلة كما في حالة جرائم السرقة والإحتيال وقد يكون مسرحها كالجرائم الأخرى كما في التزوير والإتلاف ، ويكون هدف المعاينة ضبط الأدلة على طبيعتها ، وفي سبيل ذلك لابد من مراعاة جملة من الشروط على النحو التالي:

1 ـ وجود معلومات مسبقة عن مكان إرتكاب الجريمة من حيث عدد الأجهزة المطلوب معاينتها وشبكتها.

2 ـ وجود خريطة توضح الموقع الذي ستتم معاينته، وتفاصيل المبنى أو الطابق موضوع البلاغ وعدد الأجهزة والخزائن والملفات، ويحدد ذلك من خلال مصادر سرية لجهات الأمن.

3 ـ تحديد الأجهزة المحتمل تورطها في الجريمة الماسة بالمعطيات الرقمية، حتى يتم تحديد كيفية التعامل معها فنيا قبل المعاينة، سواء من حيث الضبط أو التأمين أو حفظ الأوراق أو المستندات المتداولة.

4 ـ تأمين الأجهزة والمعدات التي سيتم الإستعانة بها في عمليات المعاينة سواء كانت الأجهزة صلبة أو لينة.

5 ـ إعداد الفريق المختص الذي يتولى المعاينة من الخبراء ورجال الضبط والأمن.

6 ـ إخطار الفريق الذي سيتولى المعاينة قبل تمامها بوقت كاف حتى يستعد من الناحية الفنية والعملية، وذلك لكي يضع الخطة المناسبة لضبط أدلة الجريمة حال معاينتها.

7 ـ تحديد البيانات والمهام والإختصاصات المطلوبة من كل عضو في فريق المعاينة كل على حدة ، وذلك حتى لا تتداخل الإختصاصات.

8 ـ إعداد خطة للمعاينة موضحة بالرسومات مع تمام المراجعة التي تكفل تمثيلها على الوجه الأمثل.

9 ـ أن تتم كل هذه الإجراءات وفق مبدأ المشروعية وفي إطار ما تنص عليه القوانين الجنائية.

10 ـ تأمين عدم إنقطاع التيار الكهربائي لأن معاينة الأجهزة وما بها من برامج وشبكات وأنظمة تشغيل لا جدوى منها في ظل عدم وجود التيار الكهربائي.

الفرع الثاني: مفهوم الدليل الإلكتروني في الجرائم الماسة بالمعطيات الرقمية.

بعد أن أصبح المجتمع المعلوماتي حقيقة واقعة ، و تعتمد المجتمعات المعاصرة في تسيير شؤونها على تقنيات الحاسبات و المعلومات ومن ثم يتعين على أجهزة العدالة الجنائية ، مع تقلص الدور التقليدي للوثائق في الإثبات ، و ازدياد مطرد في كم المعلومات المنتجة أو المعروضة في أوعية ـ لا ورقية مستخدمة ـ أن تتعامل في ممارستها لحق المجتمع في الدفاع عن كيانه ضد الإجرام مع أشكال مستخدمة في الأدلة غير المادية ، و ذلك في مجال الإثبات الجنائي و هو ما يفرض على الفكر الشرطي من جهة أن يسعى دوما لتطوير أساليب كشف المعلومات و الوسائل المستخدمة في عمليات البحث الجنائي ، والتحقيق و هو ما يتطلب برامج تخصصية في التدريب لاكتساب هذه المهارات في أعمال الإستدلال و التحقيق لجمع الأدلة في الجرائم الماسة بالمعطيات الرقمية و تحديثها على نحو يكفل استجابتها بشكل كاف ، ودون أن تتعرض حقوقهم و حرياتهم للخطر عند الإثبات في مجال الجريمة الماسة بالمعطيات التي لا تعترف بالمكان من حيث آثارها و تستعصي على القواعد التقليدية في قانون الإجراءات الجزائية[1].

كما أن استخلاص دليل الإثبات يكون بالتأكيد على ضرورة مسارعة رجال الإستدلال و التحقيق بتطوير وسائلهم البحثية و قدراتهم العلمية ، وليس بالضرورة أن يكون المحقق خبيرا في الحاسب الآلي و إنما لا بد له من الإلمام ببعض المسائل الأولية التي تمكنه من التفاهم مع خبراء الحاسب الآلي و حسن إستغلالهم في كشف الجرائم و جمع الأدلة ، كما أنه من الضروري أن يكون المحقق ملما بالإجراءات الإحتياطية التي ينبغي اتخاذها نحو مسرح الجريمة و التدابير اللازمة لتأمين الأدلة.

[1] ـ خيرت علي محرز، المرجع السابق، ص11

كذلك فقد تظهر مشكلات إستخلاص الدليل لصعوبات تتعلق بحجم و كم البيانات المتعلقة بهذه الجريمة من حيث ضخامتها ومن حيث سهولة تدميرها ، إذ يكفي بضغط زر واحد محو كم هائل من المعلومات قد ينطوي على الجريمة المعلوماتية ككل ، وذلك في جزء من الثانية وهو كل وقت الجريمة[1].

أولا: تعريف الدليل الإلكتروني.

عرف البعض الدليل بأنه الواقعة التي يستمد منها القاضي البرهان على إثبات إقتناعه بالحكم الذي ينتهي إليه[2].

وعرف البعض الأخر الدليل بأنه: الحجية التي تستخلص من واقعه أو ظاهرة مادية أو معنوية لإسنادها إلى المتهم أو نفى ذلك.

ـ الدليل الجنائي: في مرحلة المحاكمة هو الحجية القضائية الناشئة في نفس القاضي ووجدانه و التي تستخلص من واقعة أو ظاهرة أو حقيقة مادية أو معنوية متعلقة بالجريمة تقوده إلى الحقيقة الإجرائية بحيث يولد ظهورها على ساحة الإثبات لدى القاضي الإقتناع القضائي بوقوع الجريمة بأركانها القانونية أو واقعة من وقائعها أو أمر مرتبط بها أو متصل بها و إسنادها إلى متهم معين بذاته أو نفي ذلك[3].

ـ الدليل الإلكتروني: عرف بأنه الدليل الذي يجد له أساسا في العالم الإفتراضي و يقود إلى الجريمة.

وعرف أيضا بأنه: المأخوذ من أجهزة الكمبيوتر وهو يكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تجميعها و تحليلها باستخدام برامج و تطبيقات و تكنولوجيا خاصة وهي مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات و الأشكال و الرسوم و ذلك من أجل اعتماده أمام أجهزة إنفاذ و تطبيق القانون[4].

ـ الدليل الجنائي الرقمي: هي الأدلة التي تشمل جميع البيانات الرقمية التي يمكن أن تثبت أن هناك جريمة قد ارتكبت أو توجد علاقة بين الجريمة و المتضرر منها والبيانات الرقمية هي مجموعة الأرقام

[1] ـ خيرت علي محرز، المرجع السابق ،ص11، 12.
[2] ـ أحمد فتحي سرور، الوسيط في القانون الإجراءات الجزائية ، دار النهضة العربية ،الجزء الأول،1981 ،373.
[3] ـ خالد ممدوح إبراهيم، الجرائم المعلوماتية ، المرجع السابق، ص163.
[4] ـ خالد ممدوح إبراهيم،المرجع نفسه ، ص187.

التي تمثل مختلف المعلومات بما فيها النصوص المكتوبة ، والرسومات ، الخرائط ، الصوت ، أو الصور.

وعرف أيضا بأنه: هي معلومات يقبلها المنطق و العقل و يعتمدها العالم يتم الحصول عليها بإجراءات قانونية و علمية بترجمة البيانات الحسابية المخزنة في أجهزة الحاسوب و ملحقاته و شبكات الإتصال و يمكن إستخدامها في أية مرحلة من مراحل التحقيق و المحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بالجريمة أو الجاني أو المجنى عليه[1].

والدليل العلمي يخضع لقاعدة لزوم تجانسه مع الحقيقة كاملة و إذا كان الدليل العلمي له منطقه الذي يجب ألا يخرج عليه من حيث أنه يجب عدم تعارضه مع القاعدة العلمية السليمة ، فإن الدليل الإلكتروني له ذات الطبيعة إذ يجب ألا يخرج الدليل العلمي عما توصل إليه العلم الرقمي و إلا فقد معناه ، وعدم الخروج من متطلبات العلم الرقمي لا يعني أن هناك قواعد جامدة يرتبط بها الدليل الرقمي من حيث طبيعته العلمية ، وإنما يجب الأخذ في الإعتبار أن العلم الرقمي هو علم متطور جدا ، بل يجد ذاته في قدرته الكبيرة على التطور الذاتي المستمر ، سيما من حيث كونه لا يستجيب للقاعدة التقليدية.

2- الدليل الإلكتروني من طبيعة تقنية: الدليل الإلكتروني ليس بدليل مرئي يمكن فهمه بمجرد القراءة و يتمثل في بيانات غير مرئية لا تفصح عن شخصية معينة عادة ، هذه المشكلة بصفة خاصة بالنسبة لجرائم الإنترنت من الجرائم التي ترتكز على البريد الإلكتروني في ارتكابها إذ يكون من الصعب على جهات التحري تحديد مصدر المرسل[2]، و الطبيعة التقنية للدليل الإلكتروني تقتضي أن يكون هناك توافق بين الدليل المرصد و بين البيئة التي يعيش فيها ، سواء كانت الجريمة المرتكبة إحتيالا على بنوك المؤسسات المالية ، أو كانت الجريمة قذفا و سبا أو تشهيرا علنيا في حلقات النقاش أو القوائم التراسلية و غيرها ، وكذلك بثا و تداولا لصور و أفلام دعارة أطفال[3].

---

[1] - حيرت علي محرز ، المرجع السابق ، ص 24، 25، ولمزيد من التفصيل أنظر Dr .Kam wing :computer Fraude in the U .K the Picture .computer of security . Bulletin . Vol 9 nal 1986. P09

[2] - خالد ممدوح إبراهيم ، الجرائم المعلوماتية ، المرجع السابق، ص181.

[3] - Amanda Hooey .Analysis of the police and criminal evidence act sec 69/computer generates evidence wed journal of current legal issues UK.1996.issue 1.P2

3 ـ الدليل الرقمي متنوع و متطور: إن مصطلح الدليل الرقمي يشمل كافة أشكال و أنواع البيانات الرقمية الممكن تداولها رقميا ، بحيث يكون بينها و بين الجريمة رابطة من نوع ما و تتصل بالضحية على النحو الذي يحقق هذه الرابطة بينها و بين الجاني ، ويترتب على طبيعة الدليل الإلكتروني من حيث التعدد و التنوع نتيجة هامة وهي صعوبة الصول إليه ، وذلك نتيجة قيام كبرى المواقع العالمية على الإنترنت بإحاطة البيانات المخزنة على صفحاتها بسياج من الحماية الفنية لمنع التسلل للوصول غير المشروع إليها لتدميرها أو تبديلها أو الإطلاع عليها أو نسخها ، هذا من جهة ومن جهة أخرى يمكن للمجرم زيادة صعوبة عملية ضبط أي دليل يدينه و ذلك من خلال إستخدامه كلمات مرور بعد تخريب الموقع مثلا ، أو إستخدامه تقنيات التشفير.

4 ـ صعوبة التخلص من الدليل الرقمي: و هذه إحدى أهم خصائص الدليل الرقمي على الإطلاق ، بل إنه يمكن إعتبار هذه الخاصية ميزة يتمتع بها الدليل الرقمي عن غيره من الأدلة الأخرى ، فالأدلة التقليدية التي يعرفها القانون تجد قوتها أمام القضاء في مسألة التشريع بالحصول عليها ، وإذا كان الأمر كذلك بالنسبة للأدلة التقليدية فإن الحال غير ذلك بالنسبة للأدلة الرقمية ، ذلك إن موضوع التخلص من الدليل الرقمي باستخدام التخلص من الملفات في الحاسب الآلي أو الإنترنت لا تعد من العوائق التي تحول دون استرجاع الملفات المذكورة إذ تتوافر برمجيات من ذات الطبيعة الرقمية يمكن بمقتضاها إسترداد كافة الملفات التي تم إلغاؤها أو إزالتها[1].

ـ صعوبة إثبات الدليل الرقمي: يتميز الدليل العلمي بصعوبات جمة تعترض طرق إكتشافه و هو أن هذه الجرائم لم يكتشف منها إلا 01% فقط من الجرائم المرتكبة أما التي تم الإبلاغ عنها فلم تتعدى 05% وحتى القضايا التي طرحت على القضاء للفصل فيها لم تكن الأدلة فيها كافية للإدانة إلا في حدود الخمس.

ونظرا لحداثة هذه الجرائم فإن مسألة عدم فهمها حالت بين عملية إكتشاف الجريمة و إثباتها أمام القضاء ، على عكس الجرائم التقليدية، ففي الجرائم الماسة بالمعطيات الرقمية مثلا قد يكون الدليل هنا معلومات مرمزة و مشفرة من جهة وكذلك قلة خبرة جهات أجهزة العدالة الجنائية التي تتعامل مع هذه الجرائم من جهة أخرى.

[1] ـ خالد ممدوح إبراهيم ، الجرائم المعلوماتية ، ص 174.

ثانيا: صعوبة إثبات الدليل الإلكتروني في الجرائم الماسة بالمعطيات الرقمية.

1ـ قدرة الجاني على تدمير أدلة الإدانة:

من الأسباب الأساسية التي تقف وراء صعوبة إكتشاف الجرائم الماسة بالمعطيات الرقمية هي قدرة الجاني على تدمير الأدلة التي من الممكن أن تتخلف عن مثل هذه الجرائم و القدرة على تدمير الأدلة و إن كان يملكها الجاني في أغلب الجرائم متى سمحت له الفرصة و كان الوقت كافي لذلك ، إلا أن ما يميز الجرائم الماسة بالمعطيات الرقمية هي قدرة الجاني على تدمير الأدلة بوقت قياسي قد لا يستغرق أكثر من دقائق ، وربما بعض من أجزاء الثانية بحيث لا تتجاوز تلك الفترة عدد من الثواني، الأمر الذي يمكن على ضوئه القول بأن الجرائم الماسة بالمعطيات الرقمية شأنها شأن بقية الجرائم ذات الأدلة المادية حيث يتمكن الجاني في مثل هذه الجرائم أيضا من تدمير الأدلة.

ومن الوقائع العملية التي تؤيد ذلك ما قام به أحد الجناة بإدخال تعديل على نظام الحاسب ، حيث ضمنه وفي نطاق التعليمات الأمنية لحماية ما فيه من معلومات مخزنة برنامج مهمته محو هذه المعلومات بشكل تلقائي ، إذا ما تم اختراق نظام المعلومات من قبل شخص غير مرخص له ، كذلك ما قامت به عصابة إيطالية إخترقت أنظمة الحاسب الآلي ، و ذلك من خلال تصميمها جهاز يمحو تلقائيا آثار أي خطوات و تعديلات سابقة إستخدمته في اختراق نظم لحاسبات آلية خاصة بشركات معينة ، وفي جميع أنحاء العالم[1].

2ـ النشاط الإجرامي فيه لا يمكن رؤيته:

من العوامل الأخرى التي تساهم في صعوبة إثبات الجرائم الماسة بالمعطيات الرقمية كون النشاط الإجرامي الذي باشره الجاني لا يمكن رؤيته ، وهو الأمر الذي لا يمكن ضبطه ، وكونه كذلك يعود إلى أنه عبارة عن نبضات إلكترونية تسير عبر الأثير أو عبر أسلاك و فوق أنها نبضات إلكترونية فإنه لا يمكن رؤيتها لأنها غالبا ما تكون مرمزة و مشفرة ، و نجد أن من المناسب أن نبين أن التشفير غير الترميز ، فإذا يعني التشفير تحويل بيانات أو إرسالها إلى جهة محددة عبر وسيط ناقل ، بحيث لا يمكن لأي جهة غير الجهة المرسل إليها تفسير هذه البيانات المبهمة و استخلاص البيانات أو

[1] ـ محمد حامد مرهج الهيتي ، المرجع السابق، ص 213، و لمزيد من التفصيل أنظر عبد الفتاح بيومي حجازي، الدليل الجنائي و التزوير في الجرائم الكمبيوتر، دار الكتب القانونية، 2002،ص46.

المعلومات المفهومة منها ، فإن التمييز يعني عملية تحويل المعلومات من هيئة معينة إلى هيئة أخرى وفق نظام محدد لا يمكن فهمها إلا من خلال نظام يفك هذا الترميز ، وتحويله إلى أشكال و بيانات ومعلومات تظهر على الشاشة و يفهمها القارئ فبرنامج Word هو برنامج مرمز رقميا ، لذلك فهو يحتاج إلى برنامج على نفس النظام يقوم بفك ترميزه و تحويله إلى رموز مفهومة تظهر على الشاشة. لذلك فإن البرامج و المعلومات المخزنة فيه لا يمكن للإنسان أن يراها و بالتالي لا يستطيع أن يقرأها[1] فهي معدة من أجل أن تقرأها الآلة فقط ، وتظهر على شاشة الحاسب الآلي على شكل معلومات مقروءة لذلك يكون من الممكن للمجرم ألا يتم إكتشافه ، أي لا تكتشفه أيدي العدالة لأنه من جانب لا يترك أثرا ، لقدرته على تدمير آثار جريمته ، ومن جانب آخر أن ما يتركه من آثار ،إن ترك طبعا ، لا يمكن مشاهدتها ، و لا يمكن قراءتها لمعرفة أو للتعريف على ما تم من فعل.

3 ـ قلة خبرات السلطات المسؤولة عن ضبط الجرائم و التحقيق فيها:

المعلوم أم متطلبات العدالة الجنائية و تبيان الحق تفرض على الأجهزة الحكومية بشكل عام و الأجهزة المسؤولة عن تتبع الجرائم و ضبطها و التحقيق فيها بشكل خاص أن تتحمل مسؤولياتها نحو كشف المجرمين و ضبطهم و محاكمتهم ومثل هذا الأمر يقتضى أن تتوفر الإمكانيات التقنية اللازمة ، سواء في عملية التحقيق ، أو الكشف و الإستدلال عن الجرائم ، لا سيما بعد أن تطورت ليس فقط أساليب الكشف عن الجرائم ، و إنما أيضا تطورت أساليب إرتكاب الجرائم و ظهور أنماط جديدة من الجرائم ما كانت التشريعات لتعرفها من قبل ، إلا بعد أن ظهرت وسائل متطورة تمكن المجرمين من ارتكاب جرائمهم بأساليب وطرق غير معهودة لرجال السلطة العامة كالموضوع الذي بين أيدينا[2].

لذلك و بما أن جرائم الماسة بالمعطيات الرقمية تتميز بخصائص فنية سواء بالنسبة لأشخاص مرتكبيها ، أو بالنسبة للموضوع الذي ترد عليه ، فإن توفر الإمكانيات التقنية في التحقيق أو الإستدلال عن هذه الجرائم سيكون أكثر حاجة فيها من غيرها من الجرائم ، لذلك فإن القصور في توفير هذه الوسائل و الإمكانيات من شأنه أن يؤدي إلى صعوبة في اكتشاف هذه الجرائم إن لم يكن عدم ضبطها لعدم اكتشافها أصلا ، إذ ما يزيد من صعوبة إكتشاف هذه الجرائم ، هو قلة خبرة سلطات التحقيق ، بل و الغالب إنعدام تلك الخبرة لدى القائمين بالبحث عن الجرائم ، إلى جانب إنعدام أو قلة

[1] ـ محمد حامد مرهج الهيتي، المرجع السابق ، ص 215.
[2] ـ محمد حامد مرهج الهيتي، المرجع نفسه ، ص 215.

الوسائل و الإمكانيات لدى تلك الجهات إن توافر الكادر الفني سواء في البحث عن هذه الجرائم و ضبطها أو في التحقيق فيها لذلك هناك و في سبيل تذليل هذه الصعوبة من يقترح ضرورة إستقطاب و جذب الكفاءات المهنية المتخصصة في هذا المجال للإستعانة به في تحقيق هذه الجرائم و ضرورة الإستعانة بالنخبة المتخصصة في الحاسب الآلي لضبط هذه الجرائم و اكتشفاها ، وتقديم أدلة الإدانة فيها ، و تولي شرح هذه الأدلة و أبعادها أمام المحاكم[1].

4 ـ عدم تخلف الآثار المادية كما هو الأمر في الجرائم التقليدية:

في الجرائم التقليدية ذات النتيجة بمدلولها و التي يصطلح على تسميتها بالجرائم المادية كجرائم القتل مثلا ، يكون دليل الإثبات فيها مرئيا ، ذلك لأنه يتخلف عن ارتكابها آثار يمكن إدراكها بالحواس كنتيجة للوسائل التي يستخدمها الجاني فمن الممكن مشاهدة الجروح التي على جسم المجنى عليه.

أما في الجريمة الماسة بالمعطيات الرقمية ، أو المعلوماتية فإن الأمر مختلف ، فمن حيث الوسيلة التي ترتكب بها هذه الجرائم فإنها يتم ارتكابها عن طريق نقل المعلومات على شكل نبضات إلكترونية غير مرئية تنساب عبر أجزاء الحاسب الآلي و شبكة الإتصال العالمية ـ الإنترنت ـ بصورة آلية ، كما ينساب الكهرباء عبر الأسلاك ، أو أن يتم نقلها بالإشعاعات و غالبا ما يتم هذا عن طريق وحدات طرفية بعيدة بل ربما تكون هذه الوحدات لا سلكية الإتصال مما يصعِّب ضبطها ، بل أن هذه الجرائم يمكن ارتكابها عن طريق الهاتف إذ يمكن ذلك عن طريق إصدار تعليمات للحاسب الآلي ، ومن مسافات بعيدة قد تتعدى نطاق إقليم الدولة مما يزيد أمر اكتشافها صعوبة إلى صعوبتها[2].

بعد التطرق إلى صعوبة إثبات الدليل الإلكتروني حاولنا دراسة حجية الدليل الإلكتروني في التشريعات ثم موقف المشرع الجزائري من حجية هذا الدليل.

ثالثا: حجية الدليل الإلكتروني في إثبات الجرائم الماسة بالمعطيات الرقمية.

1 ـ موقف المشرع الجزائري من حجية الدليل الإلكتروني :

لم ينص المشرع الجزائري صراحة على قبول الدليل الإلكتروني ، وهذا على الأساس يمكن الإعتماد على نص المادة 212 من قانون الإجراءات الجزائية الذي ينص على مبدأ حرية الإثبات في المواد

[1] ـ محمد حامد مرهج الهيتي، المرجع السابق ، ص216 ،كذلك أنظر عبد الفتاح بيومي حجازي ، المرجع السابق ، 37
[2] ـ محمد حامد مرهج الهيتي، المرجع نفسه ،ص 213،214

الجنائية تطبيقا لنظام الإثبات الحر ، حيث يقابله نص المادة 427 قانون الإجراءات الفرنسي الذي ينص على ما لم يرد نص مخالف يجوز إثبات الجرائم بجميع طرق الإثبات ، ويحكم القاضي بناء على إقتناعه الشخصي ، وفي المقابل ينص قانون الإجراءات يجواز إثبات الجرائم بأي طريق من طرق الإثبات ماعدا الأحوال التي نص فيها القانون على خلاف ذلك ، و للقاضي أن يصدر حكمه وفقا لاقتناعه الخاص ، ولا يصوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات و التي حصلت المناقشة فيها حضوريا أمامه[1].

ومن جهة أخرى يأتي إدراج المشرع لهذه المادة ضمن الأحكام المشتركة بطرق الإثبات ، مما لايدع مجالا للشك في تطبيقها أمام كل الجهات القضائية ، و بالتالي إعتمد المشرع الجزائري نظام الإثبات الحر كأصل عام ونظام الإثبات المقيد كاستثناء[2]، وقد ساير المشرع الجزائري الإتجاه العالمي المساير نحو الاعتراف أكثر فأكثر بحجية الأدلة الإلكترونية على اختلاف أنواعها مثل الإثبات بالكتابة في الشكل الإلكتروني[3] ، و التوقيع و التصدي الإلكترونين[4].

كذلك نص المشرع الجزائري على مراقبة الإتصالات الإلكترونية وحفظ المعطيات المتعلقة بحركة السير و إلزام مؤدي الخدمات بحفظ الأدلة الإلكترونية و الإستعانة بكل شخص له مؤهلات لمساعدة الجهات القضائية المختصة[5].

يتبين لنا جليا أن المشرع الجزائري قد أخذ بحجية الأدلة الإلكترونية في الإثبات الجنائي ، نتيجة لانتشار الجرائم الإلكترونية بكافة أنواعها ، وقصد تحقيق الفاعلية في مكافحتها ، و هناك إتجاه دولي للإعتراف بحجية المراسلات الإلكترونية بمختلف أنواعها و الإعتراف بحجية الملفات المخزنة في النظم و مستخرجات الحاسوب و البيانات المسترجعة ، و حجية الملفات ذات المدلول التقني البحت و الإقرار بالإثبات بالكتابة في شكلها الإلكتروني و بصحة التوقيع الإلكتروني و تساويه في الحجية مع

---

[1] ـ أنظر المادة 212 من قانون الإجراءات الجزائية من القانون الجزائري ، القانون نفسه.

[2] ـ بوحليط يزيد ، السياسة الجنائية في مجال مكافحة الجرائم الالكترونية في الجزائر أطروحة دكتوراه ، كلية الحقوق ، قسم القانون الخاص، جامعة باجي مختار عنابة ، 2016، ص285.

[3] ـ أنظر المادة 323 مكرر 01 من الأمر رقم 75 – 58 المؤرخ في 26 – 09– 1975 و المتضمن القانون المدني و التي تنص على " يعتبر الإثبات بالكتابة في الشكل الالكتروني كالإثبات بالكتابة على الورق بشرط إمكانية التأكد من هوية الشخص الذي أصدرها و أن تكون معدة و محفوظة في ظروف تضمن سلامتها.

[4] ـ أنظر المادة 02 الفقرة الأولى من القانون رقم 15 ـ 04 يحدد القواعد العامة المتعلقة بالتوقيع و التصديق الالكترونيين الجريدة الرسمية رقم 06 الصادرة في 10، 02، 2015.

[5] ـ أنظر المواد 04 ـ 12 من القانون رقم 09– 04 المؤرخ في 05 ـ 08 ـ 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها ، ج، 47 المؤرخ في 16 ـ 08- 2009.

التوقيع الفيزيائي، و التخلي شيئا فشيئا عن أدلة قيود تحد من الإثبات في البيئة التقنية ومع كل هذا يجب مراعاة المبادئ و الشروط التي تحكم الأدلة الإلكترونية، كمبدأ المشروعية، ومبدأ وجوب مناقشة الأدلة ، وتأمين الدليل الرقمي ضد التلاعب إضافة إلى صحة الوقائع الواردة بالدليل[1].

2 ـ موقف التشريعات المقارنة من حجية الدليل الإلكتروني.

تناول عدد من التشريعات الدليل الإلكتروني و حدد حجيته في الإثبات الجنائي، في حين طبقت بعض التشريعات القواعد العامة في الدليل الإلكتروني ومن بين هذه التشريعات:

ـ موقف المشرع الايطالي: نص قانون الإجراءات الجنائية الايطالي على الأدلة المعلوماتية و طبق

القواعد العامة في الإثبات على الأدلة المعلوماتية إذ أعطى المشرع الايطالي الحرية للقاضي في قبول الأدلة[2] ، و منح المشرع الايطالي سلطة تقديرية للقاضي في قبول أي دليل لم ينص عليه القانون إذا اقتنع به ووجد أنه ملائم و يساهم في كشف الحقيقة ، واشترط القانون أن تكون الأدلة مشروعة أي تم الحصول عليها بصورة قانونية ، وأعطى الحق للأطراف بتقديم أدلتهم و تخضع هذه الأدلة أيضا للسلطة التقديرية للقاضي[3].

كما نص المشرع على أنها:

ـ تقبل الأدلة بناءا على طلب الأطراف و يتخذ القاضي القرار بدون تأخير و يستبعد الأدلة المحظورة من القانون وتلك التي تبدو تافهة أو عديمة الأهمية.

ـ يحدد القانون الحالات التي يجوز فيها للقاضي قبول الدليل من تلقاء نفسه.

ـ يجوز إلغاء القرارات الصادرة بقبول الدليل بعد سماع الأطراف في الخصومة[4].

و أجاز القانون قبول الأوراق المكتوبة أو الوثائق الأخرى التي تمثل وقائع أو تشير إلى أشخاص مسجلة عن طريق التصوير الفوتوغرافي أو السينمائي ، أو أية وسيلة أخرى وذلك إذا تلفت الوثيقة

---

[1] ـ بوحليط يزيد، المرجع السابق، ص 285 ،286

[2] ـ نصت المادة 189من القانون الإجراءات الجنائية الايطالي رقم 447 لسنة 1988على أنه للقاضي عند طرح دليل لا ينظمه القانون ، الأخذ به إذا تبين أنه ملائم لضمان التحقيق من الوقائع و لا يؤثر على حرية الإرادة ، و يعمل القاضي على قبول الدليل بعد سماع أقوال الأطراف حول طرق الحصول عليه.

[3] ـ سامي جلال فقي حسين، المرجع السابق، ص229

[4] ـ أنظر المادة 190 من قانون الإجراءات الجنائية الايطالي ، القانون نفسه.

الأصلية لأي سبب من الأسباب أو ضاعت أو سرقت و لم يكن من المستطاع استعادتها جاز استخدام صورة لها[1] ، كما أكد في نص المادة على قبول الوثائق التي تشكل الجريمة بأنه : يجب قبول الوثائق التي تشكل جسم الجريمة[2].

ومن خلال ما تقدم يمكن تبيُّن القواعد العامة للإثبات التي جاء به القانون الايطالي و ذلك لعدة أسباب منها أن المشرع الايطالي ترك الحرية للقاضي في تقدير الدليل أي منحه السلطة التقديرية الواسعة في الأخذ بالدليل من عدمه ، كما أجاز لأطراف الدعوى تقديم الأدلة التي لديهم و التي سيدرسها القاضي و يتخذ القرار بقبولها أو رفضها ، كذلك أجاز القانون قبول الأوراق المكتوبة أو الوثائق الأخرى التي تم الحصول عليها عن طريق التصوير أو أية وسيلة أخرى ، و هذه العبارة يمكن أن تندرج ضمنها الأدلة المعلوماتية المفرغة على ورق أو المسجلة على أقراص مغناطيسية أو أية دعامة خزن أخرى[3].

2 ـ موقف المشرع الألماني: أما قانون الإجراءات الجنائية الأماني فلم يورد نصا يحدد حجية الأدلة المعلوماتية ، وبالتالي تطبق القواعد العامة في الإثبات الجنائي الواردة في القانون ، وقد نص القانون على أنه تفصل المحكمة فيما يتعلق بالأدلة المقدمة وفقا لاقتناعها الحر تبعا للمناقشات في مجموعها ، وحدد القانون الألماني الأدلة التي يمكن للمحكمة قبولها حسب قناعتها ، وهي الإعتراف و الشهادة ، وتقارير الخبراء ، والمعاينة ، والمستندات ، وعلى الرغم من أن القانون الألماني قد حدد الأدلة إلا أن القضاء الألماني يميل إلى التوسع في قبول الأدلة فقد قبل الشهادة المسموعة بشرط تعزيزها بأدلة أخرى إلا أن المستندات التي اعتبرها القانون أدلة إثبات جرى تحديدها على وجه العموم و لم تحدد ما هي تلك المستندات التي يمكن قبولها ، لذلك أعطى القانون الألماني للقاضي الجنائي الحرية في قبول الأدلة و يمكن قبول الأدلة المعلوماتية إذا تم تفريغها على الورق فتقبل كأية مستندات عادية[4].

3 ـ موقف المشرع المصري: لم ينص المشرع المصري على الدليل الإلكتروني و بالرجوع إلى القواعد العامة في الإثبات الجنائي الواردة فيه يلاحظ أنه ينص على أنه يحكم القاضي في الدعوى حسب العقيدة التي تكون لديه بكامل حريته ومع ذلك فلا يجوز أن يبني حكمه على دليل لم يطرح أمامه في الجلسة ، كما نص على أن للمحكمة أن تأمر و لو من تلقاء نفسها أثناء نظر الدعوى بتقديم أي دليل

[1] ـ أنظر المادة 234 الفقرة 01، 02 من قانون الإجراءات الجزائية الإيطالي.القانون السابق.
[2] ـ أنظر المادة 235 من قانون الإجراءات الجزائية الإيطالي.القانون السابق.
[3] ـ سامي جلال فقي حسين ، المرجع السابق ، ص 300.
[4] ـ سامي جلال فقي حسين ، المرجع نفسه ، ص301.

تراه لازما لظهور الحقيقة ، ويتبن أنه يمكن تطبيق القواعد العامة للإثبات في قانون الإجراءات الجنائية المصري على الأدلة المعلوماتية و تخضع هذه الأدلة للسلطة التقديرية للقاضي في الأخذ بالدليل أو رفضه.

المطلب الثاني: دور الشهادة والخبرة في إثبات الجرائم الماسة بالمعطيات الرقمية.

إن الشهادة في مجال الجريمة الرقمية لا يختلف من حيث ماهيتها عنها في الجريمة التقليدية ، و أمر سماع الشهود متروك لفطنة المحقق ومرتبط بظروف التحقيق ، و بما أن الشهادة من أقدم و سائل الإثبات كان لزاما الرجوع إليها حتى في هذا النوع من الجرائم ، كما تعاظم دور الإثبات العلمي للدليل مع ظهور الجرائم الرقمية ، و ضرورة اشتقاق الأدلة الرقمية المطلوبة للإثبات في هذه الجرائم و كشف أنماط الجرائم المرتكبة بإستخدام الحاسب الآلي ، وهو الدور الذي يضطلع به الخبراء القضائيون فأصبح إنشاء المعامل الجنائية مطلبا ملحا لفحص الأدلة الرقمية ، و لتقييم عملية الإثبات الرقمي و تحليل الجرائم في نطاق ما يعرف باسم نظم الخبرة الأمنية ، ونظرا لحداثة الجرائم الرقمية فإنها لم تأخذ القدر الكافي من الشرح و تقنين إجراءات إثباتها ، سواء من الناحية القانونية أو الفنية وهو ما ألقى على عاتق المعنيين بكشف و تحقيق هذه الجرائم عبئا ثقيلا ، حيث تلعب الخبرة القضائية دورا مهما في إثبات هذه الجرائم فهي تنير الطريق للقاضي الذي يهتدي به لتحقيق العدالة[1].

و قد قسمنا هذا المطلب إلى فرعين تناولنا في الفرع الأول دور الشهادة في إثبات الجرائم الماسة بالمعطيات الرقمية ، وفي الفرع الثاني: دور الخبرة في إثبات الجرائم الماسة بالمعطيات الرقمية.

الفرع الأول: دور الشهادة في إثبات الجرائم الماسة بالمعطيات الرقمية.

الشهادة في إطار القاعدة الجنائية هي إدلاء الغير ـ الشهود ـ بأقوالهم عن وقائع ترتبط بالجريمة موضوع الإجراء الجنائي ، فهي بحسب الأصل أقوال يدلي بها الشهود تبين كيفية حدوث ما يؤدي إلى القول بتكامل (شهود إثبات) أو عدم تكامل (شهود نفي) أركان للجريمة ، و الأقوال التي يدلي بها الغير ليست محل رأي أو معتقد شخصي ، وإنما مصدرها حقيقة ما ، لذلك يتفق الفقه و القضاء على

[1] ـ عبد الناصر محمد محمود فرغلي ، محمد عبيد سيف سعيد المسماري ، الإثبات الجنائي في الأدلة الرقمية من الناحيتين القانونية ، و الفنية ، دراسة تطبيقية ومقارنة ، الرياض ، 2008، ص23.

أن إدلاء الشاهد بشهادته إنما هو تقرير لما يكون قد رآه أو سمعه بنفسه أو أدركه على وجه العموم بحواسه ، لذلك قيل أن الشهود هم عيون القضاء و آذانهم.

وتعد الشهادة من أقدم و أبرز وسائل الإثبات و الحصول على الأدلة حتى أنه يكاد لا يخلو منها تشريع إجرائي على مدار تاريخ القانون الجنائي ، وتتنوع الشهادة بحسب الجهة التي يتم الإدلاء بها أمامها، وهذا التنوع ليس له تأثير على قناعة محكمة الموضوع في نظام التنقيب و التحري حيث ، يملك القاضي صلاحية كبيرة في بناء قناعته بحسب ما يرتئيه و يتوافق مع ما هو مقرر في أوراق الدعوى[1] . لذلك سنتناول في هذا الفرع : تعريف الشهادة ، الشهادة في الجرائم الإلكترونية ، الشهادة الإلكترونية عن بعد ، الشاهد الإلكتروني ، إلتزامات الشاهد المعلوماتي.

1 ـ تعريف الشهادة:

الشهادة في الأصل هي إخبار الشخص بما يكون قد رآه أو سمعه بنفسه أو أدركه على وجه العموم بحواسه ، ومن ثم فإن الشهود يعتبرون دليل مباشر في الدعوى ، و الشهادة بمفهومها التقليدي قد تكون معلومات ناتجة عن إستعمال الشخص لحواسه ، مثل إستعمال حاسة السمع فقد تأتي الشهادة نتيجة سماع الشخص لأقوال صدرت عن شخص آخر ، وقد تكون ناتجة عن حاسة البصر كأن يشاهد الواقعة التي يدلي عنها الشاهد ، وعلى العموم فإن ذلك كله يرجع إلى تقدير قاضي الموضوع في الأخذ بهذه الشهادة أو عدم الأخذ بها.

2ـ الشهادة في الجرائم الإلكترونية:

تعد شهادة الشهود في نوعية الجرائم المرتكبة عبر الإنترنت ، أو تلك الناتجة عن الحاسوب عامة ،

من الأدلة الهامة التي يمكن تقديمها للمحكمة ، لكونها عاملا حاسما يمثل منطق التعامل مع نوعية هذه الجرائم ، فقيام أحد العاملين في أحد الشركات مثلا بالإدلاء بأقوال محددة ، وإن كانت تتخذ صفة العمومية أثناء التحقيق في موضوع آخر يمكن أن يكون ذو دلالة في هذا الشأن ، كما حدث في قضية Broderbund التي شهد فيها الشهود بأن مبرمجي **يونيسون** قد طلب منهم نسخ برمجية **برودرلاند** إلا أنهم قاموا بذلك بإهمال ، ففي جرائم العدوان على حقوق المؤلف فإن الشهادة التي تصلح أن تكون صادرة عن العاملين الذين تم تكليفهم بالقيام بارتكاب النسخ غير المشروع ، إذ يمكن مثلا أن

[1] عبد الأحد جمال الدين ، المرجع السابق ، ص 949.

يتولى النسخ أحد المهندسين العاملين في الشركة التي تتولى العدوان على حقوق المؤلف ، مثل السماح لمتخصص في نسخ أجزاء من برمجية لكي يتم رصدها في برمجية أخرى ، ففي جرائم العدوان على حقوق المؤلف فإن الشهادة التي تصلح يمكن أن تكون صادرة عن العاملين الذي تم تكليفهم بالقيام بارتكاب النسخ غير المشروع ، إذ يمكن مثلا أن يتولى النسخ أحد المهندسين العاملين في الشبكة التي تتولى العدوان على حقوق المؤلف ، مثل السماح لمتخصص في نسخ أجزاء من برمجية لكي يتم رصدها في برمجية أخرى [1].

3ـ الشهادة الإلكترونية عن بعد:

إن مصطلح الشهادة الإلكترونية يطلق على نوعية من الشهادة لا يكون فيها الشاهد حاضرا جلسة التحقيق (الإبتدائي أو النهائي) بذاته المادية ، أي جسديا ، وإنما تتم عبر وسائل إلكترونية أو رقمية و يثار التساؤل حول مدى قابلية و صحة مثل هذه الوسائل لعرض الشهادة أمام سلطات الإستدلال و التحقيق؟

يجب التمييز بين نوعين من أنواع إستخدام الوسائل الإلكترونية للقول بصحة الشهادة ومن ثم قبول ما ينتج عنها من أدلة:

أولا ـ حالة الشهادة المسجلة: وهي الحالة التي تكون فيها الشهادة قد تم تسجيلها في تاريخ سابق ، بحيث يمكن عرضها فيما بعد على محكمة الموضوع في التحقيق النهائي الذي تجريه في الجلسة ، و في هذه الحالة فإن محاجة الشاهد في شهادته المذكورة في الأوراق يمكن ردها باستحضار مثل هذه التسجيلات و مواجهته بها ، وفي حالة تعذر فيها سماع الشاهد لأي سبب من الأسباب كأن يكون الشاهد في حالة هروب أو إصابة لاحقة بعيب عقلي مطلق ....إلخ ، مع ما يشمل ذلك في حالة قيام الشاهد بتغيير شهادته في المحكمة ، و يشمل ذلك غياب الشاهد عن حضوره جلسة التحقيق النهائي[2].

و تستخدم سلطات التحقيق أسلوب تسجيل الشهادة و الإدلاء بالأقوال عموما ، لكونه يشكل ضمانة أساسية في عدم وجود إكراه من أي نوع ، ويمكن أن يكون واقعا على المتهم ومن ثم صحة ما يمكن أن يدعي بعدم صحة ما نسب إليه من أقوال ، و يمكن القول إجمالا أن حالة الشهادة المسجلة تتفق

[1] ـ عبد الأحد جمال الدين ، المرجع السابق ، ص 950، 951.
[2] ـ عبد الأحد جمال الدين ، المرجع نفسه ، ص 955.

تماما مع ما هو مقرر في قانون الإجراءات الجزائية إذا ما تم التوصل إلى تفسير لغوي موسع أو في أقصى الأحوال تعديل بعض المصطلحات بحيث يمثل الأمر في النهاية إعادة صياغة فقط لما هو موجود ، ومما يثبت هذا القول أن المحاكم تتولى في العادة تحصيل التفسير الملائم للعبارات الإجرائية بما يتلاءم مع حقوق الإنسان و يحقق صالح المجتمع في الدفاع الإجتماعي ضد الجريمة.

ثانيا ـ حالة الشهادة الإلكترونية الفورية: و تفرض هذه النوعية من الشهادة حصولها في التحقيق النهائي أمام محكمة الموضوع ، حيث يكون فيها الشاهد غير حاضر جسديا أو ماديا في الجلسة ، إلا أنه توفرت الوسائل اللازمة التي يمكن من خلالها الحصول على أقواله بشكل سمعي مرئي.

و القضاء حتى مرحلة ظهور فكرة الدوائر الإتصالية المتكاملة كان يرفض بقوة إمكانية إحداث إتصال صوتي بين الجلسة و الشاهد ، فالقضاء الأمريكي مثلا يعتبر كل ما يمكن أن يصدر من شخص خارج جلسة نظر الدعوى من قبيل شهادة السامع التي لا تقبل البتة أمامه ، لأجل ذلك تقررت مواد إستدعاء الشاهد في قانون الإجراءات الجنائية و التي تصل إلى حد إقامة الجزاء على مخالفته أمر الحضور للمحكمة.

أما بعد ظهور فكرة الدوائر الإتصالية المتكاملة من مغلقة و مفتوحة ، فقد أثير مدى إمكانية قبول الشهادة الفورية عبرها و هو الأمر المقبول فقها ، سيما و أن الشاهد في الغالب من الأحيان يبرز في هيئته الكاملة في هذا الإطار، فيبدو كما لو كان حاضرا و تبرز مظاهر مصداقيته في ردة فعله الطبيعية حين تعرضه لأسئلة الدفاع أو الإتهام أثناء سير جلسة التحقيق[1].

4ـ الشاهد الإلكتروني:

يقصد بالشاهد في الجرائم الماسة بالمعطيات هو الفني صاحب الخبرة و التخصص في تقنية و علوم الكمبيوتر و الشبكات ، و الذي تكون لديه معلومات جوهرية أو هامة لازمة للولوج إلى نظام

[1] ـ عبد الأحد جمال الدين ، المرجع السابق ، ص 956 (لقد كانت بدايات الأخذ بنظام الشهادة الالكترونية الفورية في القضاء الأمريكي عندما واجه القضاء مشكلة إدلاء الشهادة من قبل أشخاص وضعوا في برنامج حماية الشهود ، فقد قررت المحكمة الفيدرالية العليا الأمريكية في 12،1، 1996،بتعديل تفسير المادة (43)من القواعد الفيدرالية للإجراءات المدنية بقبولها لنظام الشهادة الالكترونية بحيث يحق الأخذ بالشهادة عبر الدوائر المغلقة عن بعد طالما كانت هناك أسباب في القانون تدعو إليه ففي قضية استلزمت إدلاء شخص محصن ببرنامج حماية الشهود ، قام القاضي Jack B.Weinstein بتقرير قبول طلب الاتهام بسماع شاهد كان موضوعا في برنامج حماية الشهود .شريطة أن يكون حضور الشاهد عبر الدوائر المذكورة كما لو كان حاضرا الجلسة بالفعل ، حيث يكون كل ما يدور في الجلسة مرئيا له بالمقابل لرؤية من هو في الجلسة له).

المعالجة الآلية للبيانات إذا كانت مصلحة التحقيق تقتضي ذلك ، و يطلق على هذا النوع من الشهود مصطلح الشاهد المعلوماتي تمييزا له عن الشاهد التقليدي ، ويشمل عدة طوائف أهمها:

ـ **مشغلو الحاسب:** عامل تشغيل الحاسوب هو المسؤول عن تشغيل هذا الجهاز و المعدات المتصلة به و يجب أن تكون عنده خبرة في استخدام الجهاز ومكوناته مثل وضع القرص في وحدة الأقراص و استخدام لوحة المفاتيح في إدخال البيانات و كذلك إستخدام الطابعة ...إلخ وكذلك مشغلو الحاسب المتخصصين في إدخال البيانات إلى الحاسب وهم يقومون بنقل البيانات من الوثائق إلى وسط التخزين حتى تتم معالجتها بواسطة الحاسب و يجب أن تكون لديهم خبرة الكتابة السريعة على لوحة المفاتيح بالإضافة إلى الخبرة الفنية و الذكاء[1].

ـ **المبرمجون:** وهم الأشخاص المتخصصون في كتابة البرامج و يمكن تقسيمها إلى فئتين هما: أ/ الفئة الأولى ـ هم مخططو برامج التطبيقات: حيث يقوم مخطط برامج التطبيقات بالحصول عل خصائص و مواصفات النظام المطلوب من محلل النظام ثم يقوم بتحويلها على برامج دقيقة و موثقة لتحقيق هذه المواصفات.

ب/ الفئة الثانية ـ هم مخططو برامج النظم: حيث تقوم هذه الفئة باختبار و تعديل و تصحيح برامج نظام الحاسبة الداخلية أي أنه يقوم بالوظائف الخاصة بتجهيز الحاسبة بالبرامج و الأجزاء الداخلية التي تتحكم في وحدات الإدخال و الإخراج ووسائط التخزين بالإضافة إلى إدخال تعديلات أو إضافات لهذه البرامج.

ـ **المحللون:** المحلل هو الشخص الذي يحلل الخطوات و يقوم بتجميع بيانات نظام معين ، ودراسة هذه البيانات ثم تحليل النظام أي تقسيمه إلى وحدات منفصلة و استنتاج العلاقات الوظيفية من هذه الوحدات ، كما يقوم بتتبع البيانات داخل النظام عن طريق ما يسمى بمخطط تدفق البيانات و استنتاج الأمكان التي يمكن مكننتها بواسطة الحاسبة الإلكترونية.

ـ **مهندسو الصيانة و الإتصالات:** وهم المسؤولون عن أعمال الصيانة الخاصة بتقنيات الحاسبة بمكوناتها و شبكات الإتصال المتعلقة بها.

[1] ـ هلالي عبد اللاه أحمد ، إلتزامات الشاهد بالإعلام في الجرائم المعلوماتية ، دار النهضة العربية ، 1997، ص23.

ـ مديرو الصيانة: و هم الذين يوكل لهم أعمال الإدارة في النظم المعلوماتية[1].

هذا و يحصر قانون الدليل الخاص بولاية كاليفورنيا الأمريكية شهود الجريمة المعلوماتية في الآتي:

ـ محلل النظم الذي صمم وحدد برنامج الكمبيوتر الذي أنتج الدليل.

ـ المبرمج الذي قام بتحرير البرنامج و اختباره.

ـ المشغل الذي يقوم بتشغيل البرنامج.

ـ طاقم عمليات البيانات الذي يعد البيانات بالصور التي يستطيع الكمبيوتر قراءتها "شريط أو أسطوانة"

ـ أمناء مكتبة الأشرطة الذين يتحملون مسؤولية توفير الأشرطة و الأسطوانات التي تشتمل على البيانات و المعلومات المصدرية الصحيحة.

ـ مهندس الصيانة الإلكترونية الذي يقوم على صيانة الأجهزة الأصلية و التأكد من عملها بصورة صحيحة.

ـ موظفو المدخلات و المخرجات و المسئولون عن سرية عمل جهاز الكمبيوتر في تنفيذ برامجه.

ـ مبرمجو صيانة النظام و المسئولون عن سرية عمل جهاز الكمبيوتر في تنفيذ برامجه.

ـ المستخدم النهائي.

و الشاهد المعلوماتي عندما يقدم المعلومات التي لديه لا بد و أن يقدمها بأسلوب سهل و مفهوم حتى يكون بمقدور سلطات التحقيق فهم و إدراك تلك المعلومات ، كما يتعين عليه أن يتوخى التحديد و الدقة في المعلومات التي يقدمها أو يبلغها لسلطات التحقيق و التحري ، وذلك بأن يقدمها وصفا أو بيانا دقيقا و محددا للشيء محل الواقعة دون زيادة أو نقصان ، هذا بالإضافة إلى تحريه الصدق و الأمانة في المعلومات التي يقدمها ، فلا يقدم معلومات كاذبة أو مستندات مزورة أو يباشر عملا غير أمين في أجهزة الكمبيوتر من شأنه خداع أو تضليل رجال السلطة العامة أو جهة التحقيق[2].

[1] ـ هلالي عبد اللاه أحمد، إلتزامات الشاهد بالإعلام في الجرائم المعلوماتية، المرجع السابق، ص24.
[2] ـ خالد ممدوح إبراهيم، المرجع السابق،ص 266.

5ـ إلتزامات الشاهد الإلكتروني:

يتعين على الشاهد المعلوماتي أن يقدم إلى سلطات التحقيق ما يحوزه من معلومات جوهرية لازمة للولوج في نظام المعالجة الآلية للبيانات سعيا للبحث عن أدلة الجريمة بداخله ، والسؤال الذي يطرح نفسه هل يلتزم الشاهد بطبع الملفات و الإفصاح عن كلمات المرور و الشفرات؟.

هناك إتجاهان في هذا الصدد هما:

ـ الإتجاه الأول: ويرى أنه ليس من واجب الشاهد وفقا للإلتزامات التقليدية للشهادة أن يقوم بطبع ملف البيانات أو الإفصاح عن كلمة المرور أو الشفرات الخاصة بالبرامج المختلفة ، ويميل إلى هذا الإتجاه الفقه الجنائي الألماني حيث يرى عدم إلتزام الشاهد بطبع البيانات المخزنة في ذاكرة الحاسبة على أساس أن الإلتزام بأداء الشاهد لا يتضمن هذا الواجب ، كما أن في القانون التركي نص على أنه لا يجوز إكراه الشاهد لحمله على الإفصاح عن كلمات المرور السرية أو كشف شفرات تشغيل البرامج المختلفة[1].

ـ الإتجاه الثاني: و يرى أنصار هذا الإتجاه أنه من بين الإلتزامات التي يتحملها الشاهد القيام بطبع ملفات البيانات أو الإفصاح عن كلمات المرور أو الشفرات الخاصة بالبرامج المختلفة ، حيث يرى إتجاه في الفقه الفرنسي أن القواعد العامة في مجال الإجراءات الجنائية تحتفظ بسلطاتها في مجال الإجراءات المعلوماتية ومن ثم يتعين على الشهود من حيث المبدأ الإلتزام بتقديم شهادتهم ، ومن ثم يجب عليهم الإفصاح عن كلمات المرور السرية التي يعلمونها ، ولكن رفض إعطاء المعلومات المطلوبة غير معاقب عليها جنائيا إلا في مرحلة التحقيق و المحاكمة.

و في هولندا يتيح قانون الحاسبة الإلكترونية لسلطات التحري و التحقيق إصدار الأمر للقائم بتشغيل النظام لتقديم المعلومات اللازمة لاختراقه و الولوج إلى داخله ، كالإفصاح عن كلمات في داخله ، كالإفصاح عن كلمات المرور السرية و الشفرات الخاصة بتشغيل البرامج المختلفة ، و إذا وجدت بيانات مشفرة أو مرمزة داخل ذاكرة الحاسوب و كانت مصلحة التحقيق تستلزم الحصول عليها ، يتم تكليف القائم على تشغيل النظام المعلوماتي بحل رموز هذه البيانات.

[1] ـ على عدنان الفيل ، المرجع السابق ، ص 64 و لمزيد من التفصيل أنظر Erman (Sahir) les crimes infomatiques et d'autres crimes dans le domain de la technologies informatique en Torquie .R. I .D. P ,1993.P.64

و في اليونان يمكن الحصول من القائم على تشغيل نظام الحاسبة على كلمة المرور السرية للولوج في نظام المعلومات ، كما يمكن الحصول منه على بعض الإيضاحات الخاصة بنظامه الأمني لكن ليس على الشاهد أي التزام بالنسبة لطباعة ملفات بيانات مخزنة في ذاكرة الحاسبة و ذلك لأنه يجب أن يشهد على المعلومات التي حازها بالفعل و ليس عن معلومات جديدة[1].

يعتبر جوهر الإلتزام بالإعلام في الجرائم المعلوماتية أنه متى كان الشاهد المعلوماتي حائزا لمعلومات جوهرية لازمة للبحث عن الأدلة تتطلبها مصلحة التحقيق فإنه يكون مطالبا بأن يعلم بها سلطات التحقيق و التحري على سبيل الإلزام و إلا تعرض للعقوبات المقررة للإمتناع عن الشهادة[2].

الفرع الثاني: دور الخبرة في إثبات الجرائم الماسة بالمعطيات الرقمية.

يقوم المحقق الجنائي في مجال الكشف عن غموض الجريمة و فاعليتها باتخاذ الكثير من الإجراءات و الوسائل المتنوعة اللازمة لتحقيق هدفه ، ولما كان ذلك يحتاج إلى جهد لا يستطيع القيام به و تيسيرا عليه لأداء عمله مما اقتضى الإستفادة من أهل الخبرة و الإستعانة بهم ، ومنذ بدء ظهور الجرائم ذات الصلة بالحاسبة الإلكترونية ، تستعين الشرطة و سلطات التحقيق أو المحاكمة بأصحاب الخبرة الفنية المتميزة في مجال الحاسبة الإلكترونية ، وذلك بغرض كشف غموض الجريمة أو تجميع أدلتها و التحفظ عليها أو مساعدة المحقق في إجلاء جوانب الغموض في العمليات الإلكترونية الدقيقة ذات الصلة بالجريمة محل التحقيق ، حيث تكتسب الخبرة أهمية بالغة في مجال الجرائم الماسة بالمعطيات الرقمية كذلك فإن العلوم و التقنيات المتصلة بها تنتمي إلى تخصصات عملية دقيقة و متنوعة و التطورات في مجالها سريعة و متلاحقة لدرجة قد يصعب معها على المتخصص استيعابها و يمكن القول بصفة عامة بأنه لا يوجد حتى الآن خبير لديه معرفة معمقة في سائر أنواع الحاسبات و برامجها و شبكتها كذلك لا يوجد خبير قادر على التعامل مع كافة أنماط الجرائم التي تقع عليها أو ترتكب بواسطتها[3] و نظرا لأهمية الخبرة في هذا المجال سنتطرق إلى:

1ـ تعريف الخبرة:

يقصد بالخبرة ، بصفة عامة المهارة المكتسبة في تخصص معين سواء بحكم العمل في ذلك

[1] ـ على عدنان الفيل ، المرجع السابق ، ص 65

[2] ـ هلالي عبد اللاه أحمد ، التزام الشاهد بالإعلام في الجرائم المعلوماتية ، المرجع السابق ، ص 25.

[3] - Philipe M. Stanley computer crime investigation and investigators computer & security nort Holland , 1986 pp - 310 – 311.

التخصص لمدة زمنية طويلة أو نتيجة دراسات خاصة تلقاها أو نتيجة الإثنين معا أي العمل و الدراسة

أما الخبرة القضائية فهي إجراء للتحقيق يعهد به القاضي إلى شخص ينعت بالخبير ، تتعلق بواقعة أو وقائع مادية يستلزم بحثها أو تقديرها إبداء رأي يتعلق بها علميا أو فنيا لا يتوافر في الشخص العادي و لا يستطيع المحقق الوصول إليه وحده[1] ، و الخبرة هي الوسيلة التي من خلالها تستطيع سلطة التحقيق و المحكمة تحديدا التفسير الفني للأدلة بالإستعانة بالمعلومات العلمية ، فهي في حقيقتها دليل مستقل عن الدليل القولي أو المادي ، وإنما هي تقديم فني لهذا الدليل فهي في مجملها تقرير أو رأي فني صادر عن الخبرة في أمر من الأمور المتعلقة بالجريمة و عادة ما يطلق على الخبير في مجال جرائم الإنترنت ـ بالخبير الإلكتروني الرقمي ـ و لا يشترط في الخبير الكفاءة العملية في مجال التخصص فحسب بل يجب أن تضاف إليها سنوات من أعمال الخبرة في المجال الذي تميز فيه و على وجه الخصوص الجرائم ذات الصلة بالحاسب الآلي فقد يتعلق الأمر بتزوير المستندات أو التلاعب في البيانات أو بالغش أثناء نقل أو بث البيانات أو جريمة الأموال أو الإعتداء على حرمة الحياة الخاصة أو عرض صور أو أفلام مخلة بالآداب العامة[2].

و يحدد المحقق للخبير مهمته و الميعاد الذي يقدم فيه تقريره ، و الأصل أن يباشر الخبير عمله في حضور المحقق و تحت إشرافه و استثناءا أن يتم ذلك في غيابه ، وبعد الحصول على المستندات خلال عملية التفتيش يصبح الأمر سهلا حيث يمكن التعرف على بالرؤية و لن يحتاج المحقق لأي مساعدة من قبل الخبير و هذه المستندات مثل أدلة عمل النظام ، سجلات إدارة الحاسبة الإلكترونية ، وثائق البرامج ، السجلات ، صيغ مداخلات البيانات و البرامج ، وكذلك صيغ مخرجات الحاسبة الإلكترونية المطبوعة و يتم التخطيط على هذه المستندات و يمكن تحديد ما إذا كانت كاملة أصلية ، أو صورا من خلال استجواب القائمين على حفظها.

---

[1] ـ محمود جمال الدين زكي، الخبرة في مواد المدنية و التجارية، مطبعة جامعة القاهرة، 1990، ص11.

[2] ـ محمد أبو علاء عقيدة، التحقيق و جمع الأدلة في مجال الجرائم الالكترونية ، بحث علمي مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية و الأمنية للعمليات الالكترونية ، أكادمية شرطة دبي مركز البحوث و الدراسات ، العدد الأول ، الإمارات العربية المتحدة ، دبي ، 2003، ص 127 .

إن الخبرة التقنية في مجال الانترنت و العالم الافتراضي لا تشتمل بالضرورة تلك النوعية من خبرة الدراسة التي ينبغي التقرير بأن دراسات الحاسوب و الانترنت لا ترتبط بمنهج دراسي أو بحثي معين أو حتى مدة زمنية يقتضيها المرء دارسا في الجامعات و المعاهد المتخصصة ، و إنما ترتبط بمهارات خاصة و بموهبة استعمال الحاسوب و الانترنت و التعامل مع تقنية المعلومات ، إذ أن أمهر مبرمجي نظم التشغيل حتى الآن مثل BILL Gates لم يكن تحصيله العلمي يتجاوز المرحلة الثانوية ـ و ذات الأمر ينطبق على دعاة الهكرة و مخترقي الأنظمة فإن أعمارهم لا تتجاوز مرحلة التعليم الثانوي و السنوات الجامعية الأولي في أحسن الأحوال.

وقد يكون التخطيط على المواد المتعلقة بوسائل الحاسبة الإلكترونية الأخرى أمرا أكثر تعقيدا مثل الأشرطة الممغنطة ، الأسطوانات ، البرامج ، و يحتاج إلى معونة أحد الخبراء الموثوق فيهم حتى يتمكن المحقق من الإلمام بمحتويات الأشرطة أو الأسطوانات دون إحداث أي تغير فيها ، و بالطبع فإن البحث عن المعلومات داخل جهاز الحاسب الإلكتروني ذاته يعد أمرا بالغ التعقيد و يحتاج إلى وجود خبير[1].

2ـ الإستعانة بالخبراء في الجرائم المعلوماتية:

إن الإستعانة بالخبراء وفق المنهج التقليدي في الإجراءات الجنائية يرتبط في الحقيقة بمنطق تقليدي يجب أن يعتمده المشرع الجزائري بحيث يسمح بتجاوزه في إطار الجرائم الماسة بالمعطيات و ذلك فضلا عن قاعدة أنه ليس في القانون ما يمنع محكمة الموضوع من ندب خبراء غير مقيدين بجدول المحكمة فإن هذا التوجه القضائي يجب أن يتم تطويره لكي يمكن الإستعانة بخبراء في العالم الإفتراضي دون حاجة لإبداء أسباب في منطوقها للإستعانة بالخبراء من خارج الجدول ، على أن يشمل التطور إمكانية أن تكون الإستعانة بالخبراء ممتدا إلى أبعد من النطاق الإقليمي والمادي ممثلا في الحدود المادية بين الدول ويمكن أن يكون هؤلاء الخبراء في خارج الإقليم وهو أمر تسمح به مقومات العالم الإفتراضي كونه يعد بيئة إتصالية رقمية.

فيمكن مثلا الإستعانة بمراكز وهيئات ومؤسسات حكومية أو خاصة تعمل في بيئة تكنولوجيا المعلومات حيث كانت قصد استجلاء الغموض الفني في نظم الإنترنت ودون أن يكون ذلك مكلفا على النحو الذي يفترض حدوثه في العالم المادي وإنما كل ما يحتاج إليه هو توافر بيئة إتصالية رقمية بتكنولوجيا المعلومات والإنترنت فإذا كان توافر مثل هذه البيئة الرقمية أمكن استصدار تشريع يحقق المقصود القانوني من هذا النظام[2].

على أن الأمر هنا على درجة كبيرة من الأهمية تتعلق بالدراية الفنية للقائم بالتحقيق ، سيما حالة عدم وجود مثل هذه الدراية الفنية لديه بهذه النوعية من الجرائم ، فهل يجوز له الإستعانة المتواصلة بالخبير الرقمي طوال فترة التحقيق؟.

[1] ـ على عدنان الفيل ، المرجع السابق ، ص 29.
[2] ـ خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص292.

هذه المسألة على درجة من الخطورة حيث أن القائم بالتحقيق يتواصل عمله بعمل الخبير الذي يستعين به في كافة مراحل التحقيق فيظهر الأمر كما لو كان القائم بالتحقيق يستعين بخبير استشاري هنا ، في حين أن بعض التشريعات منحت المتهم صلاحية الإستعانة بخبير إستشاري.

كما منح القانون صلاحية التحقيق لغرفة الإتهام باعتبارها درجة ثانية من درجات التحقيق إذ تمتلك سلطات قاضي التحقيق بالإضافة إلى سلطاتها القانونية في مراجعة التحقيق الذي قام به قاضي التحقيق أو النيابة العامة ، ومن ثم يكون لها الإستعانة بالخبراء فضلا عن ذلك كله فإنه لما كان الأصل في القانون هو مرحلة التحقيق التي تتم في جلسة المحاكمة فإن محكمة الموضوع تعد السلطة الأصلية التي يمنحها القانون الحق في إجراء تحقيق في الجلسة[1].

3ـ أنواع الخبرة التقنية:

إن الإعتماد على الأسلوب الحكومي للتعامل مع ظاهرة الإنترنت سيما في إطار نظم الإثبات ، ليجعل من منطق المفاضلة و التبعية هو المنطق السائد ، ومثل هذا الأمر سوف يجعل الجريمة تتفوق على العدالة و أجهزتها بشكل يؤدي دون شك إلى سيادة منطق الجريمة و في ما يلي بيان لما أجمل:

أ/الخبرة الخاصة:

و هذه تعد أقوى أنواع الخبرات على الإطلاق لكونها تنطلق من مفهوم السعي إلى خلق فرص منافسة حقيقية بين المنضمات الخاصة و هي تضم في جنباتها الخبرة الفردية التي تعد من أقوى و أهم مظاهر الخبرة السائدة في مجال تكنولوجيا المعلومات و الإنترنت ، ويكفي هنا أن نذكر أن المؤسسات الكبرى المتخصصة في الكمبيوتر و الإنترنت تسعى بكل جهودها إلى الإستعانة بأشخاص بينوا كفاءاتهم في مجال الكمبيوتر و الإنترنت ، حتى عصاة القانون منهم فهناك إقتصادي يحاول جاهدا إثبات عدم جدوى التخلص من هؤلاء بمعاقبتهم وفقا للقانون و إنما يلزم اللجوء إلى الحلول الإقتصادية لكي يمكن أن يظلوا عاملين في إطار الأهداف الإقتصادية بل أن من الدول من تسعى جاهدة إلى محاولة التعرف على قراصنة تحولوا مع مرور الوقت إلى رموز وطنية جراء تحركاتهم عبر الإنترنت

[1] ـ خالد ممدوح إبراهيم، المرجع السابق، ص 293.

، و إلى جانب الأفراد توجد المنظمات الخاصة في كافة المحاولات و التي سوف يكون لها السبق في مجال الخبرة[1].

و تختلف المنظمات الخاصة ما بين منظمات أهلية تتصدى لكل محاولة من المجرمين بقصد التعدي على الحقوق الإلكترونية ، وبين نوعية من المنظمات التي تسعى إلى فك طلاسم العلم الإفتراضي على أسس تجارية ، فقد إستطاعت إحدى الشركات الأسكتلندية المتخصصة في برمجيات الحاسوب و الإنترنت من إعداد مشروع خريطة للعالم الإفتراضي على غرار الخريطة الجينية للإنسان ، فقد قام بإعدادها مجموعة من خبراء البرمجة الأسكتلنديين كانوا قد شرعوا في إعداد هذا العمل في عام 1998 و استغرق إعدادها ثمانية عشرة شهرا ، و لقد كان من أهم نتائج هذه الخريطة أن تمكنت الخبرة الخاصة من رصد حركة الجريمة عبر الإنترنت ومعرفة تطوراتها في كافة مظاهرها و أشكالها ، حيث برز أكثر من أربعين مظهر من مظاهر الإجرام عبر الإنترنت ، ولقد أمكن من خلال ما تم رصده في إطار خريطة الجريمة عبر الإنترنت إدراك الخبراء لوجود ما يربو عن مائتي ألف موقع جديد للدعارة عبر الإنترنت و لقد استفاد أهل الخبرة الخاصة من رصد هذه الخريطة في التعريف على التهديدات الحقيقية التي تواجه الدول و الأفراد ، مثلا عن إخفاء النصوص بإضافة نصوص أخرى حيث يعد ذلك من أخطر المشاكل التي تواجه العالم الإفتراضي فمثل هذه المشكلة تعد ثالث أخطر مشكلة تواجه النظام الأمني في الولايات المتحدة الأمريكية بعد العدوان البيولوجي و الكيمائي[2].

ب/ الجهات التعليمية:

لما كانت شبكة الإنترنت تعد أحد منتجات العلم في حركته التقنية فإنه يمكن القول و بحق أن أقوى مظاهر الخبرة التي يمكن الإستعانة بها لمواجهة الجريمة في العالم الإفتراضي يمكن أن تكون من خلال المؤسسات و الجهات التعليمية ، فهذه الأخيرة تعد مصدر دعم متكامل لمؤسسات الدولة ككل و

هذه المؤسسات تعتمد منهج علمي غير تجاري هدفها بالتأكيد تطوير العلم ليقضى على المشكلات التي تواجه البشرية ، كما أن التفكير العلمي لا يمكن تجنيه في رصده للظاهرة الإنسانية ، والإتجاه العالمي في رصد تطورات الجريمة عبر الإنترنت يتجه إلى المؤسسات العلمية بحيث يتم دعمها ماديا و معنويا ، لتكون أفضل سبل المواجهة ، و لقد قامت عدة مؤسسات تعليمية بتكوين قاعدة تتكون من

[1] ـ حسين سعيد بن يف الغافري، السياسة الجنائية في مكافحة جرائم الإنترنت، رسالة دكتوراه، كلية الحقوق، عين الشمس، 2005، ص 443.
[2] ـ عبد الأحد جمال الدين، المرجع السابق، ص 1036

مجموعة خبراء يتمتعون بخبرة كبيرة في مجال الجرائم المعلوماتية لتكون على أهبة الإستعداد لمواجهة الجريمة عبر الإنترنت ، و كذلك دراسة الكمبيوتر بشكل دقيق في الجامعات ومن ذلك جامعة ستانفورد بأمريكا ، كذلك معهد التكنولوجيا في ماساشوستس الذي قدم للبشرية خبراء على درجة عالية من التفوق[1].

ج/ جهات الضبط القضائي:

شرعت بعض الدول في إعداد أجهزة متخصصة للخبرة في الإجرام عبر الإنترنت و في الحقيقة هو نشاط تتزعم الولايات المتحدة الأمريكية فيه قائمة أجهزة الضبط القضائي في العالم ، بحيث تجاوز نشاطها في هذا المجال الإطار الوطني نحو الدولي المتمثل في منظمة الإنتربول أيضا ، وكان آخر نشاط مؤسسي في هذا الإطار هو ذلك الفرع الجديد الذي تأسس في المباحث الفدرالية الأمريكية FBI أطلق عليه المعمل الإقليمي الشرعي للحاسوب، ومقره سان دييجو، و الذي تم افتتاحه في نوفمبر 2000 وهو بمثابة بيت خبرة عام متعدد الإستشرات في النواحي القضائية غرضه مكافحة التصعيد الخطير في الجريمة عبر الإنترنت ، و ذلك بتحليل و تصنيف الدليل الرقمي بحيث يتم إعداد محللين شرعيين للحاسوب ليكون لهم أهمية كبرى في نطاق العمل على تكثيف مواجهة الجريمة عبر الإنترنت ، وبين تعدد النواحي التي يتعامل معها المعمل الشرعي الجديد الذي يتكون من إلتقاء العديد من منظمات الضبط القضائي تتعاون فيما بينها لكي تحقق الفائدة المرجوة منها مثل إدارة مكافحة المخدرات، ووحدة التحقيقات لمكافحة المجرمين ووحدة تحقيقات الجريمة في البحرية، ووحدة الجمارك و مكتب النائب العام للمقاطعة ومكتب حاكم المقاطعة و إدارة شرطة كاليفورنيا.

د/ التعاون الدولي: قد يكون مفيدا في هذا الإطار التعرض لمنطق التعاون الدولي في مجال الخبرة التقنية، و الحقيقة أن مجال التعاون الدولي إنما يعد تقريرا مسبقا بأهمية اللجوء إلى المنظمات الحكومية في الإطار الإقليمي إذ يكون بين الحكومات المعترف بها في هذا الشأن[2].

4ـ دور الخبير التقني في حفظ الأدلة الإلكترونية:

في إطار الجرائم الماسة بالمعطيات الرقمية نميز بين الأدلة التي يلزم التحفظ عليها داخل جهاز الحاسب الآلي و بين تلك التي يلزم بقائها في العالم الإفتراضي و بين تلك النوعية من الأدلة التي

[1] ـ حسين بن سعيد بن سيف الغافري، المرجع السابق، ص 453.
[2] ـ عبد الأحد جمال الدين، المرجع السابق، ص 1038، و ما بعدها.

تنتمي إلى العالم الرقمي ، و مع ذلك يمكن اللجوء إلى إخراجها في إطار الحاسوب و العالم الرقمي إلى العالم المادي بحيث يتم التعامل معها كمخرجات يقبلها القضاء كأدلة كاملة في الجريمة تساعد في الإدانة و كذلك في البراءة إن التحفظ على الأدلة داخل جهاز الكمبيوتر من العمليات المعقدة التي تحتاج بداية إلى رصد دقيق لمدى صحة البيانات التي يحتوى عليها الكمبيوتر ، و هذا الأمر يستلزم بالضرورة قيام الخبير التقني بالكشف بداية على المدى الذي تكون عليه صحة حركة الكمبيوتر سيما من حيث الخلل و العطب ، و يعطي العدوان الفيروسي مثالا حيويا هنا ، إذ يكفي أن يكون هناك فيروس في الجهاز لكي يتم التشكيك في صحة الأدلة المستفادة من هذا الكمبيوتر ، ومثال هذا الإتجاه نجده في التشريع الإنجليزي ، وتتم عملية حفظ الأدلة داخل جهاز الكمبيوتر بأساليب متعددة تتمثل في أبسط مظاهرها باستخدام أسلوب الحفظ العادي و أقوى مظاهرها في عمليات حجز الحاسوب على الدليل الموضوع فيه ذلك ، إن الدليل الرقمي هو في العادة ملف يحتوي على بيانات رقمية تعطي مظهرا معلوماتيا محددا غير قابل للتحويل إلى مظهر آخر بإجراء تعديلات رقمية في البيانات المذكورة[1].

أما بالنسبة لعملية حفظ الأدلة في العالم الرقمي فإنه يتطلب من الخبير التقني القيام برصد موقع الإنترنت أو المعلومات التي تشير إلى الجريمة و التي تكون في مظاهر مختلفة الأشكال ، كما لو كانت الجريمة من جرائم القذف و السب في غرف المناقشة ، ففي مثل هذه الحالة الأخيرة يتم اللجوء

إلى ذاكرة الخادم الذي يتولى ربط هذه الغرف عبر العالم الرقمي لكي يمكن التوصل إلى تحديد موضوع السب و القذف و تاريخه و إذا كانت الجريمة من جرائم النشر عبر الإنترنت فقد يكتفي بمجرد اللجوء إلى ذاكرة الحاسب الآلي المستخدم هنا دون حاجة إلى تحديد الخادم.

وفي مثل هذه الحالة يقوم خبير باستخدام برمجيات مساعدة للتوصل إلى القيام بالحفظ في العالم الرقمي ، كما هو الشأن في حجز و تشفير هذه المواقع بعد تحديد جديتها و دقتها ومسارها و هذا أمر يترتب عليه عدم إمكانية حذفها من العالم الرقمي ، وإذا قام أحدهم بذلك فإن ذلك يعد قرينة على أنه هو من ارتكب الجريمة ، و تستدعى عملية حفظ الأدلة في العالم الرقمي لزوم قيام الخبير بعرض الأدلة في المحكمة أو على جهات التحقيق ، ومثل هذا الأمر يجعل عمل الخبير يستمر لمرحلة

[1] ـ خالد ممدوح إبراهيم، فن التحقيق في الجريمة المعلوماتية، المرجع السابق، ص 309.

المحاكمة ، كما هو شأن حال عرض الدليل المقدم إلى محكمة الموضوع أمام جهة قضائية أعلى كالإستئناف أو النقض.

و درءا للمشكلات التي يمكن أن تنجم عن حفظ الأدلة في العالم الرقمي فإن العديد من المحاكم لجأت إلى ميكنة إدارتها رقميا ، حيث يتم تسليم الأدلة إلى إدارة متخصصة تتولى بدورها حفظ الأدلة في العالم الرقمي لعرضها على القضاء كلما تطلب الأمر ذلك[1].

[1] ـ خالد ممدوح إبراهيم ، المرجع السابق ، ص 310

المبحث الثاني: الجزاءات المقررة للجرائم الماسة بالمعطيات الرقمية.

إن الجرائم المعلوماتية تعد من الموضوعات الحديثة التي فرضت نفسها بقوة على المستوى الوطني والدولي على حد سواء ، والتي تطرح على المشرع الجنائي ضرورة مواجهتها بترسانة قانونية حاسمة ورادعة لمكافحتها وعقاب مرتكبيها.

لذلك قسمنا هذا المبحث إلى مطلبين: تناولنا في المطلب الأول: الجزاءات المقررة للشخص الطبيعي ، وفي المطلب الثاني الجزاءات المقررة للشخص المعنوي.

المطلب الأول: الجزاءات المقررة للشخص الطبيعي.

تنقسم العقوبات المقررة للشخص الطبيعي في الجرائم الماسة بالمعطيات الرقمية إلى عقوبات أصلية وأخرى تكميلية لذلك تناولنا في الفرع الأول: العقوبات الأصلية، و في الفرع الثاني: العقوبات التكميلية.

الفرع الأول: العقوبات الأصلية.

تختلف العقوبات الأصلية باختلاف الجريمة لكونها تضم في كل الحالات الحبس والغرامة ، وهذا على النحو الآتى:

أولا ـ العقوبات الواردة في قانون العقوبات

ـ العقوبة المقررة لجريمة الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات: يعاقب على هذه الجريمة في صورتها البسيطة أي على الدخول أو البقاء الذي لا يترتب عنه أي ضرر بالحبس أي كل من يدخل عن طريق الغش في كل أو جزء من المنظومة للمعاجة الآلية للمعطيات أو يحاول ذلك ، وتضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام تشغيل المنظومة تكون العقوبة الحبس[1] ، بينما تضاعف العقوبة على الجريمة في صورتها المشددة إذا ترتب عن الجريمة حذف أو تغيير لمعطيات المنظومة[2]، أو إذا ترتب عن الجريمة تخريب نظام إشتغال المنظومة.

[1] ـ يعاقب بالحبس من ستة أشهر إلى سنتين وبغرامة من 50.000 دج إلى 150.000 دج (أنظر المادة 394 مكرر الفقرة 1) من قانون العقوبات الجزائري.القانون السابق.

[2] ـ أنظر المادة 394 مكرر الفقرة 2 من قانون العقوبات الجزائري (الحبس من ثلاثة أشهر إلى سنة وبغرامة مالية من 50.000 دج إلى 100.000 دج).القانون السابق.

تضاعف العقوبات المنصوص عليها في هذا القسم إذا استهدفت الجريمة الدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للنظام العام دون الإخلال بتطبيق العقوبات الأشد ، فتتشدد العقوبة في جريمة الدخول والبقاء غير المشروع داخل النظام ويتحقق هذا الظرف عندما ينتج عن الدخول أو البقاء إما حذف أو تغيير للمعطيات التي يحتويها النظام وإما تخريب نظام إشغال المنظومة ففي الحالة الأولى تضاعف العقوبات المقررة في الفقرة الأولى من المادة 394 مكرر.

أما في الحالة الثانية فإن هذا الظرف المشدد هو ظرف مادي حيث يكفي أن يقوم الدخول أو البقاء غير المشروع.

ـ العقوبة المقررة لجريمة الإعتداء على المعطيات: يعاقب فاعل هذه الجريمة بالحبس[1] وتضاعف العقوبة إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام[2].

ـ العقوبة المقررة لجرائم التعامل غير المشروع في المعطيات: يعاقب فاعل هذه الجرائم بغض النظر عن صورها المحددة سابقا بالحبس[3] وتضاعف العقوبة إذا استهدفت الجريمة الدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام[4].

ثانيا ـ العقوبات الواردة في قانون التصديق والتوقيع الإلكترونيين.

كذلك يعاقب بالحبس كل أدلى بإقرارات كاذبة للحصول على شهادة تصديق إلكتروني موصوفة[5].
ويعاقب بالحبس[6]، كل مؤدي لخدمات التصديق الإلكتروني أخل بالتزام إعلام السلطة الإقتصادية بالتوقف عن نشاطه في الآجال المحددة.
كذلك يعاقب بالحبس[7]، كل من يقوم بحيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني موصوف خاصة بالغير[1].

---

[1] ـ من ستة أشهر إلى ثلاثة سنوات وبالغرامة من 500.000 دج إلى 2.000.000 دج (المادة 394 مكرر).القانون السابق.
[2] ـ أنظر المادة 394 مكرر1 من قانون العقوبات الجزائري (.تصبح ، الحبس من سنة إلى ستة سنوات والغرامة من 1.000.000 دج إلى 4.000.000 دج) القانون السابق.
[3] ـ من شهرين إلى ثلاثة سنوات وبالغرامة من 1.000.000 دج إلى 5.000.000 دج. من قانون العقوبات ، القانون نفسه.
[4] ـ تصبح الحبس من أربعة أشهر إلى ستة أشهر والغرامة من 2.000.000 دج إلى 10.000.000 دج من قانون العقوبات ، القانون السابق.
[5] ـ المادة 66 من القانون رقم 15-04 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين. (من ثلاثة أشهر إلى ثلاثة سنوات وبغرامة من 20.000 دج إلى 200.000 دج أو بإحدى هاتين العقوبتين) من قانون العقوبات ، القانون السابق.
[6] ـ من شهرين إلى سنة وبغرامة من 200.000 دج إلى 1.000.000 دج أو بإحدى هاتين العقوبتين فقط. من قانون العقوبات ، القانون السابق.
[7] ـ من ثلاثة أشهر إلى ثلاثة سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج أو بإحدى هاتين العقوبتين فقط. من قانون العقوبات ، القانون السابق.

ويعاقب بالحبس[2]كل من يخل عمدا بالتزام تحديد هوية طالب شهادة تصديق إلكتروني موصوف

، ويعاقب بالحبس[3] ، كل من يؤدي خدمات التصديق الإلكتروني للجمهور دون ترخيص أو كل مؤدي لخدمات التصديق الإلكتروني يستأنف أو يواصل نشاطه ، بالرغم من سحب ترخيصه.

ويعاقب بالحبس[4] كل شخص مكلف بالتدقيق يقوم بكشف معلومات سرية إطلع عليها أثناء قيامه بالتدقيق ، ويعاقب كل شخص يستعمل شهادته للتصديق الإلكتروني الموصوفة لغير الأغراض التي منحت من أجلها[5].

ثالثا: العقوبات المقررة في قانون حق المؤلف والجزائري والحقوق المجاورة.

كذلك يعاقب مرتكب جنحة تقليد مصنف أو أداء فني كما هو منصوص عليها في المادتين 151و152 أعلاه، بالحبس، سواء كان النشر قد حصل في الجزائر أو في الخارج[6].

و نفس القانون نص على أنه " يعد مرتكبا الجنحة المنصوص عليها....يستوجب العقوبة المقررة في المادة 153 أعلاه كل من يشارك بعمله أو الوسائل التي يحوزها للمساس بحقوق المؤلف أو أي مالك للحقوق المجاورة"[7].

ونص كذلك على أنه في حالة العود " تضاعف في العقوبة المنصوص عليها في المادة 153من هذا الأمر"[8].

وبناء على ما تقدم و بتحليل هذه المواد يتبن أن القاضي لا يملك السلطة التقديرية في فرض الغرامة مع الحبس وحده فقط، بل لا بد من الجمع بينهما، إلا أن هذا لا يمنع من القول بوجود سلطة تقديرية

---

[1] - أنظر المادة 67 – 68 من القانون رقم 15-04.القانون السابق.

[2]- من سنة إلى ثلاثة سنوات وبغرامة من 200.000 دج إلى 2.000.000 دج أو بإحدى هاتين العقوبتين من شهرين إلى ثلاثة سنوات وبغرامة من 20.000 دج إلى 200.000 دج أو بإحدى هاتين العقوبتين. من قانون العقوبات ، القانون السابق.

[3] - المادة 69 – 72 من القانون رقم 15-04.القانون السابق.

[4] - من ثلاثة أشهر إلى سنتين وبغرامة من 20.000 دج إلى 200.000 دج أو بإحدى هاتين العقوبتين فقط (المادة 73) من القانون رقم 15-04.

[5]- يعاقب بغرامة من 2000 دج إلى 200.000 دج (أنظر المادة 74 من القانون رقم 15-04). القانون السابق

[6] - أنظر المادة 153 من الأمر 03-05 الصادر بتاريخ 2003.07.19 المتعلق بحق المؤلف و الحقوق المجاورة المعدل و التمم للأمر 14/37

[7] - يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات و بغرامة مالية من 500.000 دج إلى 1.000.000 دج (أنظر المادة 154 من الأمر المتعلق بحق حماية المؤلف و الحقوق المجاورة من الأمر نفسه).

[8] - أنظر المادة 156 الفقرة الأولى من الأمر المتعلق بحق حماية المؤلف و الحقوق المجاورة من الأمر نفسه.

للقاضي في تحديد مدة العقوبة المتناسبة مع الفعل الإجرامي ، وهذه السلطة ليست مطلقة لأنها بدورها تخضع لرقابة المحكمة العليا[1].

رابعا- العقوبات الواردة في قانون حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

وفقا للقانون المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي فإنه ودون الإخلال بالعقوبات الأشد المنصوص عليها في التشريع الساري المفعول[2] ، يعاقب كل موظف لا يحترم الكرامة الإنسانية والحياة الخاصة والحريات العامة أو يتعدى على حقوق الأشخاص وشرفهم وسمعتهم بمناسبة أدائه لمهامه المتعلقة بمعالجة المعطيات ذات الطابع الشخصي[3]، وتكون العقوبة هي الحبس.

كما يعاقب بالحبس[4] ، كل من يقوم بمعالجة المعطيات ذات الطابع الشخصي دون الحصول على الموافقة الصريحة للشخص المعني[5]، أو يطلع الغير على المعطيات ذات الطابع الشخصي الخاضعة للمعالجة خارج إطار أدائه لمهامه.

ويعاقب بنفس العقوبة كل من يقوم بمعالجة معطيات ذات طابع شخصي رغم اعتراض الشخص المعني عندما تستهدف هذه المعالجة لا سيما الإشهار التجاري أو عندما يكون الإعتراض مبنيا على أسباب شرعية.

كما يعاقب بالحبس كل من ينجز أو يأمر بإنجاز معطيات ذات طابع شخصي دون الحصول على تصريح أو ترخيص مسبق من طرف السلطة الوطنية[6].

ويعاقب بنفس العقوبات كل من يقدم تصريحات كاذبة أو يواصل نشاط معالجة المعطيات رغم سحب وصل التصريح أو الترخيص الممنوح له من طرف السلطة الوطنية.

---

[1]- خثير مسعود ، المرجع السابق ، ص 100

[2]- المادة 54 من القانون رقم 18-07 المتعلق بحماية المعطيات ذات الطابع الشخصي.القانون السابق، (الحبس من سنتين إلى خمس سنوات وبغرامة من 200.000دج إلى 500.000دج). القانون.

[3]- المادة 07 من القانون رقم 18-07 ، القانون نفسه

[4] - من سنة إلى ثلاثة سنوات وبغرامة من 100.000دج إلى 300.000 دج من القانون رقم 18- 07، القانون نفسه.

[5]- وإذا كان الشخص المعني عديم أو ناقص الأهلية تخضع الموافقة للقواعد المنصوص عليها في القانون العام، ويمكن للشخص المعني أن يتراجع عن موافقته في أي وقت.

[6]- المادة 12 من القانون رقم 18-07 المتعلق بحماية المعطيات ذات الطابع الشخصي (.يعاقب بالحبس من سنتين إلى خمس سنوات وبغرامة من 200.000دج إلى 500.000دج، المادة56)

ويعاقب بالحبس كل من يقوم بمعالجة المعطيات الحساسة[1] دون الموافقة الصريحة من الشخص المعني وفي غير الحالات المنصوص عليها في القانون[2].

كما يعاقب بالحبس كل من قام بإنجاز أو استعمال معالجة معطيات لأغراض أخرى غير تلك المصرح بها والمرخص لها.

ويعاقب بالحبس كل من يقوم بجمع معطيات ذات طابع شخصي بطريقة تدليسية أو غير نزيهة أو غير مشروعة[3].

كما يعاقب بالحبس كل من سمح لأشخاص غير مؤهلين بالولوج إلى معطيات ذات طابع شخصي.

ويعاقب بالحبس كل من يعرقل عمل السلطة الوطنية:

- بالإعتراض على إجراء عملية التحقيق في عين المكان.
- عن طريق رفض تزويد أعضائها أو الأعوان الذين وضعوا تحت تصرفها بالمعلومات
- والوثائق الضرورية لتنفيذ المهمة الموكلة لهم من طرف السلطة الوطنية أو إخفاء أو إزالة المعلومات المذكورة.
- عن طريق إرسال معلومات غير مطابقة لمحتوى التسجيلات وقت تقديم الطلب أو عدم تقديمها بشكل مباشر وواضح[4].

ونصت القانون المتعلق بحماية الأشخاص الطبيعيين في مجال حماية المعطيات ذات الطابع الشخصي[5]، على أنه ودون الإخلال بالأحكام الجزائية التي يستدعي تطبيقها طبيعة المعلومات المعنية، يعاقب أعضاء السلطة الوطنية الذين يفشون معلومات محمية بموجب هذا القانون بالعقوبات المنصوص عليها في المادة 301 من قانون العقوبات.

ويعاقب بالحبس كل من يلج إلى السجل الوطني لحماية المعطيات ذات الطابع الشخصي دون أن يكون مؤهلا لذلك.

1- المادة 03 الفقرة رقم 06 هي معطيات ذات طابع شخصي تبين الأصل العرقي أو الإثني أو الآراء السياسية أو القناعات الدينية أو الفلسفية أو الإنتماء النقابي للشخص المعني أو تكون متعلقة بصحته ، بما فيها معطياته الجينية.

2 - المادة 57 من القانون المتعلق بحماية المعطيات ذات الطابع الشخصي، يعاقب بالحبس من سنتين إلى خمس سنوات وبغرامة من 200.000 إلى 500.000 دج.

3- المادة 59 من القانون رقم 18-07. المتعلق بحماية المعطيات ذات الطابع الشخصي.(يعاقب بالحبس من سنة إلى ثلاثة سنوات وبغرامة من 100.000 دج إلى 300.000دج).

4- المادة 61 من القانون رقم 18-07. المتعلق بحماية المعطيات ذات الطابع الشخصي (يعاقب بالحبس من ستة أشهر إلى سنتين وبغرامة من 60.000 دج إلى 200.000دج أو بإحدى هاتين العقوبتين فقط).

5 - المادة 62 من القانون رقم 18-07 المتعلق بحماية المعطيات ذات الطابع الشخصي.القانون نفسه.

كما يعاقب بالحبس من ، كل مسؤول عن المعالجة يرفض دون سبب مشروع ، حقوق الإعلام أو الولوج أو التصحيح أو الإعتراض المتعلقة بالمعطيات ذات الطابع الشخصي.

ودون الإخلال بالعقوبات الأشد المنصوص عليها في التشريع الساري المفعول يعاقب المسؤول عن المعالجة الذي يخرق الإلتزامات المتعلقة بسرية وسلامة المعالجة[1].

كما يعاقب بنفس العقوبة كل من يقوم بالإحتفاظ بالمعطيات ذات الطابع الشخصي بعد المدة المنصوص عليها في التشريع الساري المفعول وتلك الواردة بالتصريح أو الترخيص

كما يعاقب بالحبس ، مقدم الخدمات الذي لا يقوم بإعلام السلطة الوطنية والشخص المعني عن كل انتهاك للمعطيات الشخصية.

ويعاقب بالحبس كل من ينقل معطيات ذات طابع شخصي نحو دولة أجنبية خرقا لأحكام القانون[2].

ويعاقب بالحبس من كل من يقوم بوضع أو حفظ في الذاكرة الآلية المعطيات ذات الطابع الشخصي المتعلقة بجرائم أو إدانات أو تدابير أمن في غير الحالات المنصوص عليها في القانون.

و يعاقب بالحبس كل مسؤول عن المعالجة وكل معالج من الباطن ، وكل شخص مكلف بالنظر إلى مهامه بمعالجة معطيات ذات طابع شخصي يتسبب أو يسهل ولو عن أهمال الإستعمال التعسفي أو التدليسي للمعطيات المعالجة أو المستلمة أو يوصلها إلى غير المؤهلين لذلك.

ويعاقب الشخص المعنوي الذي يرتكب الجرائم المنصوص عليها في هذا القانون وفقا للقواعد المنصوص عليها في قانون العقوبات

يمكن أن يتعرض الأشخاص الذين يخالفون هذا القانون إلى العقوبات التكميلية المنصوص عليها في قانون العقوبات[3]

كما يمكن الأمر بمسح كل أو جزء من المعطيات ذات الطابع الشخصي التي هي محل معالجة والتي نتج عنها ارتكاب جريمة، يؤهل أعضاء ومستخدمو السلطة الوطنية لمعاينة مسح هذه المعطيات.

ويصادر محل الجريمة بغض إلى إعادة تخصيصه أو تدميره في إطار التشريع الساري المفعول.

ويتحمل المحكوم عليه مصاريف إعادة التخصيص أو التدمير.

---

[1]- المواد 66-67-68 من القانون رقم 18-07. المتعلق بحماية المعطيات ذات الطابع الشخصي.القانون السابق

[2]- يعاقب بغرامة من 200.000دج إلى 500.000دج (المادة 44 من القانون رقم 18-07) المتعلق بحماية المعطيات ذات الطابع الشخصي.القانون نفسه.

[3]- المواد 71- 70 من القانون رقم 18-07 المتعلق بحماية المعطيات ذات الطابع الشخصي.القانون نفسه.

ويعاقب على محاولة ارتكاب إحدى الجنح المنصوص عليها في هذا القانون بنفس العقوبات المقررة للجريمة التامة.

في حالة العود تضاعف العقوبات المنصوص عليها[1].

الفرع الثاني: العقوبات التكميلية.

نص المشرع الجزائري على عقوبات تكميلية إلى جانب العقوبات الأصلية لذلك نص في قانون العقوبات على أنه " مع الإحتفاظ بحقوق الغير حسن النية يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم،

علاوة على إغلاق المحل أو مكان الإستغلال إذا كانت الجريمة قد أرتكبت بعلم مالكها[2] ".

أما المصادرة فتشمل الأجهزة والبرامج والوسائل المستخدمة في ارتكاب جريمة من الجرائم الماسة بالمعطيات الرقمية ، أما إغلاق المواقع فيتعلق بالمواقع التي تكون محلا للجريمة الماسة بالمعطيات الرقمية و إغلاق المحل أو مكان الإستغلال إذا كانت الجريمة قد أرتكبت بعلم مالكها ومثال ذلك إغلاق المقهى الإلكتروني الذي ترتكب منه مثل هذه الجرائم شرط توافر عنصر العلم لدى مالكها.

المطلب الثاني: الجزاءات المقررة للشخص المعنوي.

أقر المشرع الجزائري المسؤولية الجزائية للشخص المعنوي عن ارتكاب أحد الجرائم الماسة بأنظمة

المعالجة الآلية للمعطيات، وذلك في المادة 394 مكرر5 من قانون العقوبات وتنقسم العقوبات المقررة للشخص المعنوي إلى عقوبات أصلية وأخرى تكميلية.

لذلك قسمنا هذا المطلب إلى فرعين تناولنا في الفرع الأول: العقوبات الأصلية ، وفي الفرع الثاني ، العقوبات التكميلية.

الفرع الأول: العقوبات الأصلية.

لقد أقر المشرع الجزائري المسؤولية الجزائية للشخص المعنوي وذلك لنص المادة 18 من قانون العقوبات حيث نصت على " العقوبات المطبقة على الشخص المعنوي في مواد الجنايات والجنح وهي:

[1]- المادة 73- 74 من القانون رقم 18-07. المتعلق بحماية المعطيات ذات الطابع الشخصي، القانون السابق.

[2] - المادة 394 مكرر6 من قانون العقوبات، القانون السابق.

ـ الغرامة التي تساوي مرّة إلى خمسة مرات الحد الأقصى للغرامة المقدرة للشخص الطبيعي من القانون الذي يعاقب على الجريمة.

ـ واحدة أو أكثر من العقوبات التالية:

- حل الشخص المعنوي.
- غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز خمس سنوات.
- الإقصاء من الصفقات العمومية لمدة لا تتجاوز خمس سنوات.
- المنع من مزاولة نشاط أو عدّة أنشطة مهنية أو إجتماعية بشكل مباشر أو غير مباشر نهائيا أو لمدة لاتتجاوز خمسة سنوات.
- مصادرة الشيء الذي أستعمل في ارتكاب الجريمة أو نتج عنها.
- نشر أو تعليق حكم الإدانة.
- الوضع تحت الحراسة القضائية لمدة لاتتجاوز خمس سنوات ، وتنصب الحراسة القضائية على ممارسة النشاط الذي أدى إلى الجريمة ، أو الذي أرتكبت الجريمة بمناسبته.
- وبالنسبة للغرامة المطبقة على الشخص المعنوي عند ارتكابه إحدى الجرائم الماسة بالأنظمة المعلوماتية تعادل خمسة مرّات الحد الأقصى للعقوبة المقررة للشخص الطبيعي ،

ونص القانون على أنه " يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم الماسة بالمعطيات الرقمية كالدخول والبقاء بالغش وإذا ترتب عن هذه الأفعال حذف أو تغيير لمعطيات المنظومة ، أو الإعتداء العمدي على المعطيات ، بغرامة تعادل خمس مرّات الحد الأقصى للغرامة المقررة للشخص الطبيعي[1].

[1] ـ أنظر المادة 394 مكرر4 من قانون العقوبات الجزائري، القانون السابق.

يعاقب الشخص المعنوي الذي ارتكب إحدى الجرائم المنصوص عليها في القانون الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين ، بغرامة تعادل خمس مرات الحد الأقصى للغرامة المنصوص عليها بالنسبة للشخص الطبيعي.

الفرع الثاني: العقوبات التكميلية.

لم يكتفي المشرع الجزائري بالنص العام والذي يحدد مقدار الغرامة المقررة للشخص المعنوي بل أعاد تكرار نفس العقوبة حيث نص على " العقوبات المطبقة على الشخص المعنوي في مواد الجنايات والجنح وهي:

ـ الغرامة التي تساوي مرّة إلى خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي من القانون الذي يعاقب على الجريمة.

ـ واحدة أو أكثر من العقوبات التالية:

- حل الشخص المعنوي.
- غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز خمسة سنوات.
- الإقصاء من الصفقات العمومية لمدة لا تتجاوز خمسة سنوات.
- المنع من مزاولة نشاط أو عدّة أنشطة مهنية أو إجتماعية بشكل مباشر أو غير مباشر نهائيا أو لمدة لا تتجاوز خمس سنوات.
- مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها.
- نشر أو تعليق حكم الإدانة.
- الوضع تحت الحراسة القضائية لمدة لا تتجاوز خمس سنوات ، وتنصب الحراسة القضائية على ممارسة النشاط الذي أدى إلى الجريمة ، أو الذي أرتكبت الجريمة بمناسبته.
- وبالنسبة للغرامة المطبقة على الشخص المعنوي عند ارتكابه إحدى الجرائم الماسة بالأنظمة المعلوماتية يعاقب بغرامة تعادل خمس مرّات الحد الأقصى للعقوبة المقررة

للشخص الطبيعي ، ونص القانون على أنه " يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم كالدخول والبقاء بالغش وإذا ترتب عن هذه الأفعال حذف أو تغيير لمعطيات المنظومة ،أو الإعتداء العمدي على المعطيات ، بغرامة تعادل خمس مرّات الحد الأقصى للغرامة المقررة للشخص الطبيعي[1].

يعاقب الشخص المعنوي الذي إرتكب إحدى الجرائم المنصوص عليها في القانون رقم 15-04 الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين ، بغرامة تعادل خمس مرات الحد الأقصى للغرامة المنصوص عليها بالنسبة للشخص الطبيعي.

وتختلف هذه الغرامة باختلاف تلك المقررة للشخص الطبيعي وذلك تبعا لوجود أو عدم وجود ظروف

التشديد وعليه تشدد غرامة الشخص المعنوي تبعا لتشديد غرامة الشخص الطبيعي وتصادر التجهيزات التي أستعملت لارتكاب الجريمة طبقا للتشريع المعمول به[2].

ـ كما وسع المشرع من دائرة التجريم فنص على العقوبات المطبقة في حالة الإشتراك والشروع " كل من شارك في مجموعة أو في إتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وكان هذا التحضير مجسدا بفعل أو عدّة أفعال مادية يعاقب بالعقوبات المقررة للجريمة ذاتها[3]، وذلك بشرط:

ـ إتفاق مجموعة.

ـ تحضير مسبق مجسد بفعل مادي للجماعة فإذا ارتكبها واحد فقط فلا يعاقب.

ـ فعل المشاركة في الإتفاق.

ـ بينما تقرر المادة 394 مكرر7 من قانون العقوبات أنه يعاقب على الشروع في ارتكاب الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات بالعقوبات المقررة للجريمة ذاتها.

وقد نص الأمر المتعلق بحماية حق المؤلف على العقوبات التكميلية بالنسبة للشخص المعنوي كالغلق و المصادرة و نشر ملخص الحكم الصادر في الدعوى لذلك سنتطرق إلى:

[1] ـ أنظر المادة 394 مكرر4 من قانون العقوبات الجزائري. القانون السابق.
[2] ـ أنظر الفقرة الثانية من المادة 72 من القانون رقم 15-04 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.القانون السابق.
[3] ـ أنظر المادة 394 مكرر5 من قانون العقوبات الجزائري.القانون السابق.

ـ الغلق:

للمحكمة الحكم بغلق المؤسسة التي يستغلها المقلدون سواء كانت مملوكة لهم أو مستأجرة ، ويجوز كذلك الحكم بالغلق المؤقت أو النهائي لهذه المؤسسة و ذلك بالموازاة مع حجم الخسائر أو نوع الجريمة القائمة و يرجع الفصل لمحكمة الموضوع[1] ، وقد نص على ذلك بأنه " يمكن للجهة القضائية المختصة أن تقرر الغلق المؤقت لمدة لا تتعدى ستة (06) أشهر للمؤسسة التي يستغلها المقلد أو الشركة أو أن تقرر الغلق النهائي عند الاقتضاء"[2].

ـ المصادرة:

تعتبر المصادرة وجوبيه مما يلزم القاضي بأن يحكم بمصادرة و إتلاف جميع الوسائل و العتاد المستخدم في هاته الجريمة ، لذلك نص المشرع على أنه " تقرر الجهة القضائية المختصة : مصادرة المبالغ التي تساوي مبلغ الإيرادات أو أقساط الإيرادات الناتجة عن الإستغلال غير الشرعي لمصنف أو أداء محمي مصادرة و إغلاق كل عتاد أنشأ خصيصا لمباشرة النشاط غير المشروع وكل النسخ المقلدة[3] ، وقد حددت المادة 159 من قانون حماية حق المؤلف الجهة التي يمكن أن تؤول إليها هذه الأموال ، والوسائل محل المصادرة بحيث قررت تسليمها للمؤلف أو مالك الحقوق أو ذوي حقوقهما ، وهي بذلك تعتبر بمثابة تعويض عن الضرر اللاحق بهم.

ـ نشر ملخص الحكم :

نصت المادة 58 من قانون حماية حق المؤلف على نشر ملخص الحكم ، ويقصد بهذه العقوبة التشهير بالمحكوم عليه و التأثير على شخصيته الأدبية فهي ماسة بالشرف و الاعتبار ، وهي عقوبة تكميلية وجوبيه يجب الحكم بها دائما في حال صدور حكم بالإدانة حتى ولو وقف تنفيذ الحكم[4].

[1] ـ خثير مسعود ، المرجع السابق ، ص 101.
[2] ـ أنظر المادة 156 الفقرة 02 من الأمر المتعلق بحق حماية المؤلف و الحقوق المجاورة.القانون السابق.
[3] ـ أنظر المادة 157 الأمر المتعلق بحق حماية المؤلف و الحقوق المجاورة .القانون نفسه.
[4] ـ خثير مسعود ، المرجع نفسه، ص 102

ملخص الباب الثاني:

التفتيش وما في حكمه في نطاق البيئة الرقمية ينظر إليه في كثير من الأحيان على أنه غير مجد لما يكتنفه من صعوبات أثناء تنفيذه ، وبالذات ما يتم في الفضاء الإفتراضي (في بيئة الإنترنت) مقارنة بالجرائم التقليدية.

وفيما يخص محل التفتيش في البيئة المعلوماتية ، فهو قد يرد على المكونات المادية للحاسب الآلي وملحقاته ، وهذه لا خلاف يذكر حول خضوعها للتفتيش والضبط طبقا لقواعد قانون الإجراءات الجزائية ، بما في ذلك البيانات المخزنة في أوعية أو وسائل مادية كالأشرطة الممغنطة والأقراص الصلبة والضوئية ، وذلك تبعا للمكان أو الحيز الموجودة فيه ، ومن ثم إذا كانت موجودة بمسكن المتهم أو أحد ملحقاته فتحكمها القواعد ذاتها التي يخضع لها تفتيش المسكن ، إذ يجوز تفتيشها وضبطها متى كان تفتيش المسكن جائزا ، والعكس صحيح ، وفي حال وجودها في مكان عام فيحكمها ما يحكم هذا المكان من أحكام.

في حين أنه إذا كان الحاسب في حوزة شخص خارج مسكنه ، فإن تفتيشه عندئذ يخضع للقواعد ذاتها التي يخضع لها تفتيش الشخص بوصفه أحد متعلقاته ، يستوي أن يكون الحائز هو مالك الجهاز أم سواه.

ومن ناحية أخرى ، وهو الأهم الذي يعنينا بالذات ، أن التفتيش وما في حكمه قد يرد على الجانب المنطقي للحاسوب ، المتمثل في المعلومات والبيانات المعالجة إلكترونيا.

أما فيما يخص التحقيق في الجرائم الماسة بالمعطيات الرقمية فإن الهدف منه كإجراء قانوني هو تحليل بيانات الحاسوب من خلال تقصي المعلومات لكشف الفاعل وما فعله ومع من فعله ، بالإضافة إلى متى و أين ولماذا قام بفعلته ، بناء على ذلك تعد مهمة المحققين في الجرائم الماسة بالمعطيات الرقمية من أصعب المهام في مجال تقنية المعلومات وذلك لأنه يجب على المحقق أن يكون مؤهلا تقنيا بالإضافة إلى إلمامه بمجال القانون ، وسواء كانت الجريمة قد تم وقوعها أو لازالت جارية ، ففي النهاية يتحتم على المحققين تجهيز تقارير مفصلة عن النتائج المتحصل عليها واتخاذ الإجراءات القانونية بشأنها ، وحتى لو أنه يمكن للمجرمين المتمرسين الدخول على مجموعة من المعدات تسهل عملية إخفاء الملفات التي يمكن أن تجرمهم ، إلا أن القيام بعمل التحليل الجنائي لمعلومات الحاسوب

على وجه تقني وقانوني وتحليلي من شأنه أن يوضح الحقائق التي تؤدي إلى الكشف عن الأعمال الإجرامية مثل التجسس والتخريب ضد الأشخاص ، أو تجاوز سياسات الشركات بالإضافة إلى أعمال الاختراقات.

وقد قرر المشرع الجزائري جملة من العقوبات في حق مرتكبي الجرائم الماسة بالمعطيات الرقمية حيث تختلف العقوبة حسب درجة الفعل المرتكب وبالنظر إلى مرتكبها فيما إذا كان شخصا طبيعيا أو معنويا ، والتي تتمثل في عقوبات أصلية وعقوبات تكميلية تطبق على الشخص الطبيعي، و الشخص المعنوي.

الخـاتمة

مما لا شك فيه أن التقدم العلمي الهائل في مجال تقنيات المعلومات و تدفقها في العقود الثلاثة الأخيرة ، قد أحدث ثورة إلكترونية تطبق الآن في كافة مجالات الحياة و أضحى من الصعوبة بمكان الإستغناء عن خدمتها و فوائدها العظيمة و المتنامية ، حيث يستغل بعض المجرمين المكتشفات العلمية و ما تقدمه من وسائل متقدمة في ارتكاب العديد من الجرائم التقليدية مستغلين الإمكانيات الهائلة لهذه المخترعات ، أو إستحداث صور من الإجرام ترتبط بهذه التقنيات الحديثة التي تصير محلا لهذه الجرائم أو وسيلة لارتكابها كما تعرضنا له في بحثنا هذا.

وفي مقابل المزايا التي وفرتها المعلوماتية بشكل عام لحياة الأفراد والجماعات ، فإنها كأي ظاهرة جديدة كان لها أثار سلبية ، تمثلت بشكل أساسي في الإنتشار الرهيب للجرائم الماسة بالمعطيات الرقمية جعل المشرع الجزائري يبحث في مدى نجاعة الأنظمة والقوانين السائدة في مكافحة هذا النوع المستحدث من الجرائم ، ومعرفة مكامن النقص والقصور من أجل صياغة تشريعات جديدة تضمن تحقيق أقصى فعالية ممكنة في مكافحة هذه الجريمة ، وهو ما كان فعلا من خلال جملة من القوانين الخاصة بمكافحة الجرائم المعلوماتية بشكل عام خاصة القانون رقم 09-04 والقانون 15-04.

غير أنه من الضروري ليس فقط سن تشريعات عقابية لمكافحة الجرائم الإلكترونية ، بل أن تأخذ هذه التشريعات بعين الإعتبار ضبط المصطلحات بدقة بالنظر لخصوصية الجرائم الماسة بالمعطيات الرقمية من جهة ، واعتبارا لمبدأ الشرعية الجنائية الذي يحكمها من جهة أخرى.

كما حاول المشرع الجزائري مواكبة التطور الحاصل في مجال ضبط الجريمة المعلوماتية من خلال النص على سبل إستعانة رجال الضبطية القضائية بالكوادر المؤهلة للبحث والتحري في هذا النوع من الجرائم وتحديد مجال التنسيق بين مختلف الأجهزة المعنية بذلك ، بالإضافة إلى حث المواطنين على المشاركة في مكافحة الجرائم الماسة بالمعطيات الرقمية وذلك من خلال تشجيعهم على الإبلاغ عن هذه الجرائم.

وعلى العموم فإن الواقع يؤكد صعوبة تطبيق القوانين المعاقبة على الجريمة الإلكترونية في الجزائر، لقلّة خبرتها في هذا الشق ، وغياب المختصين والخبراء القادرين على تشخيص الجريمة قبل عرضها على المحكمة للفصل فيها.

حيث أن استصدار قوانين لمعاقبة مرتكبي الجرائم الإلكترونية غير كاف ، مع عدم تهيئة الأسس التقنية الكفيلة بتصنيف درجات هذه الجرائم وحدّة أضرارها قبل إصدار العقوبة ، هذا فضلا عن غياب التواصل الدائم بين القضاء والمختصين في الإتصالات ، ما أفرز شبه تذبذب وغموض في شأن العقوبات الدقيقة في مثل هذه الجرائم» ، وفي السياق ذاته يعاقب القانون الجزائري في الغالب مرتكبي هذه الجرائم بالسجن القصير المدى أو بالغرامة المالية ، « بحكم أن جل الجرائم الإلكترونية المرتكبة في الجزائر تصب أو تصنّف قانونيا كسرقة » ، كما يلاحظ أيضا أن نسبة إرتكاب هذه الجرائم في الجزائر متوسطة مقارنة بباقي دول العالم ، غير أن ذلك لا يعني عدم تنامي هذه الجرائم في السنوات الأخيرة على المستوى الوطني وذلك مع زيادة الإقبال على استخدام برامج الحاسوب والإنتشار الكبير لشبكة الإنترنت ، وما يصاحبها من خدمات إلكترونية ، أدت إلى ظهور الجرائم الإلكترونية بأشكالها المختلفة.

و بعد تخصيص هذا الموضوع بالدراسة تم التوصل إلى جملة من النتائج و إصدار بعض التوصيات وهي كالأتي:

1ـ النتائج:

في ضوء ما تقدم تم التوصل إلى النتائج الآتية:

ـ أحسن المشرع الجزائري باستحداثه الهيئة الوطنية للجرائم المتصلة بتكنولوجيا الإعلام والإتصال و مكافحتها و لكن كان عليه إعداد و تجهيز قوات خاصة تعمل تحت هذه الهيئة حتى يمكن لها أن تقدم ولو جزء قليل من الخبرة و المساعدة في التحقيق لكافة المحاكم الوطنية وذلك نظرا لكثافة إنتشار هذا النوع من الجرائم و سرعة زوال الدليل الإلكتروني.

ـ نظرا لخصوصية الجرائم التي ترتكب في البيئة الإلكترونية فقد خصها المشرع بقانون مستقل هو القانون رقم 09 ـ 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها ، تضمن مجموعة إجراءات جد استثنائية تتلاءم مع البيئة الإلكترونية.

ـ إن الجرائم الماسة بالمعطيات الرقمية هي سلوك غير مشروع فهي اعتداء على بيانات و أرقام و حسابات بنكية لأشخاص آخرين و يعتمد المجرمون على تقنيات حديثة عالية في علوم الحاسوب و

الإنترنت ، و بإعتبار أن هذا النوع من الإجرام كباقي الجرائم فهي تتكون من أركان الجريمة و المعروفة بالركن الشرعي و المادي و المعنوي.

ـ بعد دراسة موضوع الجرائم الماسة بالمعطيات الرقمية نجد أن أهم خاصية لها تتمثل في الحاسب الآلي باعتباره هو أداة إرتكاب هذه الجرائم ، فيقع الإعتداء على الحاسب الآلي أو ملحقاته ، وجرائم ترتكب على شبكة الإنترنت ، جرائم عابرة للحدود ، وهي جريمة يصعب إكتشافها و إثباتها بسبب سرعة محو الآثار و الأدلة فهي جريمة ناعمة أما فيما يخص خصائص الأشخاص اللذين يقومون بهذه الجرائم أي مرتكب الجريمة فهو شخص ذو خبرة فائقة يستعمل وسائل تقنية عالية تعرقل الوصول للدليل الالكتروني....

ـ تعتبر الجرائم الماسة بالمعطيات الرقمية من الجرائم التي ترتكب ضد أفراد أو مجموعات بوجود دافع إجرامي لإلحاق الضرر عمدا بسمعة الضحية بشكل مباشر أو غير مباشر ، وذلك باستخدام شبكات الإتصال الحديثة (الإنترنت) بواسطة غرف الدردشة ، البريد الإلكتروني ، أو بواسطة الرسائل النصية القصيرة رسائل الوسائط المتعددة.

ـ قد لا تقتصر الجرائم الإلكترونية على الإعتداء على الأفراد أو المجموعات و إنما قد تكون على الصعيد الدولي لتشمل مجموعة من الجرائم كالتجسس الإلكتروني و السرقة المالية و غيرها من الجرائم العابرة للحدود و تكون أكثر خطورة عندما تستهدف الأمن الوطني.

ـ أدى التطور العلمي و التكنولوجي الحديث إلى اختراع وسائل الإتصال الحديثة كالهواتف الذكية و أجهزة الإعلام الآلي ووسائل التنصت على المحادثات الهاتفية ما أدى إلى إقتحام البريد الإلكتروني وكسر الشيفرات الخاصة و العبث بالملفات الخاصة بالأفراد ما زاد من احتمال تهديد حرمة الحياة الخاصة.

ـ إذا كانت أغلب الدساتير المعاصرة قد ركزت إهتمامها على الإعتراف للفرد بحقه في سرية المراسلات إذا فهو حق دستوري لكن مع التطور الذي يشهده العالم اليوم في تكنولوجيا الإتصالات شهد العالم جريمة الإختراق وهي من أكثر الجرائم المعلوماتية انتشارا باختراق البريد الالكتروني و الإستيلاء على محتوياته أو سرقة ما فيه ، أو تدمير المعلومات بعدة طرق ووسائل يستخدمها القراصنة.

ـ يعد الإرهاب الإلكتروني من أخطر أنواع الإرهاب على الدول في العصر الحاضر كيف لا و قد أصبح أكثر ضراوة لاعتماده على التكنولوجيا المتطورة مما زاد في اتساع مسرح عملياته الإرهابية ، وبالتالي أصبح من الصعب القضاء على المجرم الإلكتروني الجديد.

ـ لم تقتصر إساءة استخدام الشبكة المعلوماتية على الأشخاص فحسب بل تعدى الأمر ليصل إلى الذمة المالية للغير مما شكل اعتداء على أموالهم المادية.

2ـ التوصيات:

في ختام هذا البحث المتواضع نتقدم بعدد من التوصيات التي من الممكن أن تساهم في معالجة الثغرات التي يعاني منها القانون في مجال المعالجة الآلية للمعطيات هذا من جهة و النقص في أجهزة التحقيق من جهة أخرى:

ـ ضرورة تدخل المشرع الجزائري من خلال تعديل قانون العقوبات و الإجراءات الجزائية ، فالحاجة إلى تشريعات جزائية متخصصة في مجال المعالجة الآلية للمعطيات باتت من الوضوح بشكل لا يخفى على أحد فكان على المشرع إيرادها في قانون خاص ، كما فعل المشرع الأمريكي.

ـ عقد اتفاقيات تعاون قضائي في مجال مكافحة الجرائم المعلوماتية و الإنابة القضائية في مجال التحقيق في هذه الجرائم ، وذلك لأن هذه الجرائم عابرة للحدود و التي لا تمتد فيها سلطات الدولة لإجراءات قضائية من معاقبة و تحقيق و تفتيش ... في دول أخرى لتعارضها مع سيادة تلك الدول الأمر الذي يقتضي إنابة سلطات الدولة التي يقع على إقليمها الجاني المراد التحقيق معه أو الحاسوب المراد تفتيشه و معاينته ، و يستحب اتخاذ إتفاقية بودابست لسنة2001 حول مكافحة الإجرام المعلوماتي أساسا لعقد هذه الإتفاقيات كونها تتضمن تنظيما و معالجة جديدة لهذه الجرائم في جوانبها الموضوعية و الإجرائية.

ـ إعداد دورات تدريبية في مراكز متخصصة لرجال التحقيق حتى يتم الإلمام بالمعرفة اللازمة لمكونات الحاسوب حيث يجب على المحقق التعرف على مكونات الحاسوب لأن التحقيق و جمع الأدلة في الجرائم المتعلقة بالجرائم الماسة بالمعطيات الرقمية يتطلب مهارات فنية عالية ليصبح قادرا على جمع الأدلة الإلكترونية و المحافظة عليها من التلف.

ـ للإستعانة بالخبراء وضع المشرع مجموعة من الشروط ومن بينها شرط التقييد في جدول المحكمة هذا في الجرائم التقليدية ، و بقي هذا الشرط حتى في الجرائم الإلكترونية ، وكان على المشرع تطوير هذه الفكرة حتى يمكن الإستعانة بخبراء خارج الجدول ممتدا إلى أبعد من النطاق الإقليمي و المادي ممثلا في الحدود المادية بين الدول و يمكن أن يكون هؤلاء الخبراء من خارج الإقليم ، وهو أمر تسمح به مقومات العالم الإفتراضي ، كونه يعد بيئة اتصالية رقمية.

ـ يجب الإهتمام بتدريب الخبراء و المحققين و القضاة على التعامل مع الجرائم الإلكترونية ذات الطبيعة الفنية المعقدة ، إضافة إلى ضرورة الإستعانة بذوي الكفاءات المتميزة بتكنولوجيات المعلوماتية بحيث تتم الإستفادة من تقليص الثغرات الأمنية على الشبكة المعلوماتية و إيجاد وسائل الوصول إلى محترفي الشبكة إلى جانب رجال القانون للسيطرة على الأمن المعلوماتي.

ـ مد سبل التعاون و التنسيق مع المؤسسات الدولية و المحلية المعنية بمكافحة الجرائم المعلوماتية ومن بينها المنظمة الدولية للشرطة الجنائية ـ الإنتربول ـ لمواجه كافة أشكال الجرائم الإلكترونية.

ـ إنشاء مركز قومي عربي لأمن الحاسبات و المعلومات و ضمان عدم إصابتها بالفيروس و ذلك كما فعلت الدول المتطورة تكنولوجيا حماية من الإعتداء عبر الشبكة العالمية الإنترنت ومثال ذلك ما قامت به الولايات المتحدة الأمريكية عند استحداث جهاز FBI الأمريكي عام 2000 مركزا خاصا بمكافحة جرائم الإنترنت و قد كانت مهمته كيفية مجابهة الجرائم المعلوماتية ، وكذلك ما قامت به فرنسا عندما أنشأت مكتبا مركزيا لمكافحة الجرائم المتصلة بتكنولوجيا المعلومات و الإتصالات تابعا لوزارة الداخلية و ذلك سنة 2000.

ـ الأخذ بما جاء في توصية المجلس الأوروبي بشأن مشاكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات ، إذا دعت الضرورة تشكيل وحدات خاصة لمكافحة جرائم الحاسب الآلي و إعداد برامج خاصة لتأهيل العاملين في مجال العدالة الجنائية لتطوير معلوماتهم في مجال تكنولوجيا المعلومات

ـ إنشاء قسم جديد بكليات الحقوق بالجامعات لدراسة الحماية القانونية للمعطيات الرقمية.

ملخـــص

الموضوع باللغات الأجنبية

The abstract of the first section:

The world is witnessing a huge and rapid development in the world communications technology, so that the modern means of communication, especially the Internet, become an indispensable means, and an engine of the new civilization, on which the idea of communication not transition is based, and this network is one of the results of integration between the revolution of information and communication technology ; This network, which was developed at a tremendous speed has been able to remove the borders and distances between countries and make the world a small village, but this technology has brought with negative effects of crimes ***called crimes against digital data****, so, in the chapter , we discussed the definition of digital data as: digital or non-numeric facts that are carried out in a systematic manner whose significance can be understood directly without engaging in extrapolative inductive processes for their complex evidence through more than one statement.*

Then we discussed the characteristics of this crime. The most prominent of these characteristics is that these crimes are committed by the computer as the main means used most in the crime and by attacking other computers and access to programs theft and destruction; the Internet was a fertile area for attacks, so some resort to in order to achieve criminal goals. Considering that these crimes are transboundary, they have abolished all geographical boundaries, thus making them acquire an international nature, such as the penetration to banks' codes and money laundering in different countries of the world. Another characteristic is that it is difficult to be detected and proved because they do not leave external traces, this makes it more complicated, they are also considered soft crimes because they do not require violence to steal information and data or transfer from one side to another or to know the codes of banks and robbing their assets, despite the absence of violence, the result are achieved and here lies the softness of these Crimes, these crimes of digital data require high technical expertise to be discovered and searched and setting the evidence professionally, but the reality proved that there is a lack of experience in the security and judicial services to prove these crimes.

In the second chapter, we dealt with forms of the infringement of digital data and the most prominent of them committed against against people, money and security. These crimes were used to violate the inviolability of private lives of people, and they became more complicated due to modern scientific and technological development, leading to invent smart means of communication, used to eavesdropping conversations, breaking e-mails, breaking their codes and tampering with files of individuals, which increased the possibility of intrusion on their secrets and violation of their sanctity without right.

In this chapter, we also dealt with crimes involving money on the Internet, which were not limited to the methods of abusing the technical

revolution of people, but went beyond it to the financial disclosure of others through banks by credit cards and other methods of fraud, even moral funds such as writings and inventions were not away from digital attacks ; As for the national security aspect, it is known that the development witnessed by the world today at all levels was a turning point and divided the world into a very sophisticated part and a backward one. Telecommunications technology had its prominent position, but some of these countries exploited it negatively to commit crimes such as electronic espionage, piracy and breaches of the sites of the Ministry of Defense in some countries ; so those acts were classified as electronic terrorism and considered a criminal phenomenon whose effects exceeded the borders of one state and thus acquired a global character that threatens the security and integrity of humanity and human rights, its fundamental importance on the one hand and the interests of peoples on the other.

Résumé de la première section:

Le monde est un développement énorme et rapide de la technologie des communications mondiales, de sorte que les moyens de communication modernes, en particulier l'Internet, deviennent un moyen indispensable, et un moteur de la nouvelle civilisation, sur laquelle l'idée de communication ne transition est basée, et ce réseau est l'un des résultats de l'intégration entre la révolution des technologies de l'information et de la communication; Ce réseau, qui a été développé à une vitesse vertigineuse a été en mesure d'éliminer les frontières et les distances entre les pays et faire du monde un petit village, mais cette technologie a apporté des effets négatifs des crimes dits crimes contre des données numériques, de sorte que, dans le chapitre , nous avons discuté de la définition des données numériques comme: faits numériques ou non numériques qui sont réalisées de manière systématique dont l'importance peut être compris directement, sans se livrer à des processus inductifs extrapolatives pour leur démontrer la preuve par plus d'une instruction.

Ensuite, nous avons discuté des caractéristiques de ce crime. La plus importante de ces caractéristiques est que ces crimes sont commis par l'ordinateur comme le principal moyen utilisé le plus dans le crime et en attaquant d'autres ordinateurs et l'accès au vol et la destruction des programmes; Internet était un terrain fertile pour les attaques, donc certains ont recours à des objectifs criminels. Considérant que ces crimes sont transfrontaliers, ils ont aboli toutes les frontières géographiques, les rendant ainsi acquérir un caractère international, comme la pénétration aux codes des banques et le blanchiment d'argent dans différents pays du monde. Une autre caractéristique est qu'il est difficile à détecter et prouvé parce qu'ils ne laissent pas de traces extérieures, ce qui rend plus compliqué, ils sont également considérés comme des crimes mous parce qu'ils ne nécessitent pas de violence pour voler des informations et des

données ou le transfert d'un côté à l'autre ou de connaître les codes des banques et voler leurs biens, malgré l'absence de violence, le résultat est atteint et est ici la douceur de ces crimes, ces crimes de données numériques nécessitent des compétences techniques élevées à découvrir et à rechercher et établir la preuve professionnelle , mais la réalité prévoyait un manque d'expérience dans les services de sécurité et les services judiciaires pour prouver ces crimes.

Dans le deuxième chapitre, nous avons eu affaire à des formes de violation des données numériques et le plus important d'entre eux commis contre les personnes, l'argent et la sécurité. Ces crimes ont été utilisés pour violer l'inviolabilité de la vie privée des gens, et ils sont devenus plus complexes en raison du développement scientifique et technologique moderne, ce qui conduit à inventer des moyens intelligents de communication, utilisés à des conversations d'écoute électronique, brisant les e-mails, brisant leurs codes et la falsification avec des fichiers d'individus, ce qui a augmenté la possibilité d'intrusion dans leurs secrets et la violation de leur sainteté sans droit.

Dans ce chapitre, nous avons également abordé des crimes impliquant de l'argent sur Internet, qui ne se limitaient pas aux méthodes d'abuser de la révolution technique des gens, mais on est allé au-delà de la divulgation financière des autres par les banques par cartes de crédit et d'autres méthodes de fraude même les fonds moraux tels que les écrits et les conventions ne sont pas loin des attaques numériques; En ce qui concerne l'aspect de la sécurité nationale, il est connu que le développement témoigne le monde d'aujourd'hui à tous les niveaux a été un point tournant et divisé le monde en une partie très sophistiquée et un en arrière. La technologie des télécommunications a sa position de premier plan, mais certains de ces pays exploité négativement à commettre des crimes tels que l'espionnage électronique, la piraterie et les violations des sites du ministère de la Défense dans certains pays; de sorte que ces actes ont été classés comme le terrorisme électronique et considéré comme un phénomène criminel dont les effets ont excédé les frontières d'un Etat, et donc acquis un caractère mondial qui menace la sécurité et l'intégrité de l'humanité et des droits de l'homme, son importance fondamentale d'une part et les intérêts des les peuples de l'autre.

The abstract of the second section:

Inspection and the like in the digital environment is often viewed as ineffective in the course of its implementation, especially in virtual space (in the Internet environment) compared to traditional crimes.

In the area of the matter of inspection in the information environment, it may be related to physical components of the computer and its accessories, and there is no dispute about the subject of inspection and control in accordance with the rules of the Code of Criminal Procedure, including data stored in containers or physical means such as magnetic tapes and hard and optical drives, depending on Of the place or space where it is situated, and then if it is located in the defendant's residence or one of its annexes, it shall be subject to the same rules as the inspection of the dwelling. It may be searched and seized when the house inspection is permissible, and vice versa, if they were in a public place, they are governed by provisions that govern this place. Whereas if the computer is in the possession of a person outside his or her home, then its inspection is subject to the same rules as the person being searched as a possessor, the owner being the owner of the computer or another one.

On the other hand, and most importantly, we are concerned that the inspection and the like may be answered seen in the logical side of the computer, namely electronically processed information and data.

As for the investigation of crimes against digital data, the purpose of the legal process is to analyze computer data by investigating information to reveal the actor and what he did and with whom, as well as when, where and why did it, therefore the task of investigators in the crimes of digital data from is one of the most difficult tasks in the field of information technology because the investigator must be technically qualified in addition to knowledge of the field of law, whether the crime has occurred or is still ongoing, in the end it is imperative that the investigators must prepare detailed reports on the results obtained and take legal action, and even if experienced criminals have access to a set of equipment that facilitates the concealment of files that can criminalize them, the computer, forensic, and analytical analysis of computer information will clarify the facts that lead to the detection of criminal acts such as espionage and sabotage against people, or beyond corporate policies as well as penetrations.

The Algerian legislator imposes a number of penalties on perpetrators of offenses involving digital data. The penalty varies according to the degree of the act committed and in view of the perpetrator whether he is a natural or moral person, namely, original penalties and supplementary penalties applied to the natural person.

Le résumé de la deuxième section :

L'inspection dans un environnement numérique est souvent considérée comme inefficace au cours de sa mise en œuvre, en particulier dans l'espace virtuel (dans l'environnement Internet) par rapport aux crimes traditionnels.

Dans le domaine de la question de l'inspection dans l'environnement de l'information, il peut être lié à des composants physiques de l'ordinateur et ses accessoires, et il n'y a pas de contestation sur le sujet de l'inspection et de contrôle conformément aux règles du Code de procédure pénale , y compris les données stockées dans des conteneurs ou des moyens physiques tels que les bandes magnétiques et les disques durs et optiques, selon du lieu ou de l'espace où il se trouve, et si elle est située dans la résidence ou l'une de ses annexes du défendeur, elle est soumis aux mêmes règles que l'inspection du logement. Il peut être fouillé et trié lorsque l'inspection de la maison est autorisée, et inversement, s'il était dans un lieu public, il est régi par les dispositions qui régissent cet endroit. Alors que si l'ordinateur est en possession d'une personne en dehors de sa maison, puis l'inspection est soumise aux mêmes règles que la personne recherchée en tant que possesseur, le propriétaire étant le propriétaire de l'ordinateur ou un autre.

D'un autre côté, et surtout, nous sommes préoccupés par le fait que l'inspection et autres éléments similaires puissent être pris en compte du côté logique de l'ordinateur, des informations et des données précédemment traitées électroniquement.

Quant à l'enquête sur les crimes contre les données numériques, dans le but de la procédure judiciaire est d'analyser les données informatiques en enquêtant sur des informations de révéler l'acteur et ce qu'il a fait et avec qui, ainsi que quand, où et pourquoi at-il donc la tâche des enquêteurs spécialisés dans les crimes de données numériques est l'une des tâches les plus difficiles dans le domaine des technologies de l'information parce que l'enquêteur doit être techniquement qualifié, en plus de la connaissance du domaine du droit, si le crime a été commis ou est toujours en cours, en la fin, il est impératif que les enquêteurs doivent préparer des rapports détaillés sur les résultats obtenus et une action en justice, et même si les criminels expérimentés ont accès à un ensemble d'équipements qui facilite la dissimulation de fichiers qui peuvent les ériger en infraction pénale, l'ordinateur, de médecine légale, et L'analyse analytique de l'information informatique permettra de clarifier les faits qui conduisent à la détection d'actes criminels tels que l'espionnage et le sabotage contre des personnes, ou au-delà. politiques privées ainsi que des pénétrations.

Le législateur algérien impose un certain nombre de sanctions aux auteurs d'infractions impliquant des données numériques. Les dérogations pénales en fonction du degré de l'acte commis et de l'auteur, qu'il s'agisse

d'une personne physique ou morale, à savoir les peines initiales et les peines complémentaires appliquées à la personne physique,

قائمة المصادر والمراجع

ـ القرآن الكريم.

أولا . المصادر :

1- الدستور الجزائري الصادر في 1963 المعدل والمتمم.

2- الإتفاقية الأمريكية لحقوق الإنسان الموقعة بتاريخ 22-11-1969

3- الإتفاقية الأوروبية لحماية الإنسان و الحريات الأساسية ، الموقعة في روما بتاريخ 04-11-1950.

4- الاتفاقية العربية لمكافحة الارهاب ،

5- اتفاقية المجلس الأوروبي الخاصة بحماية الأفراد من معالجة المعلومات و الموقعة بتاريخ 28، 01، 1981.

6- إتفاقية جتيف المرجع نفسه.

7- إتفاقية دول مجلس التعاون الدول الخليج العربية لمكافحة الارهاب المنعقدة في مدينة الرياض بالمملكة العربية السعودية عام 1987.

8- اتفاقية منظمة الدول الأمريكية لمنع و قمع الارهاب الموقعة في واشنطن بتاريخ 02-02-1971.

9- الإتفاقية الأوروبية لقمع الارهاب ، الصادرة عن المجلس الأوروبي و التي أبرمت في 10نوفمبر 1976 و دخلت حيز النفاد في أوت 1978.

10- الأمر رقم 66-155 المؤرخ في 8 جوان المتضمن قانون العقوبات الجزائري المعدل و المتمم.

11- الأمر رقم 56 - 155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية الجزائري.

12- الأمر رقم 75 -58 المؤرخ في 26 ـ 09 ـ 1975 المتضمن القانون المدني المعدل و المتمم

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

14- القانون رقم 09. 04 المؤرخ في 05 . 08 . 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها ، جٍ 47 المؤرخ في 16 . 08. 2009 .

15- القانون رقم 15 . 04 يحدد القواعد العامة المتعلقة بالتوقيع و التصديق الالكترونيين الجريدة الرسمية رقم 06 الصادرة في 10، 02، 2015

16- المرسوم التشريعي رقم 92-03المؤرخ في 30-09-1992 المتعلق بمكافحة الإرهاب و التخريب ،ج،ر عدد 70، بتاريخ01-10-1992.

17- الأمر رقم 05/03المؤرخ في 19 يوليو 2003 المتعلق بحقوق المؤلف و الحقوق المجاورة ،ج، ر العدد 44 ، المؤرخة في 23،07،2003.

18- دستور 2008.

19- دستور دولة البحرين الصادر في 1973.

20- دستور دولة الكويت الصادر في 1962.

21- دستور سلطنة عمان الصادر في 1996.

22- القانون الاتحادي لدولة الإمارات المتعلق بحماية جرائم المعلومات لسنة 2006.

23- القانون الأردني رقم 85المتعلق بالمعاملات الالكترونية الصادرة في 2001.

24- القانون الأردني من قانون جرائم أنظمة المعلومات المؤقت في الجريدة الرسمية رقم 5056 بتاريخ 16،09،2010.

25- القانون الارني رقم 85 المتعلق بالمعلومات الالكترونية لسنة 2001.

26- قانون الامارات العربية المتحدة المتعلق بالمعاملات التجارية الإلكترونية لسنة ، 2006.

27- القانون الامريكي المتعلق بالمعا ملات التجارية الالكترونية ، سنة 1999.

28- قانون البحرين رقم 83المتعلق بالمعاملات الالكترونية لسنة 2002.

29- قانون التوقيع الالكتروني المصري رقم 15 لعام 2004.

30- القانون السعودي المتعلق بمكافحة جرائم المعلوماتية الصادرة بتاريخ 2007.03.26

31- قانون العقوبات السوري المضاف بالقانون رقم 36لسنة 1978.

32- قانون العقوبات الفرنسي و لمزيد من التفصيل أنظر الموقع الآتي http//www.legi Fance .Gouv.Fr.

33- قانون العقوبات المصري المضاف بالقانون رقم 97لسنة 1992.

34- قانون العقوبات المصري المعدل بالقانون رقم 147لسنة 2006.

35- القانون الفرنسي رقم 652/28 المتعلق بالإتصالات السمعية و البصرية الصادر في 26،07،1982.

36- قانون المعاملات الإلكترونية الأردن رقم 85 لسنة 2001.

37- قانون المعاملات الإلكترونية الإماراتية لسنة 2002.

38- القانون رقم 04.09 المؤرخ في 05غشت 2009متضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها ، جر، العدد 47.

39- المرسوم الملكي السعودي المتعلق بنظام مكافحة الجرائم المعلوماتية السعودية ، الصادر في 27،4 ، 2008.

40- الأمم المتحدة ، دراسة حول تشريعات مكافحة الإرهاب في دول الخليج العربية و اليمن ، نيويورك ، سنة 2009، ص08.

ثانيا: المراجع.

الكتب:

1- أبو بكر جابر الجزائري منهج المسلم ،كتاب عقائد و آداب و أخلاق عبادات و معاملات ، دار الغد الجديد للنشر و التوزيع الطبعة الاولى.

2- أبو سريع أحمد عبد الرحمن ، بحث علمي بعنوان إستخدام الانترنت في تعاطي المخدرات . المخدرات الرقمية ، الموقع نفسه.

3- أحسن بوسقيعة ، الوجيز في القانون الجزائي العام ، الطبعة الأولى ، الديوان الوطني للأشغال التربوية ، الجزائر ، 2002.

4- أحمد حسام طه تمام ، الجرائم الناشئة عن استخدام الحاسب الآلي (الحماية الجنائية للحاسب الآلي ، دراسة مقارنة)، دار النهضة العربية ، القاهرة ، الطبعة الأولى ، 2000.

5- أحمد حسام طه تمام ، الحماية الجنائية لتكنولوجيا الإتصالات ، دراسة مقارنة ،دون طبعة ، دار النهضة العربية ن مصر 2002،

6- ـ أحمد شوقي أبوخطو ، تعويض المجنى عليهم من الأضرار الناشئة عن جرائم الإرهاب ، دار النهضة ، القاهرة ،1992.

7- احمد عبد الرزاق السنهوري ، الوسيط في شرح القانون المدني ، حق الملكية ، الجزء الثاني ، دار إحياء التراث العربي ، بيروت ، 1952.

8- أحمد عبد الكريم سلامة القانون الدولي الخاص ، دار النهضة العربية ، القاهرة ، 2008.

9- أحمد فتحي سرور ، الوسيط في القانون الإجراءات الجزائية ، دار النهضة العربية ،الجزء الأول،1981.

10- أسامة عبد الله قايد ، الحماية الجنائية للحياة الخاصة و بنوك المعلومات ، دون طبعة ، دار النهضة العربية ، مصر ، سنة 1994.

11- الإعلان العالمي لحقوق الإنسان اعتمد بموجب قرار الجمعية العامة المؤرخ في 10-12-1984.

12- السند عبد الرحمان عبد الله ، الأحكام الفقهية للتعاملات الالكترونية ، دار الوراق ، ط2 الرياض 2006.

13- العهد الدولي الخاص بالحقوق المدنية و السياسية أعتمد وعرض للتوقيع و التصديق و الإنظمام بموجب القرار الجمعية العامة للأمم المتحدة المؤرخ في 16-12-1966.

14- العوضي عبد الهادي ، الجوانب القانونية للبريد الالكتروني ، دار النهضة العربية ، د ط ،القاهرة.

15- القاسم محمد بن عبد الله ، أساسيات أمن المعلومات ، مكتبة الملك فهد الوطنية ، ط2 ، الرياض ، 2008.

16- إمام حانين عطا الله ، الإرهاب البنيان القانوني للجريمة ، دار المطبوعات الجامعية ،سنة 2004.

17- أمير فرج يوسف ، الجرائم المعلوماتية على شبكة الانترنت ، دار المطبوعات الجامعية ، الإسكندرية ، سنة2008.

18- أمير فرج يوسف الجريمة الالكترونية و المعلوماتية و الجهود الدولية و المحلية للمكافحة ، الطبعة 01مكتبة الوفاء القانونية ، الاسكندرية ، سنة 2011.

19- انتصار نوري الغريب ، أمن الكمبيوتر و القانون ، دار الراتب الجامعية ، بيروت ،1994.

20- أنظر المادة الألى من التوصيات الصادرة عن المؤتمربكلية الحقوق المنعقد بجامعة الأسكندرية في 4-5-6 يونيو 1987

21- أنيس المومني ، قانون العقوبات في مواجهة مخاطر الأنترنت ، رسالة ماجستير في القانون الجنائي ، جامعة عنابة ، الجزائر ، سنة 2003.

22- أيمن عبد الحفيظ ، الإتجاهات الفنية و الأمنية لمواجهة الجرائم المعلوماتية ،بدون نشر،2005.

23- إيهاب فوزي السقا ، الحماية الجنائية و الأمنية لبطاقات الإئتمان ، دار الجامعة الجديدة ، الإسكندرية ، سنة 2007.

24- بلفريد لطفي لمين ، الفضاء السبراني : هندسة و فواعل مقال منشور بالمجلة الجزئرية للدراسات السياسية ، العدد 05، سنة 2016.

25- جعفر حسن جاسم الطائفي ،جرائم تكنولوجيا المعلومات ، درا البداية ، عمان ، سنة 2007.

26- حتمت قاسم ، مدخل لدراسة المكتبات و علم المعلومات ، القاهرة ، دار غريب ، سنة1990.

27- حسن بن أحمد الشهري ، الأنظمة الإلكترونية الرقمية المطورة لحفظ حماية سرية المعلومات من التجسس ، المجلة العربية للدراسات الأمنية و التدريب ، المجلد 28، العدد 56.

28- خالد ممدوح إبراهيم ، امن مراسلات البريد الالكتروني ، الدار الجامعية ، دط ، الإسكندرية ،2008.

29- خالد بن نواف الحربي ، الأمن و الحماية في الأنترنت ، المملكة العربية السعودية.

30- خالد ممدوح إبراهيم ، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي،الإسكندرية، 2010.

31- خالد ممدوح ابراهيم ، الجرائم المعلوماتية ،دار الفكر الجامعي ، الطبعة ألولي ، الإسكندرية ، 2009.

32- خالد ممدوح ابراهيم ، أمن الجريمة الالكترونية ، الدار الجامعية ، سنة 2008.

33- خثير مسعود ، الحماية الجنائية لبرامج الكومبيوتر أساليب و ثغرات، دار الهدى ،الجزائر طبعة 2010.

34- خيرت علي محرز، التحقيق في جرائم الحاسب الآلي ، دار الكتاب الحديث ، 2012.

35- رشا خليل ،جرائم الاستغلال الجنسي للأطفال عبر الانترنت ، جامعة ديالى ، مجلة الفتح العدد 27 ، العراق 2006.

36- رشيدة بوكر ، جرائم الإعتداء على نظام المعالجة الآلية في التشريع الجزائري و المقارن ، منشورات الحلبي الحقوقية ، الطبعة 01 سنة2012.

37- زاهر راضي ، استخدام مواقع التواصل الاجتماعي في العالم العربي ، مجلة التربية ، العدد 15 ، جامعة عمان الأهلية ، سنة 2003.

38- ـ سامي جلال فقي ، التفتيش في الجرائم المعلوماتية ،دراسة تحليلية ، دار الكتب القانونية ، مصر ، 2011.

39- سعيد حسب الله عبد الله، شرح قانون أصول المحاكمات الجزائية ، دارين الأثير للطباعة ، الموصل ، 1998.

40- سورة الحجرات.

41- شادي ناصف ،فضائح الفيس بوك ،أشهر موقع استخبارتي على شبكة الأنترنت ،سورية ،دار الكتاب العربي ،سنة 2009.

42- صالح بن محمد المسند ، جرائم الحاسب الآلي الخطر الحقيقي في عصر المعلومات مقال بالجلة العربية للدراسات الأمنية و التدريب ، المجلد 15، العدد 29، الرياض.

43- صالح جواد كاظم ، مباحث في القانون الدولي، التكنولوجيا الحدسثة و السرية الشخصية ، الطبعة 1،دار الشؤون الثقافية العامة ، بغداد ، سنة 1991.

44- عبد الأحد جمال الدين.

45- عبد الباقي الصغير ،الحماية الجنائية و المدنية لبطاقات الائتمان الممغنطة ، دار النهضة العربية ، القاهرة ، 2003.

46- عبد الحميد ابراهيم ، العلاقة بين الإرهاب المعلوماتي و الجرائم المنظمة ، الدورة التدريبية مكافحة الجرائم الإرهابية المعلوماتية حلال الفترة من 9-13 مارس 2016بالقنطيرة بالمغرب.

47- عبد الفتاح بيومي ، المبادئ العامة في جرائم الصحف ،دار النهضة العربية ، 2008.

48- عبد الفتاح بيومي حجازي ، الدليل الجنائي و التزوير في الجرائم الكمبيوتر ، دار الكتب القانونية ، 2002.

49- عبد الفتاح بيومي حجازي ، مبادي الإجراءات الجنائية في جرائم الكمبيوتر ، و الأنترنت ، دار الفكر الجامعي ، الإسكندرية ، الطبعة 01، سنة 2006.

50- عبد الفتاح يومي حجازي ، التزوير في جرائم الكمبيوتر و الأنترنت ، دار الكتب القانونية ، مصر ، سنة 2008.

51- عبد الله أحمد المشرخ ، مكافحة الإجرام الاقتصادي و المالي ، مجلة الفكر الشرطي ، إدارة شرطة الشارقة ، العدد الثالث ، سنة 2000،07،13.

52- عبد الله بن عبد العزيز بن فهد العجلان ، الإرهاب الإلكتروني في عصر المعلومات ، بحث مقدم إلى المؤتمر الدولي الأول حول حماية أمن المعلومات و الخصوصية في قانون الأنترنت ، و المنعقد بالقاهرة في المدة من 2-4 يونيو 2008.

53- عبد الله بن ناصر ، الحماية الجنائية للبريد الالكتروني ،دراسة تأصيلية مقارنة ،جامعة نايف العربية للعلوم الأمنية ، الرياض ، سنة 2012.

54- عبد الله سليمان ، شرح قانون العقوبات الجزائري القسم العام ، الجزء الأول ، ديوان المطبوعات الجامعية ، الجزائر ، سنة 1998.

55- عبد الناصر محمد محمود فرغلي ، محمد عبيد سيف سعيد المسماري ، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية و الفنية ، دراسة تطبيقية مقارنة جامعة نايف العربية للعلوم الأمنية ، 2007.

56- عبد الناصر محمد محمود فرغلي ، محمد عبيد سيف سعيد المسماري ، الإثبات الجنائي في الأدلة الرقمية من الناحيتين القانونية ، و الفنية ، دراسة تطبيقية ومقارنة ، الرياض ، 2008

57- عبود السيراج ، قانون العقوبات ، القسم العام ، الطبعة الرابعة ، مطبوعات جامعة ديمشق ، سنة 1990.

58- عطاء الله فشار ، مواجهة الجريمة المعلوماتية في التشريع الجزائري ، مقال منشور بكلية الحقوق و العلوم السياسية ، جامعة الجلفة ، ولم يذكر عنوان المجلة ، العدد ، و السنة.

59- على أحمد ، حق الخصوصية في القانون الجنائي ، دراسة مقارنة ، المؤسسة الحديثة للكتاب ، طرابلس، سنة 2006،

60- على عدنان الفيل ، إجراءات التحري وجمع الأدلة و التحقيق الإتبدائي في الجريمة المعلوماتية دراسة مقارنة ، المكتب الجامعي الحديث، 2011.

61- على عدنان الفيل ، الإجرام الإلكتروني دراسة مقارنة ، منشورات زين الحقوقية و الأدبية ، الطبعة الأولى ، سنة 2011.

62- علي حسن محمد الطوالبة ، على نظم الحاسوب و الانترنت ، دراسة مقارنة ، عالم الكتاب الحديث ، الأردن ، 2004.

63- علي عبد القادر قهوجي ، الحماية الجنائية لبرامج الكمبيوتر ، المكتبة القانونية ، القاهرة ، 1999.

64- علي محمد صالح ،حقوق الإنسان و حرياته ، دار الثقافة للنشر و التوزيع ، سنة 2005.
65- علي يوسف الشكري ، الإرهاب الدولي ،دار أسامة للنشر و التوزيع ، الطبعة الأولى ،سنة 2008.
66- عمر أبو الفتوح عبد العظيم ، الحماية اجنائية للمعلومات المسجلة إلكترونيا ، دراسة مقارنة ، دار النهضة العربية ، القاهرة ، سنة2010.
67- عمر محمد أبو بكر بن يونس ، الجرائم الناشئة عن استخدام الانترنت ، دار النهضة العربية ، القاهرة ، 2004.
68- عمرو عيسى الفقى ، الجريمة المعلوماتية ،جرائم الحاسوب الألي و الانترنت في مصر و الدول العربية،المكتب الجامعي الحديث ، الإسكندرية ،2006.
69- عن موقع إسلام أن لاين. محمود سامي الشوا: "ثورة المعلومات وانعكاساتها على قانون العقوبات". دار النهضة 1995.
70- فادي سالم ، الوجه الإلكتروني في الصراع العربي الاسرائلي / مجلة انترنت العالم العربي ، السنة الرابعة ، العدد الثاني ، سنة 2000.
71- فاطمة نعناع ، مقالة بعنوان قنبلة إلكترونية في بريد الجامعة ،منشور في مجلة إنترنت العالم العربي ، السنة الألى ، العدد السابع ، إبريل 1998.
72- فريال حسين ،مقال منشور بعنوان القدف و الذم في شبكات التواصل بجريدة النور، العدد 732،بتاريخ 10-08-2016.
73- قارة أمال ، الحماية الجزائية للمعلوماتية في التشريع الجزائري ، دار هومة ، الجزائر ، الطبعة 02 ، 2007،ص125
74- قدري عبد الفتاح الشهاوي ، ضوابط التفتيش في التشريع المصري و المقارن ، منشأة المعارف ، الإسكندرية ، 2005.
75- ماجد عمار ، المسؤولية القانونية الناشئة عن استخدام فيروس برامج الكمبيوتر و وسائل حمايتها ، دار النهضة العربية ،1989.
76- مارتن لوسيان، سر الحياة الخاصة ، المجلة الفصلية ، القانون المدني الفرنسي ،سنة1959.
77- مأمون سلامة ، قانون الإجراءات الجنائية ، دار الفكر العربي ، الطبعة الأولى ،1980.
78- مجدي محب الدين ، القذف و السب ،مصر 2002.
79- محمد أبو علاء عقيدة ، التحقيق و جمع الأدلة في مجال الجرائم الالكترونية ، بحث علمي مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية و الأمنية للعمليات الالكترونية ، أكادمية شرطة دبي مركز البحوث و الدراسات ، العدد الأول ، الإمارات العربية المتحدة ، دبي ، 2003.

80- محمد البخاري ، الأنترنت و مبادئ الأمن المعلوماتي الدولي : الدورة المعلوماتية فجرت الحواجز القائمة بين الشعوب ، شبكة الضياء للمؤتمرات و الدراسات أنظر الموقع diae.net تاريخ الإطلاع على الموقع في 04-06-2016.

81- محمد أمين الرومي ، جرائم الكمبيوتر و الانترنت ، دار المطبوعات الجامعية ، الاسكندرية ، سنة 2003.

82- محمد أمين الشوابكة ، جرائم الحاسوب و الانترنت ، الجريمة المعلوماتية ، دار الثقافة للنشر و التوزيع ، عمان ، الطبعة 01، سنة 2007.

83- محمد بن عبد الله بن علي المنشاوي ، جرائم الانترنت في المجتمع السعودي ، د ن ت ، الرياض 2003.

84- محمد بنعبد اللهبن علي المنشاوي،جرائم الأنترنت في المجتمع السعودي ،أكادمية نايف العربية للعلوم الأمنية ، الرياض ، سنة2003.

85- محمد حماد مرهج الهيتي ،جرائم الحاسوب ،دراسة تحليلية، دار المناهج للنشر و التوزيع،الطبعة الأولى ،عمان ،2006.

86- محمد دباس الحميد ، ماركو ابراهيم نينو ، حماية أنظمة المعلوماتية ، دار حامد للنشر و التوزيع ،عمان، الطبعة 01، سنة 2007.

87- محمد سامي الشوا، ثورة المعلومات و إنعسكاساتها على قانون العقوبات ، دار النهضة العربية ، سنة 2003.

88- محمد طارق عبد الرؤوف ،جريمة الاحتيال عبر الانترنت ، منشورات الحلبي الحقوقية ،لبنان ،2011.

89- محمد عبيد الكعبي ، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الأنترنت ، دار النهضة العربية ، القاهرة.

90- محمد عزيز شكري ، الإرهاب الدولي و النظام العالمي الراهن ، ديمشق.

91- محمد على سالم ، حسون عبيد ، هجيج الجريمة المعلوماتية ، مجلة جامعة بابل ، العلوم السياسية ، العدد 14، العراق ،سنة 2008.

92- محمد قاسم النصر ، الحق في سرية المراسلات في بعض النظم ، 2006.

93- محمد محمد الشلش ، مقال بعنوان حقوق الملكية الفكرية بين الفقه و القانون ، جامعة القدس المفتوحة ، مجلة جامعة النجاح الوطنية ، فلسطين ، 2006.

94- محمد محمد شتا ، فكرة الحماية الجنائية لبرنامج الحاسب الآلي ، دار الجامعة الجديدة للنشر 2002.

95- محمد يوسف علوان ، محمد خليل الموسى ، القانون الدولي لحقوق الإنسان المصادر ووسائل الرقابة ، الجزء الأول ، دار الثقافة للنشر و التوزيع ، الأردن ، الطبعة 01، سنة 2005.

96- محمود أحمد عبابنة ، جرائم الحاسوب و أبعادها الدولية ، دار الثقافة للنشر و التوزيع الاردن ، 2009.

97- محمود جمال الدين زكي ، الخبرة في مواد المدنية و التجارية ، مطبعة جامعة القاهرة ، 1990

98- محمود نجيب حسن ، شرح قانون العقوبات ، القسم العام ، الطبعة السادسة ، دار النهضة العربية ،1989.

99- محمود نجيب حسني ، شرح قانون الإجراءات الجنائية ، ط3 ، دار النهضة العربية ، القاهرة ، 1998.

100- مفتاح محمد دباب ، معجم المصطلحات و تكنولوجيات المعلومات و الاتصالات ، الدار الدولية للنشر ، القاهرة 1995.

101- ممدوح خليل بحر، حماية الحياة الخاصة في القانون الجنائي المقارن أطروحة دكتوراه ، جامعة القاهرة مكتبة دار الثقافة للنشر و التوزيع، الأردن ،سنة 1996،ص159.

102- ممدوح عبد الحميد عبد المطلب ، جرائم الكومبيوتر و شبكة المعلومات العالمية مكتبة الحقوق ، الشارقة (الإمارات العربية المتحدة)، الطبعة الأولي ،2001.

103- منصور بن سعيد القحطاني ، مهددات الأمن المعلومات و سبل مواجهتها ، جامعة نايف العربية للعلوم الأمنية ،2008.

104- منصور بن صالح السلمي ، المسؤولية المدنية لانتهاك الخصوصية في نطاق مكافحة جرائم المعلوماتية ، السعودية ، جامعة نايف العربية للعلوم الأمنية ، كلية الدراسات العليا سنة2010.

105- منير محمد الجنبهي ، ممدوح الجنبهي ، جرائم الانترنت و الحاسب الآلي ووسائل مكافحتها ، دار الفكر الجامعي ، الإسكندرية ، دون طبعة ، 2006.

106- نائلة محمد فريد فورة ، جرائم الحاسب الآلي الاقتصادية ، منشورات الحلبي ، الطبعة 01، سنة 2005.

107- نبيل أحمد حلمي الإرهاب الدولي وفقا لقواعد القانون الدولي العام ، دار النهضة العربية ، القاهرة.

108- نبيلة هبة هروال ، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات ، دار الفكر الجامعي ، الإسكندرية ،2007.

109- نسرين عبد الحميد نبيه ، الجريمة المعلوماتية و المجرم المعلوماتي، منشأة المعارف ، الأردن.

110- نضال يوسف إليا ، ورقة علمية بعنوان الاحتيال الالكتروني عبر الانترنت في اطار ندوة علمية ، واقع خدمة الانترنت و انعكاسها على المستهلك العراقي ، جامعة الموصل ، بغداد 23،12،2008، العراق.

111- نهلا عبد القادر المومني ، الجرائم المعلوماتية ، دار الثقافة للنشر و التوزيع ، الطبعة 01، عمان ، سنة 2008.

112- هدى حامد قشقوش ، جرائم الحاسوب الألي في التشريع المقارن ، دار النهضة العربية ، القاهرة ، 1992.

113- هشام محمد فريد رستم ، الجوانب الإجرائية للجرائم المعلوماتية ، مكتبة الآلات الحديثة ، أسيوط ، 1994.

114- هشام محمد فريد رستم ، قانون العقوبات و محاضر تقنية المعلومات ، مكتبة الآلات الحديثة 1992.

115- هلالي عبد اللاه أحمد ، إلتزامات الشاهد بالإعلام في الجرائم المعلوماتية ، دار النهضة العربية ، 1997.

116- هلالي عبد اللاه أحمد ، تفتيش نظم الحاسب الآلي و ضمانات المتهم المعلوماتي ، الطبعة الأولى ، دار النهضة العربية ، القاهرة ، 1997.

117- وحمود عرابي ، الارهاب ،مفهومه ،أواعه ، أسبابه آثاره ، أسباب المواجهة ، دار الثقافة للنشر ، الطبعة الأولى ، القاهرة 2007.

118- ياسر رجب التهامي ، خذع الهاكرز ، دون طبعة ، سنة2008،

المجلات العلمية:

الأطروحات والمذكرات:

1- أحمد مسعود مريم ، آليات مكافحة جرائم تكنولوجيات الإعلام والاتصال في ضوء القانون رقم 09-04 ، مذكرة ماجستير في الحقوق تخصص قانون جنائي ، كلية الحقوق والعلوم السياسية ، قسم الحقوق ، جامعة قاصدي مرباح ، نوقشت بتاريخ 23 /2013/04.

2- بن سعيد صبرينة ، حماية الحق في حرمة الحياة الخاصة في عهد التكنولوجيا ، أطروحة دكتوراة ، جامعة باتنة ، الجزائر، 2015.

3- بهاء فهمي الكبيجي ، مدى توافق أحكام جرائم أنظم المعلومات في القانون الأردني ، رسالة ماجستير في القانون العام ، جامعة الشرق الأوسط ، 2013.

4- بوحليط يزيد ، السياسة الجنائية في مجال مكافحة الجرائم الالكترونية في الجزائر أطروحة دكتوراه ، كلية الحقوق ، قسم القانون الخاص ، جامعة باجي مختار عنابة ، 2016.

5- بوعمرة آسيا ، النظام القانوني لقواعد البيانات ، مذكرة ماجستير ، جامعة الجزائري ، سنة 2005.
6- تركي بن عبد الرحمن الموشير ، بناء نموذج أمني لمكافحة الجرائم المعلوماتية و قياس فاعليته ، أطروحة دكتوراه ، كلية الدراسات العليا بجامعة نايف العربية للعلوم الأمنية ، الرياض ، سنة 2009.
7- ـ حسين سعيد بن يف الغافري ، السياسة الجنائية في مكافحة جرائم الانترنت ، رسالة دكتوراه ، كلية الحقوق ، عين الشمس ، 2005.
8- حقاص صونية ، حماية الملكية الفكرية الأدبية و الفنية في البيئة الرقمية في ظل التشريع الجزائري ، مذكرة ماجستير ، جامعة قسنطينة ، 2002.
9- خمايسية حفيظة ، التعاون الدولي في مكافحة جرائم الانترنت ، رسالة ماجستير ، المركز الجامعي خنشلة ،2012.
10- دردور وسيم ، جرائم المعلوماتية على ضوء القانون الجزائري و المقارن ، رسالة ماجستير ، جامعة قسنطينة ، 2013.
11- سامي عبد الرحمان واصل ، إرهاب الدولة في إطار القانون الدولب العام ، رسالة لنيل درجة الدكتوراه في القانون جامعة عين شمس ، القاهرة 2003.
12- صغير يوسف ، الجريمة المرتكبة عبر الانترنت ، مذكرة ماجستير في القانون تخصص ، القانون الدولي للأعمال ، جامعة تيزي وزو ، 2013.
13- عاقلي فضيلة ،الحماية القانونية للحق في حرمة الحياة الخاصة ،أطروحة دكتوراه ،جامعة قسنطينة ، الجزائر ،2012.
14- قارة أمال ، الجريمة المعلوماتية ، رسالة ماجسير ، جامعة الجزائر ، سنة 2002.
15- مباركي دليلة ، غسيل الأموال أطروحة دكتوراه علوم تخصص ، قانون جنائي باتنة ، الجزائر ، 2008.
16- هدى طلب علي ، الإثبات الجنائي في جرائم الانترنت و الإختصاص القضائي بها ، مذكرة ماجستير ، تخصص قانون عام ، كلية الحقوق ، جامعة النهرين ، 2012.
17- تجسس ،ويكيديا ،الموسوعة الحرة على الموقع الآلي . .http//Ar Wikipédia.arg/wiki

المراجع باللغات الأجنبية.

1- Amanda Hooey .Analysis of the police and criminal evidence act sec 69/computer generates evidence wed journal of current legal issues UK.1996.issue 1.P2
2- Bensoussan Alain (sous la direction de) , Internet : aspect Juridique , édition Hèmes ,Juin 1996 (France) ,page 109
3- Erman (Sahir) les crimes infomatiques et d'autres crimes dans le domain de la technologies informatique en Torquie .R. I .D. P ,1993.P.64

4- http// www- assakina. com ./book .59149.11،6،2016 تاريخ الاطلاع على الموقع بتاريخ
5- U.S.congress.Senate Committee on Governmental affairs. Report (accompany S.2236.95th congress2nd session) Washington .DC.
6- André Lucas ,jean Devréze jean Frayssinent , Droit de L'informatique et de l'internet edition Dallas ,collection thémis (Droit Privé) November 2001 (France) de la page 683 à684
7- DAVID DAVIES.Computer.Virus-the Major Computer Abuse Threat of 1988.p02.
8- Glaser. L'infraction (Int) London .P211 –
9- Philipe M. Stanley computer crime investigation and investigators computer & security nort Holland , 1986 pp - 310 – 311.
10- Rosephillppe les criminalities information que sais-je ? les édition .PUF.1988.P 490.
11- vassilaki(Irini) computer crimes and other crimes against information technology in Greece .Rev . Intern .De.Dr.Pen.P371

المراجع الإلكترونية:

1- أبو سريع أحمد عبد الرحمن ، بحث علمي بعنوان إستخدام الانترنت في تعاطي المخدرات . المخدرات الرقمية . في ديسمبر 2010 ،ص 05، 06 على الموقع www.child-trafficking.org وتم الاطلاع على الموقع بتاريخ 15،06،2017.
2- التوصية الصادرة عن الهيئة الإستثمارية للمجلس الأوروبي ، المرقمة 428، الصادرة بتاريخ 23 جانفي 1970.
3- الحماية الجنائية للبيانات المعلوماتية ذات الصلة بالحق في الحياة الخاصة عل الموقع الآتي www.fsjes-agadir.info تاريخ الإطلاع على الموقع بتاريخ 20-08-2016.
4- إيهاب شوقي ،الإرهاب الإلكتروني ، مقال منشور بتاريخ 11ديسمبر 2015على الموقع الآتي http//www.assakina.com وقد تم الإطلاع على هذا الموقع بتاريخ 18-11-2016
5- بحث علمي بعنوان : تمييز بطاقة الائتمان غيرها من البطاقات المصرفية ، منشور على الموقع التالي www aladalacenter com و قد تم الاطلاع على الموقع بتاريخ 27، 06، 2017.
6- بحث علمي بعنوان : ماهية بطاقة الائتمان ،وأنواعها و طبيعتها القانونية ، منشور على الموقع الآتي : www aladalacenter com وتم الاطلاع على الموقع بتاريخ 21،06،2017
7- ثناء أحمد المغربي ، بحث علمي حول الوجه القانونية لبطاقات الائتمان ، منشور على الموقع الآتي : www droit- dz
8- جابريال ويمان ، الإرهاب على الشبكة العالمية ، منشور على الموقع الآتي www.assakina.comتاريخ النشر 2006و تم الإطلاع على الموقع بتاريخ 29-11-2016.
9- حسين بن سعيد الغافري،الحماية القانونية للخصوصية المعلوماتية في ظل مشروع قانون المعلومات الإكترونية العماني.

10- حيرت علي محرز ، المرجع السابق ، ص 24، 25، ولمزيد من التفصيل أنظر Dr .Kam wing :computer Fraude in the U .K the Picture .computer of security . Bulletin. Vol 9 nal 1986. P09

11- رامي عايش ، شبكة التواصل الاجتماعي عند ما تصبح فخا ، ورقة علمية نشرت بتاريخ 19، 09، 2015 على الموقع التالي www.albayan.com و تم الاطلاع على الموقع بتاريخ 31، 05، 2017.

12- طافر زهيرو برترفاس الهاشمي ، واقع بطاقات الائتمان في الجزائر ، المركز الجامعي بشار، مقال منشور على الموقع www.neevia.com ص 1،2 وقد تم الاطلاع على الموقع بتاريخ 21،06،2017

13- عبد الرحمان عثمان ، الإرهاب ال'كتروني ، أنماطه و سبل مكافحته ، مقال منشور بتاريخ 26-11-2016 www.egynews.net و قد تم الإطلاع على هذا الموقع بتاريخ 02-12-2016.

14- فضيلة عاقلي ، الجريمة الالكترونية و إجراءات مواجهتها من خلال التشريع الجزائري ، مقال منشور على الموقع الآتي : www.jilrc.com بتاريخ 2017.04.10 و تم الاطلاع على الموقع بتاريخ 2017.10.21 .

15- ماجد عمر عبادي ، جريمة الاحتيال عبر البريد الالكتروني ، دراسة مقارنة ، جامعة النجاح الوطنية على الموقع الأتي : www.adelmor.com وقد تم الاطلاع على الموقع بتاريخ 09،05،2017

16- محمد صالح الألفي، جرائم الاعتداء على البطاقات الائتمانية كأحد الأنماط الإجرامية المستحدثة ، ورقة عملية منشورة على الموقع الآتي www.eastlows.com و تم الاطلاع على الموقع بتاريخ 20، 06،2017، ص07.

17- محمد محمد صالح الالفي ، بحث علمي بعنوان :أنماط جرائم الانترنت ، ص 11 منشور على الموقع التالي www.eastlaws.com //http وتم الاطلاع على هذا الموقع بتاريخ 2017.06.28

18- مدير البحث العلمي في وزارة الأوقاف ، الإرهاب الإلكتروني ، الثوابت و المتغيرات ، مقال منشور على الموقع الإلكتروني بتارخ 14-12-201 www.bathpaty.sy وقد تم للإطلاع على هذا الموقع بتاريخ 29-11-2016.

19- مقال بعنوان الجريمة الالكترونية منشور على الموقع الآتي : www.droit-dz.com و قد تم الإطلاع على الموقع بتاريخ 29،10، 2017

20- مقال بعنوان قضية إنتهاك خصوصية رسائل المستخدمين ضد الفيس بوك من الموقع الآتي: https//pro3xplain.com

21- مقال منشور بالجريدة الوطن بعنوان قضايا ، الإرهاب الإسرائلي الإلكتروني ، العرب و التجسس الإسرائلي الإلكتروني على الموقع الآتي:http//alwatan.com/détails/57008.

22- مقال منشور على الموقع التالي www.gnume.com وقد تم الإطلاع على الموقع بتاريخ 2017/05/07.

23- ورقة علمية بعنوان إنتهاك سرية الاتصالات الشخصية ، نشرت على الموقع www.badil.info.com نشرت بتارخ 2014/08/20.

24- ورقة مقدة لمؤتمر أمن المعلومات و الخصوصية في ظل قانون الأنترنت، القاهرة المنعقد في يومي 4-5 يونيو 2008.

25- www.miishawi.com Word.acc.net / vb/shothread K php ?t 7187.

الفهرس