الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة 20 أوت 1955 سكيكدة

كلية الحقوق و العلوم السياسية
قسم الحقوق

الحماية الجنائية للمعطيات الشخصية عبر الأنظمة المعلوماتية

مذكرة متممة لنيل شهادة الماستر في القانون الجنائي والعلوم الجنائية
التخصص: قانون الجنائي والعلوم الجنائية

إعداد الطالب:
- محمد رواق

إشراف الأستاذ:
رابح بازين

غ !

الاسم واللقب	الرتبة العلمية	الصفة	الجامعة
– سلطاني بكير	أستاذ مساعد	رئيسا	جامعة 20 أوت 1955
– رابح بازين	أستاذ مساعد	مشرفا ومقررا	جامعة 20 أوت 1955
– فيلالي منصف	أستاذة مساعد	مناقشا	جامعة 20 أوت 1955

السنة الجامعية: 2019-2020


بسم الله الرحمن الرحيم

قال الله تعالى:

بِسْـــمِ اللَّـهِ الرَّحْمَـٰنِ الرَّحِيـــمِ

﴿ رَبِّ أَوْزِعْنِي أَنْ أَشْكُرَ نِعْمَتَكَ الَّتِي أَنْعَمْتَ عَلَيَّ وَعَلَى وَالِدَيَّ وَأَنْ أَعْمَلَ صَالِحًا تَرْضَاهُ وَأَدْخِلْنِي بِرَحْمَتِكَ فِي عِبَادِكَ الصَّالِحِين ﴾

الآية: 19 سورة النمل

كلمـة شكــر

قال رسول الله صلى الله عليه وسلم: « إذا ساعدكم أحد فكافئوه فإن لم تجدوا بما تكافؤه فاثنوا عليه ».

صدق رسول اله عليه أفضل الصلاة والسلام

أولا وقبل كل شيء نشكر الله عز وجل على أنه هدانا بالقوة لإتمام هذا العمل المتواضع.

أحيطكم بالذكر أنتم أساتذتي الكرام سفراء العلم سراج الظلام لأنكم كنتم وما زلتم مرجعنا وسندنا لأنكم أخذتم بأيدينا وكنتم مصفاد أفكارنا التي لولاكم لما تجسد هذا وما كان هذا العمل ليكون.

نوجه بالشكر للأستاذ الفاضل الكريم المحترم **بازين رابح** الذي لم يبخل علينا بالإرشاد والتوجيه لإتمام هذا العمل بالشكل تام ومثابرته معنا جزاه الله خيرا وأطال في عمره.

وأتقدم بشكري لعائلتي الكبيرة والصغيرة وأصدقائي وكل من ساهم معي بالكثير أو بالقليل من أجل إتمام هذه الدراسة.

والكمال لله وحده عز وجل وإليه يرجع الفضل والثناء

كله هو هم نعم المولى ونعم النصير

المقدمة

مقدمة

إن التطور الهائل الذي شهده كل من مجال تقنية المعلومات ومجال الاتصال والاندماج المذهل الذي حدث بينها فيما بعد، كان المحور الأساسي الذي قامت عليه تقنية المعلومات إذ أصبحت جميع القطاعات المختلفة تعتمد في أداء عملها بشكل أساسي على استخدام الأنظمة المعلوماتية لما تتميز به من عنصري السرعة والدقة في تجميع المعلومات وتخزينها ومعالجتها، ومن تم نقلها وتبادلها بين الأفراد والشركات والمؤسسات المختلفة داخل الدولة الواحدة أو بين عدة دول، فبات يطلق على هذا العصر عصر المعلومات فمنذ وقت ليس ببعيد كان كم المعلومات المتولدة عن التفاعلات البشرية محدودًا إلى حد كبير ولم يشكل حجمها أي مشكلة أمام عمليات تجميعها وتخزينها وإعادة استرجاعها، إلا أنه ومع تقدم البشرية وتزايد معارف الإنسان وعلومه بدأ كم المعلومات يتزايد ويتكاثر وصارت الطرق التقليدية لتجميع وتنظيم هذه المعلومات عاجزة عن تلبية احتياجات المستفيدين منها بكفاءة وفعالية، وأصبح من الضروري اللجوء إلى استخدام أساليب علمية وتقنية متطورة لمراجعة هذه الطفرة، فكان أن أظهرت الحاسبات الإلكترونية، بالإضافة إلى ظهور مستحدثات تقنية كأقراص الفيديو الرقمية وأقراص الليزر، ووسائط الاتصال ... وذلك من أجل تسهيل التحكم في المعلومات ومعالجتها واسترجاعها، وهو ما دعا بالكثير من رجال الاقتصاد والاجتماع إلى وصف

الثورة المعلوماتية بالثورة الصناعية الثانية بالمقارنة مع الثورة الصناعية الأولى التي تحققت في القرنين التاسع عشر والعشرين، ففي حين كان هدف الثورة الأولى إحلال الآلة محل الجهد البدني للإنسان ، فإن هدف الثورة الثانية هو إحلال الآلة محل النشاط الذهني للإنسان.

وفي مرحلة لاحقة من مسار عصر تقنية المعلومات تم التوصل إلى فكرة الربط بين أجهزة الإعلام الآلي، ووسائل الاتصال، الأمر الذي أثمر على ظهور شبكات المعلومات، ولعل أهمها على الإطلاق شبكة الانترنت (شبكة المعلوماتية).

ثم استتبع اتساع ونماء كل من تكنولوجيا الاتصالات والحاسبات من جهة، والبرمجية بما تضمنته من هندسة البرمجيات وصناعتها من جهة أخرى، والاندماج المذهل الذي حدث بينهما إلى الوصول إلى استحداث تقنية نظم المعالجة الآلية للمعطيات.

ومن دون شك تضاعفت أهمية هذه التقنية وازداد الاعتماد عليها في نقل وتبادل المعلومات بالصوت والصورة عبر أنحاء العالم، نظرا لما تتميز به من شمول وسعة محتواها وما توفره من مال وجهد ووقت، وأصبحت بذلك نظم المعالجة الآلية للمعطيات بسبب التقنيات التي تقوم عليها والمتمثلة في الحواسيب والشبكات المعلوماتية أكثر انتشارا في كل القطاعات والمجالات (كالصناعة والتجارة، النقل، الصحة، التعليم، الدفاع

والبحوث....) وبدا من الصعب أن تقوم هذه القطاعات بأداء أعمالها دون الاعتماد بشكل أساسي على هذه التقنية الحديثة، فقد أصبحت من لوازم الحياة المتطورة سواء على المستوى العام أم الخاص، حيث تعتمد المؤسسات الحكومية والخاصة على حد سواء في تسيير أعمالها بشكل أساسي على استخدام نظم المعالجة الآلية.

لكن وعلى الرغم من المزايا الهائلة التي تحققت وتتحقق كل يوم بفضل تقنية المعلومات على جميع الأصعدة وفي شتى ميادين الحياة المعاصرة، فإن هذه الثورة التكنولوجية المتنامية صاحبتها في المقابل جملة من الانعكاسات السلبية والخطيرة جراء سوء استخدام هذه التقنية، ذلك أن الآثار الإيجابية المشرقة لعصر تقنية المعلومات لا تنف الانعكاسات السلبية التي أفرزتها هذه التقنية، نتيجة إساءة استخدام الأنظمة المعلوماتية واستغلالها على نحو غير مشروع وبطرق من شأنها أن تلحق الضرر بمصالح الأفراد والجماعات، الشيء الذي استتبعه ظهور أنماط جديدة من الاعتداءات على تلك المعلومات المخزنة في بيئة افتراضية، ليس هذا فحسب بل سهلت هذه التقنية ارتكاب بعض الجرائم التقليدية، فازدادت هذه المخاطر تفاقما في ظل البيئة الافتراضية التي تمثلها شبكة المعلومات، مما أفرز نوعا جديدا من الجرائم، لم يكن معهودا من قبل عرفت بالجرائم المعلوماتية، أو جرائم تقنية المعلومات.

وعلى ضوء ذلك فإن هذه الظاهرة الإجرامية التقنية أثارت العديد من المشكلات في نطاق قانون الإجراءات الجزائية الذي وضعت نصوصه لتحكم الإجراءات المتعلقة بجرائم تقليدية لا توجد صعوبات كبيرة في إثباتها أو التحقيق فيها وجمع الأدلة المتعلقة بها، مع خضوعها لمبدأ الاقتناع الشخصي للقاضي الجزائي.

وهو الأمر الذي كان عاملا حاسما لتدخل المشرع بنصوص قانونية إجرائية تحمل معها طرقا إجرائية مدعمة من قبل التقنية ذاتها، ليمكن من خلالها استنباط الدليل الذي يتوافق مع الطبيعة التقنية لهذه الجرائم ووسائل ارتكابها، مما أدى إلى ظهور نوع جديد من الأدلة يمكن الاعتماد عليه في إثبات هذه الجرائم من ذات الطبيعة التقنية التي تتميز بها البيئة محل الجريمة المعلوماتية.

وقد كان ذلك بأن قام المشرع الجزائري بتعديل قانون الإجراءات الجزائية بموجب القانون 22/06 المؤرخ في 20 ديسمبر 2006 ، بالإضافة إلى إصداره للقانون 04/09 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام والاتصال، ومن خلالهما أوجد المشرع طرقا إجرائية تتفق والطبيعة التقنية للجريمة المعلوماتية.

مشكلة البحث

ولقد أثارت هذه الأنماط الإجرامية المستحدثة على الإنترنت عدة مشاكل نظرا لأنه من الصعب السيطرة على هذه المشكلة، وعلى الجرائم التي ترتكب عبرها، هذا من جهة،

ومن جهة أخرى من الصعب اكتشاف هذه الجرائم أو تحديد مصدرها، لأن الجاني يستخدم اسما مستعارا أو غير حقيقي.

ومن الصعب أيضا إيقاف ارتكاب الجريمة عبر الشبكة بسبب سرعة نشر المعلومات وتسجيلها على الحاسبات الخادمة في الخارج مما يجعلها تجوب العالم في لحظات.

وذكرنا بأن هذه الجرائم ترتكب عن طريق أنماط إجرامية مستحدثة، وتتمثل هذه الأنماط الإجرامية في الفيروسات و سرقة الأسرار السياسية و التجارية وهذا يدفعنا إلى طرح الاشكالية التالية:

الاشكالية:

إلى أي مدى وفق المشرع الجزائري في الحماية القانونية للمعطيات الشخصية عبر الأنظمة المعلوماتية؟

ولتحليل الإشكالية نطرح التساؤلات التالية:

- ماهي النظام المعلوماتي والجريمة المعلوماتية؟
- ماهي القيمة القانونية للدليل الرقمي؟

- ماهي الجزاءات والعقوبات المقررة لجرائم الاعتداء الماسة بالأنظمة المعلوماتية، وكيف تتم إجراءاتها؟

ولدلك اقتضت دراسة موضوع البحث تقسيمه إلى فصلين تعقبهما خاتمة وذلك على النحو الآتي:

- الفصل الأول: استعرضت فيه الإطار المفاهيمي لنظام المعلوماتي و الجرائم الماسة للأنظمة المعلوماتية وقسمته إلى مبحثين:

المبحث الأول: ماهي النظام المعلوماتي في الجزائر ق(04-15) .

المبحث الثاني: أهمية نظام المعالجة الآلية للمعطيات للحماية الفنية.

المبحث الثالث: ماهية الجريمة المعلوماتية وأساليب ارتكابها وأطرافها

أهمية البحث:

ترجع أهمية هذا البحث إلى أنه من الموضوعات الحديثة المرتبطة بتطور وسائل الاتصالات الحديثة.

وإن اختيار الحماية الجنائية للمعلومات على شبكة الانترنت لما تمثله المعلومات من قيمة اقتصادية لا تقل بأي حال من الأحوال عن قيمة الأشياء المادية، ويتعين وضع نظام ملائم لحمايتها من الناحية الجنائية .ومما زاد من أهمية هذا البحث هو ظهور أنماط إجرامية مستحدثة بشأن الاعتداء على المعلومات على شبكة الانترنت .مما جعل الفقه

والقضاء المقارن يحاول التصدي لهذه الظاهرة وهذا ما سوف نعالجه في موضوعنا وذلك ببيان مفهوم الجريمة المعلوماتية، وأنواعها، والجهود المبذولة لمكافحتها، وذلك بمحاولة لسد الفراغ التشريعي في القوانين القائمة.

أهداف البحث:

إن الهدف من هذه الدراسة يتمثل في الآتي:

- التعرف على كيفية إسباغ الحماية الجنائية على شبكة الانترنت وتحديد المقصود بالجرائم المعلوماتية والمجرم المعلوماتي.

- بيان مدى صلاحية النصوص التقليدية في التعامل مع جرائم المعلومات المستحدثة.

منهج البحث:

ومن خلال الدراسات السابقة والتي تطرقت في مجملها على الإطار المفاهيمي و القانوني للحماية الجنائية سواء الشخص الطبيعي أو المعنوي من شتى الأطروحات والمدكرات منها الدكتوراه، والماجستير، والماستر.

الفصل الأول:

ماهيــة الأنظمة المعلوماتية والجرائـم المتعلقة بها ودوافعــها

يمثل نظام المعلوماتية المسألة الأولية أو الشرط الأولي الذي يلزم تحققه حتى يمكن البحث في توافر أو عدم توافر أركان أي جريمة من جرائم الاعتداء على هذا النظام،[1] فإذا أثبت تخلف هذا الشرط الآلي لا يكون هناك مجال للبحث حول الجرائم الواقعة عليه، ونشير هنا إلى أنه وكما سبق الذكر أن الاعتداء على المعلومات المعالجة بواسطة النظام المعلوماتي هي ما يسمى بالجرائم المعلوماتية وهي الطائفة التي تنتمي إليها الجرائم الواقعة على المعلومات السرية المعالجة بواسطة النظام المعلوماتي، ويؤدي توافر هذا الشرط إلى الانتقال إلى المرحلة التالية وهي بحث توافر أركان أي جريمة من الجرائم محل الدراسة، إذ أن هذا الشرط يعتبر عنصرا لازما لكل منها ولذلك يكون من الضروري تحديد مفهوم نظام المعلوماتي ولإيضاح المقصود بنظام المعلوماتية يتعين علينا أن نتعرض لتعريف نظام المعلوماتية (المبحث الأول) وأهمية إخضاع نظام المعلوماتي للحماية الفنية وماهية الجريمة المعلوماتية وأساليب ارتكابها وأطرافها.

[1] – أطلق الفقهاء على النظام المعلوماتي اسم الحاسب الآلي، حيث أن لفظ الحاسب الآلي يعتبر قاصرا على جهاز الحاسب الآلي بمكوناته من شاشة العرض ولوحة المفاتيح ووحدة التشغيل، بينما أصبح في الوقت الحاضر يتصل بمكونات أخرى.

المبحث الأول: ماهية النظام المعلوماتي في الجزائر في القانون (04-15)

عبر المشرع الجزائري عن الجريمة المعلوماتية في القانون (04-15) بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات معبرا في ذلك عن النظام المعلوماتي بنظام المعالجة الآلية للمعطيات، ذلك أن هذه الأخيرة ترتكب بواسطة وعلى النظام المعلوماتي رغم أن محلها هو المعلومات ولأن الأمر يتطلب ضرورة توضيح مفهوم النظام المعلوماتي كان لابد من التطرق لتعريفه (المطلب الأول) ومن فرعه الأول: اصطلاحا وقانونيا وفي الفرع الثاني مفهوم المعالجة الإلكترونية للبيانات والتعرف على مكوناته في المطلب الثاني.

المطلب الأول: مفهوم النظام المعلوماتي:

يستعمل مصطلح النظام أو الأنظمة بصورة واسعة في لغة خطابنا اليومي وبأشكال ومضامين مختلفة، فنجد الكثير من الناس يستعملونه للتعبير عن أسلوب ونمط معيشتهم الاجتماعية، الاقتصادية والسياسية، فيقال مثلا: نظام التعليم الكمبيوتر، الاقتصاد وغيرها، والملاحظ أن سعة انتشار هذا المصطلح يعود في الواقع إلى أن

الإنسانية تعيش في عالم يتكون من عدد غير محدود من الأنظمة إذ أن هذا العصر هو عصر الأنظمة.[1]

الحقيقة أن عملية نظام المعلوماتي تحتاج آلية منظمة تتولى عمليات جمع وتوفير المعلومات اللازمة ومعالجتها هذا وللحاجة إلى إجراءات ووسائل تساعد على القيام بذلك فظهر مصطلح "نظام المعلومات" والتي تعرف أيضا أنها «مجموعة الإجراءات التي تقوم بتجميع ومعالجة وتخزين وتوزيع المعلومات بهدف دعم عمليات صنع القرار»، وفي نفس الوقت ظهر مصطلح نظام المعالجة الآلية باعتباره الوساطة التي أفرزتها عمليات الدمج بين كل الوسائل الحوسبة والاتصال والوسائط المتعددة بما قدمته من قدرة على رقمنة الصورة وتحويلها إلى مادة تفاعل بين المستخدم وبين المحتوى[2] وعلى الدمج بين النظام والمعالجة لابد من التطرق إلى تعريف النظام المعلوماتي.

الفرع الأول: تعريف النظام المعلوماتي

تعددت التعريفات التي قيلت في النظام المعلوماتي بين الفقهية والتشريعية وسيتم التطرق إليها كالتالي:

[1] – رشيدة بوبكر، جرائم الاعتداء على نظام المعالجة الآلية في التشريع الجزائري المقارن، ط1، منشورات الحلبي الحقوقية، بيروت، لبنان، 2012، ص 49.

[2] – رشيدة بوبكر، مرجع سابق، ص 50، مشار إليه لدى أيمن عبد الله الفكري، جرائم نظم المعلومات، دراسة مقارنة، دار الجامعية الجديدة الإسكندرية، 2007، ص 224.

أولا: التعريف الاصطلاحي للنظام المعلوماتي

فالنظام هو مصطلح مشتق من الكلمة اللاتينية "Systema"، التي تعني الكل المركب من عدد من الأجزاء ووفقا للمعجم الشامل فإن النظام هو عنصر مركب يتم تشكيله من عدة وحدات متميزة متصلة مع بعضها البعض بواسطة عدد من العلاقات، التي تنشأ لتحقيق التفاهم والترابط بين هذه المكونات أو الوحدات المختلفة، وفي معجم "La rousse" في الجزء العاشر منه تم تعريف النظام بأنه يتحقق في مفهومين الأول "اعتبار النظام مجموعة من العناصر التي تمارس وظائفها من خلال علاقتها بطريقة مماثلة"، والثاني يقصد به: "مجموعة الأوامر التي تتم بوسائل متعددة من أجل الحصول على نتائج محددة"[1]، وعرف أيضا أنه " مجموعة من العناصر أو الأجزاء المترابطة التي تعمل بتنسيق تام وتفاعل تحكمها علاقات وآلية عمل معينة في نطاق محدد لتحقيق غايات مشتركة وهدف عام"[2]

وعرفه بعض الفقهاء أيضا "أنه مجموعة المكونات ذات علاقة متداخلة مع بعضها تعمل على نحو متكامل داخل حدود معينة لتحقيق هدفا أو أهداف مشتركة في بيئة ما وفي سبيل ذلك يقبل مدخلات ويقوم بالعمليات وينتج مخرجات ويسمح باستقبال مدخلات

[1] – رشيدة بوبكر، مرجع سابق، ص ص، 49،50.

[2] – صليحة علي صداقة، الأبعاد القانوني والأخلاقي للمعلوماتية الصحية، دار المطبوعات الجامعية، الإسكندرية، 2017، ص 23.

مرتدة"[1]، وكان هذا التعريف على أساس أن النظام يختلف باختلاف المجال الذي ينتمي إليه.

ثانيا: التعريف القانوني للنظام المعلوماتي

لم يعرف المشرع الفرنسي النظام المعلوماتي، في حين اقترح مجلس الشيوخ الفرنسي مفهوم لنظام المعالجة الآلية للمعطيات بمناسبة تعديل قانون العقوبات هو: "أنه كل مركب يتكون من وحدة أو مجموعة وحدات معالجة والتي تتكون كل منها من الذاكرة والبرامج والمعطيات وأجهزة الإدخال والإخراج وأجهزة الربط، والتي يربط بينها مجموعة من العلاقات التي عن طريقها تتحقق نتيجة معينة وهي معالجة المعطيات، وعليه يكون هذا المركب خاضع لنظام الحماية الفنية"[2]

وتجدر الإشارة أن القانون الفرنسي المسمى بقانون "قودفران" "Gogfrai, Loi"[3] نسبة إلى أحد النواب الفرنسيين المسمى بقودفران الذي عدل بصفة نهائية نظرة المشرع

[1] – طارق طه، مقدمة في نظم المعلومات الإدارية والحاسبات الآلية، الطبعة الثالثة، منشأة المعارف الإسكندرية، 2000، ص 16.

[2] – Houande Alain ..Linant de Bellefont xavier, pratique du droit de l'informatique, edition Delmas (5 edition avril 2002, (France), p 250.

[3] – القانون رقم 575/2004 لجوان 2004 المتعلق بالثقة في الاقتصاد المعلوماتي، الميمم في 11 جويلية 2010 تحت عنوان "مكافحة الإجرام المعلوماتي" الجريدة الرسمية رقم 143 المؤرخة في 24 جوان 2004.

الفرنسي حول اعتبار الأنظمة المعلوماتية عن مال في حد ذاته، ولابد على قانون العقوبات أن يحميه من المساسات غير المشروعة.[1]

وعرفته نص المادة الأولى من الفصل الأول تحت تسمية المصطلحات من اتفاقية بودابست كالتالي: "كل آلة سواء بمفردها أو مجموعة عناصر أخرى، تنفيذا لبرنامج معين، بأداء معالجة آلية للبيانات"، ومنه يعتبر نظام المعلومات جهاز يتكون من معدات وبرامج قائمة للمعالجة الآلية للبيانات الرقمية، ويمكن أن تشمل على طرق سهلة لإدخال واستخراج وتخزين البيانات، ويمكن أن تكون متفرقة أو متصلة مع أجهزة مماثلة أخرى داخل الشبكة.[2]

وعرفته الاتفاقية العربية[3] لمكافحة جرائم تقنية المعلومات لسنة 2012 في الفصل الأول منها في المادة الثانية في تعريفها لبعض المصطلحات أنه "النظام المعلوماتي مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات والمعلومات" ومهما كان أسلوب معالجتها للمعطيات فإنها تشكل نظام معلوماتي.[4]

---

[1] – Lucas André, Jean Devreze, Jean Frayssinet, Droit de l'informatique et l'internet, collection themis (droit privé), 2001, (France, p 679 – 680.

[2] – كما عرفت المذكرة التفسيرية لاتفاقية بودابست المعالجة الآلية على أنها: "تعني مجموعة من العمليات التي تطبق على البيانات من خلال برنامج معلوماتي".

[3] – الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2012 عن الموقع الإلكتروني.
http://www.lawjo.net/vb/showthread/php?26439

[4] – Houande Alain, Op at, p 250.

ويقصد أيضا بنظم الحاسب الآلي كل مكونات الحاسب المادية والمعنوية وشبكات الاتصال الخاصة به، الأشخاص والتي يمكن بواسطتها تحقيق وظيفة أو هدف محدد،[1] ويعرف أيضا أنه "هو النظام الذي يحتوي على معلومات آلية تقنية مسماة محمية بإجراء أمني".[2]

كما أورد قانون الأونيسترال النموذجي بشأن التجارة الإلكترونية في مادته الثانية تعريف النظام المعلوماتي باعتباره " النظام الذي يستخدم لإنشاء رسائل البيانات وإرسالها واستلامها أو تخزينها أو لتجهيزها على أي وجه آخر"[3]

ولقد نص عليه المشرع الجزائري بموجب الفقرة ب من المادة 2 من القانون رقم 04/09 لسنة 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته بأنه "أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آلية المعطيات تنفيذا لبرنامج معين".

أما المشرع الفرنسي، فلم يتطرق لتحديد مفهوم نظام المعالجة الآلية للمعلومات موكلا مهمة ذلك إلى الفقه والقضاء، حيث عرفه الفقه الفرنسي أنه "كل مركب يتكون من

[1]– محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، الإسكندرية، 2004، ص 56.

[2] – Guillaume Champy, la fraude informatique, tome 1, presse universitaires d'Aix–Marseille, 1992, p 88.

[3] – قانون الأنيسترال كان بموجب القرار الذي اتخذته الجمعية العامة للأمم المتحدة بناء على تقرير اللجنة السادسة (1/51)، ص 628.

وحدة أو مجموعة من أو مجموعة وحدات معالجة تتكون كل منها من الذاكرة والبرامج والمصطلحات وأجهزة الربط والتي يبينها مجموعة من العلاقات عن طريقها تحقق نتيجة معينة وهما معالجة المعطيات على أن يكون هذا المركب خاضع لنظام الحماية الفنية.[1]

ومما سبق نستنتج أن هناك من يأخذ المفهوم الموسع للنظام والعكس وفي الحقيقة ويمكن القول أن نظام المعالجة الآلية للمعطيات هو تعبير يخضع للتطور السريع الذي يلحق بالبيئة الرقمية[2].

الفرع الثاني: مفهوم المعالجة الإلكترونية للبيانات

المعالجة بصفة علامة هي تحويل شيء ما من صورته الطبيعية إلى أخرى تعبر عن نتيجة ما يمكن الاستفادة منها أي أن عملية المعالجة هي تحويل أي شيء من شكله الخام إلى شكل جديد يستفاد منه أي أن المعالجة الإلكترونية هي عبارة عن معالجة بواسطة أجهزة إلكترونية وهذه الأجهزة بها يقصد على العموم الحاسوب لأنه مكون من عدة أجهزة تعمل كلها بواسطة شرائح إلكترونية، وهذه الشرائح الإلكترونية هي المتحكم في كل عمليات المعالجة وبالتالي فهي معالجة إلكترونية، وللتفصيل أكثر سيتم تحديد المقصود بالمعالجة والمعالجة الآلية (أولا) وفقا لفكرة أساسية للحاسب الآلي (ثانيا).

[1] – http://www.droit.com/forum/Showthread.phpt=5955 يوم الاطلاع على الموقع 2020/08/19.

[2] – http://faculty.psau.edi.Sa/filedownload/doc-13-ppt 03f84bb247bf032f7a7d94d5852caec7original.ppt تاريخ الإطلاع على الموقع 2020/08/19.

أولا: المقصود بالمعالجة والمعالجة الآلية للبيانات

يمكن للحاسب الآلي القيام بالمعالجة الإلكترونية للبيانات ولكن بشرط وجود خطوات المعالجة أي وجود برنامج المعالجة وهنا البرنامج هو عبارة عن خطوات متسلسلة كتبت بأسلوب يفهمه الحاسوب وزود بها الحاسوب بطريقة ما كي يقوم بتطبيقها كلما دعت الحاجة.[1]

أ- المقصود بالمعالجة:

المعالجة بصفة عامة هي تحويل شيء ما من صورته الطبيعية إلى صورة أخرى تعبر عن نتيجة ما يمكن الاستفادة منها فمعالجة الحديد الخام يمكن أن تعطينا أشكال عديدة من معدات حديدية ومعالجة بعض الأرقام قد تعطينا إجمالي المصروفات أو الربح وهكذا بعبارة أخرى إن عملية المعالجة هي تحويل أي شيء من شكله الخام إلى شكل جديد يستفاد منه في حياتنا بشكل عام، ويعني بكلمة "آلية" أي بدون تدخل بشري مباشر.[2] كما تعني المعالجة عملية تحويل البيانات من شكل إلى آخر.[3]

[1] – أنظر كذلك الموقع الإلكتروني http://www.mprog.org/comp1.hfm الاطلاع عليه يوم 2020/08/19.

[2] – المادة الأولى من الفصل الأول – المصطلحات– من اتفاقية بودابست السالفة الذكر.

[3] – http://www.vercon.sci.eg/Matrials/1-4.html يوم الاطلاع على الموقع 2020/08/30.

ب- المقصود بالمعالجة الالكترونية للبيانات:

المعالجة الإلكترونية هي ليست معالجة يدوية أو ميكانيكية أو حرارية بل هي وبكل بساطة عبارة عن معالجة بواسطة أجهزة إلكترونية ومن هذه الأجهزة هي الحاسوب لأنه مكون من عدة أجهزة تعمل كلها بواسطة شرائح إلكترونية وهذه الشرائح الإلكترونية هي المتحكم في عمليات المعالجة وبالتالي فهي معالجة إلكترونية.

والمعالجة الآلية للمعطيات وفق ما هو متعارف عليه في المجال التقني "مجموعة من العمليات المترابطة والمتسلسلة بدءا من جمع المعطيات و إدخالها إلى نظام المعالجة الآلية ومعالجتها وفقا للبرامج التي تعمل بها نظام المعالجة الآلية وصولا إلى تحليلها وإخراجها بصورة معلومات"[1].

وعرف القانون الفرنسي[2] رقم 17/78 من خلال المادة 5 منه عملية المعالجة أنها "عبارة عن مجموعة من العمليات التي تتم آليا، وتتعلق بالتجميع والتسجيل والإعداد والتعديل والاسترجاع والاحتفاظ ومحو المعلومات ومجموعة العمليات التي تتم آليا بغرض استغلال المعلومات وخصوصا عمليات الربط والتقريب وانتقال المعلومات ودمجها مع بيانات أخرى أو تحليلها للحصول على معلومات ذات دلالة خاصة".

[1] – رشيدة بوبكر، مرجع سابق، ص 52.

[2] – القانون رقم 17/78 المؤرخ في 16 جانفي 1978 المتعلق بالحريات والمعلوماتية المعدل بموجب القانون رقم 2004/801 المؤرخ في 6 أوت 2004 الخاص بالمعالجة الآلية للمعلومات الرقمية.

أما عن المقصود بمعالجة المعطيات فهي مجموعة العمليات التي تحول المعطيات إلى عمليات، حيث إن المعطيات أو البيانات هي مجموعة الحقائق الأولية والأشكال التي عادة ما تكون غير منظمة أو معالجة، في حين أن المعلومات هي البيانات المعالجة.

وفي إطار المادة الأولى من اتفاقية بودابست من الفصل الأول يقصد بمعالجة البيانات هي مجموعة عمليات تطبق على بيانات ويتم تسجيلها عن طريق تنفيذ برنامج المعلوماتية.[1] تأسيسا على ما سبق فإن المعلومة الخام هي البيانات ويمك أن تقدم تحت أشكال مختلفة كالأرقام والكتابات المجمعة والرموز والإحصائيات الخام، وأن كل معلومة ليست بيان ولكن كل بيان هو معلومة،[2] ومنه يعتبر صوت الإنسان بيانات وضغط دمه وقوة الرياح بيانات وكثافة الضباب بيانات والضحك بيانات وغيرها وقد سبق التفصيل في مدلول البيانات أعلاه.

ثانيا: المقصود بفكرة عمل الحاسوب

تتلخص فكرة عمل الحاسوب، في كونه جهاز لديه القدرة على المعالجة وذلك من خلال الشرائح الإلكترونية التي حاول صانعيها أن يقلدوا فيها عمل الدماغ البشري وكيفية معالجته لأمور الدنيا بشكل عام.

[1] – المادة الأولى من الفصل الأول – المصطلحات– من اتفاقية بودابست السالفة الذكر.

[2] – رشدي محمد علي محمد عيد، الحماية الجنائية الموضوعية للمعلومات عبر شبكة الإنترنت، دار النهضة العربية، القاهرة، 2013، ص 11.

من ذلك يمكننا أن نقول أن الحاسوب يمكنه القيام بالمعالجة ولكن شرط وجود خطوات المعالجة أي وجود برنامج المعالجة وهذا البرنامج هو عبارة عن خطوات متسلسلة كتبت بأسلوب يفهمه الحاسوب، وزوّد بها هذا الأخير بطريقة تقنية يقوم بتطبيقها كلّما دعت الحاجة، حيث تمثل البرامج الكيان المعنوي إضافة إلى المعطيات.[1]

جهاز الحاسوب هو عبارة عن جهاز له القدرة على المعالجة وهي أهم ميزة يمتلكها ولكي تنجح عملية المعالجة يجب تزويد الحاسوب بالبرنامج ولكون المعالجة تتم على بيانات ما فإنه يجب أ يتم إدخال هذه البيانات إلى الحاسوب وسيقوم بمعالجتها وفقا للبرنامج المستخدم، وفي النهاية سيقوم الحاسوب بإخراج المعلومات أو النتائج التي تحصل عليها كحصيلة نهائية معالجة.

المطلب الثاني: مكونات النظام المعلوماتي

الفرع الأول: مدخلات

وهي البيانات التي تغذي بها النظام، فجميع أنواع البيانات وبعض المعلومات المسترجعة أحيانا، توضع في نظام الحاسوب من خلال وسائل إدخال مناسبة وفي مقدمتها لوحة مفاتيح والفأرة والماسح الضوئي.

[1] – أنظر الموقع الإلكتروني، http://www.mproug.org/Ccomp1.htm تاريخ الاطلاع عليه 2020/08/14.

الفرع الثاني: المخرجات

وهي المعلومات التي تنتج عن النظام، وهنا ينبغي أن تنتقل البيانات والمعلومات المعالجة من وحدة المعالجة المركزية إلى وسيلة إخراج مناسبة للمعلومات، مثل: شاشة الحاسوب أو وسيلة مناسبة أخرى.

الفرع الثالث: تشغيل وتحليل

وهي الطرق والوسائل المختلفة، لتشغيل المدخلات حتى يمكن التوصل إلى المخرجات ويطلق على عملية التحليل والتشغيل اسم "المعالجة".

والحقيقة أن وجود نظام المعالجة الآلية للمعطيات هو شرط أساسي لكي نبحث ما إذا كان هناك اعتداء على نظام المعالجة الآلية من عدمه، وبالنظر إلى أهمية المعلومات المعالجة آليا وقيمتها فقد اعتبرت مالًا بل وتفوق المال في قيمتها وبالتالي جرم الاعتداء عليها.[1]

فكما يعتبر وجود النظام المعلوماتي شرط أولي في الجرائم المعلوماتية، فهل يعتبر أيضا إخضاعه للحماية الفنية شرط أساسي أم لا ؟. وهذا ما سيتم التفصيل فيه من حيث التطرق إلى أهمية إخضاع نظام المعالجة الآلية للمعطيات للحماية الفنية.

[1] – عبد الفتاح بيومي حجازي، مكافحة جرائم الكومبيوتر والإنترنت في القانون العربي النموذجي، ط1، دار النهضة العربية، الإسكندرية، 2009، ص 66.

المبحث الثاني: أهمية نظام المعالجة الآلية للمعطيات للحماية الفنية

بمناسبة دراسة الحماية الجزائية للمعلومات الإلكترونية السرية أو ما تم التعبير عنه بالأسرار المعلوماتية، والتي يتم معالجتها بواسطة النظام المعلوماتي من جهة، ومن خلال هذه الدراسة لطالما تم طرح سؤال مضمونه هل يشترط إخضاع النظام المعلوماتي للحماية الفنية من عدمه ليحظى بالحماية القانونية ؟ بعبارة أخرى هل من الضروري حتى يحمي القانون البيانات السرية المعالجة آليا داخل النظام المعلوماتي أن يكون المسؤول عنه قد عنى بتأمين ذلك النظام، بأن يخضعه كحماية فنية أو لا يشترط ذلك ؟. ومنه فأيّ نظام معلوماتي فهو محل حماية قانونية رغم عدم تأمينه فنيًا.

للإجابة على هذا التساؤل سنتعرض لبعض الآراء الفقهية أحدهم يذهب إلى ضرورة تأمين النظام المعلوماتي ليحظى بالحماية الفنية وآخر العكس.

المطلب الأول: الاتجاه المقيد للحماية الفنية

يذهب رأي إلى ضرورة وجود نظام أمني، ذلك أن القانون يجرم الاعتداء على نظم الأمن المتضمنة في النظام المعلوماتي ويستند أنصار هذا الرأي لعدة حجج منها إنّ الاعتداء على النظام الأمني – شرط مفترض– لقيام الجرائم التي تتعلق بالمعلوماتية، والعدالة تقتضي عدم العقاب على فعل يعد اعتداء على حق لم يتحوط له صاحبه فضلا

عن أن التسليم برأي غالبية الفقه يعني توسعا في مجال التجريم، فكل دخول غير مشروع جريمة وذلك أمر غير منطقي.[1]

فيرى أصحاب هذا الاتجاه ضرورة قصر الحماية الجنائية على تلك الأنظمة التي وفر لها أصحابها حماية فنية فحسب، ويستندون في تبرير رأيهم هذا إلى الحجج الآتية:

- أن المنطق السليم والعدالة يقتضيان قصر الحماية الجنائية على الأنظمة المحمية بأنظمة أمان فحسب ذلك لأن القانون الجنائي لا يساعد إلّا الأشخاص المجتهدين، ومن غير المعقول حماية معلومات هامة تركها المسؤولون عنها دون أي إجراءات تكفل لها الحماية ولا ينبغي حماية حق لم يتحوط صاحبه، وهذا يجعل الأشخاص لا يلجأون إلى القانون الجنائي إلا عندما تعجز تلك التدابير الوقائية عن حماية أنظمتهم.

وقد قاس أصحاب هذا الرأي جريمة الدخول غير المصرح به على جريمة انتهاك حرمة المسكن حيث أن هذه الأخيرة لا تقوم بمجرد دخول المسكن بغير رضا صاحبه وإنما يجب لقيامها أن يصحب ذلك الدخول وسائل تدل على عدم رضا صاحب المسكن كالتهديد أو الاحتيال.[2]

[1] – خيثر مسعود، الحماية الجنائية لبرامج الكومبيوتر، دار الهدى للطباعة والنشر، عين مليلة، الجزائر، 2010، ص 112.

[2] – محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي، دار الجامعة الجديدة للنشر، الإسكندرية، بدون طبعة، 2007، ص 134.

• ومن جهة أخرى أن أنظمة الحاسبات تتميز بالانفتاح على الخارج عبر شبكات المعلومات، هذه المعلومات قد تكون من الأهمية بحيث يصبح من الواجب حمايتها، وإلّا أصبح الدخول إليها سهلا، وهذه الأنظمة لها القابلية للتعرض لهجومات ولهذا وجبت حمايتها.[1]

• إن القانون المعلوماتية والحريات الفرنسي الصادر في 06 جانفي 1978 يعتبر سابقة تشريعية مهمة في هذا الشأن وإذ يفرض هذا القانون على مالك النظام أو المسؤول عنه، التزاما بتأمين هذا النظام وفقا لمادة 29. وكذلك المادة 226 فقرة 17من قانون العقوبات تعاقب على كل إجراء أو معالجة آلية لمعلومات اسمية دون اتخاذ الإجراءات اللازمة لتأمين هذه المعلومات، ولا ينبغي حصر هذا الأمر في المعلومات الشخصية، وإنما يجب أن يشمل كل المعطيات بما فيها التي تحميها المادة 323-1 من قانون العقوبات الفرنسي، فلا تحظى بالحماية إلا تلك المعطيات المحمية بأجهزة أمان.

إن إقامة الدليل على قيام الركن المادي للجريمة والتحقق من توافر القصد الجنائي لدى فاعلها يتطلب وجود أنظمة الأمان، فاختراق هذه الميزة يسهل عملية الكشف عن الجريمة لأنه يترك في العادة أثرا يدل عليه، كما أم هذا الاختراق يساعد على التحقق من وجود القصد الجنائي لدى الفاعل، وعليه فإن التفسير السليم لنص تجريم الدخول غير

[1] – محمد خليفة، المرجع نفسه، ص 134.

المصرح به، يقتضي قصره على اختراق الأنظمة المحمية دون سواها، فبينما يتطلب فعل الدخول كان مشروعا.[1]

إن اشتراط النّص بأن يكون الفعل قد تم عن طريق الغش وهو شرط يتصل بمجريات الجريمة لأن فعل الدخول في حد ذاته، هو أسلوب محايد لا يدل بنفسه على عدم المشروعية ولم يجد المشرع أبدا من اشتراط الغش وهو الذي يتحقق باختراق نظم الأمان.[2]

المطلب الثاني: الاتجاه الموسع للحماية الجنائية

ورأي آخر يقتضي بعدم ضرورة وجود الحماية الفنية رغم قوة حجج المنادين بتضييق الحماية الجنائية وحصرها في الأنظمة المحمية فقط فإن هناك اتجاه آخر يرى بأن أنظمة الحاسبات الآلية وما تحويه من المعطيات لابد أن تحظى بالحماية بغض النظر عن احتوائها أنظمة الأمان أو عدم احتوائها.

ويرد أن سكوت القانون يدل على عدم اشتراطه لهذا الأمر، ومن المعروف أن المبادئ العامة في تفسير القانون الجنائي تقتضي عدم إضافة شرط لم ينص عليه القانون، فالنص جاء عاما ولم يفرق بين نظام محمي وآخر غير محمي.

[1] – محمد خليفة، المرجع نفسه، ص 135.

[2] – محمد خليفة، المرجع نفسه، ص 136.

إن الأخذ بفكرة نظام الأمان يضعنا أمام مشكل عويص الحلّ، وهو تحديد متى يصلح نظام ما لأن يكون نظام أمان ؟ وما هو الحد الأدنى من الأمان ؟ أي كيف نحدد نوع الأمان وكمّه ؟.

هذا وقد كان القضاء الفرنسي واضحاً في عدم أخذه بالشرط المتقدّم ، وتأكّد ذلك في حكم لمحكمة استئناف باريس صدر سنة 1994، بيّن أنّه ليس من اللازم لقيام جريمة الدخول غير المصرح به بأن يكون فعل الدخول قد تمّ بمخالفة تدابير أمنيّة، وأنّه يكفي لقيام الجريمة أن يكون الدخول قد تم ضدّ إرادة المسؤول عن النظام. كما أن الاجتهاد القضائي الفرنسي يعتبر أن جريمة الدخول تتحقق في غياب الحماية الفنية.[1]

وفي حكم أخر ذهبت إليه محكمة استئناف باريس أدانت المتهم في قضية " bluetouf" حيث قام القرصان باختراق نظام معلوماتي لوكالة الوطنية لأمن الصحة والتغذية والبيئة والعمل وسرقة الملفات بالرغم من أن دخول النظام لم يكن محميا.

والوضع في قانون العقوبات الجزائري مشابه للوضع في قانون العقوبات الفرنسي، إذ لم تشر المادة 394 مكرر إلى ضرورة أن سكون نظام المعالجة الآلية للمعطيات محميا بجهاز أمان، وإنما جاء النص عاما، وعليه فإن جميع الأنظمة سواء كانت محمية أو غير محمية تحظى بحماية هذا القانون.

[1] – Valérie SEDALLIAN; Légiférer sur la sécurité informatique: la quadrature du cercle? 5décembre 2003, P11 sur le site www.juriscom.net

إلا أنه وكما يذهب الرأي الأول أن المسألة واضحة ولا تحتاج إلى الآلية للمعلومات صدرت دون أن تتضمن شرط الحماية الفنية، والمبادئ المستقرة في القانون الجنائي أنه لا يجوز تقييد النص المطلق أو تخصيص النص العالم طالما لم ينص المشرع على ذلك، سيما أن عدم ذكر شرط الحماية الفنية يعني أن المشرع قد أراد استبعاد هذا الشرط.

كما أن المناقشة البرلمانية تؤكد أنها كانت ضد اشتراط هذه الحماية، وحتى ولو ورد نص الذكر على هذه الحماية كشرط ضمن الأعمال التحضيرية للقانون، فإنه لا يكتسب أهمية لعدم إلزامية هذه الأعمال التحضيرية وإنما يستعان بها في تفسيره غمض من النصوص أو تعارض مع بعضه البعض. وتطبيقا لذلك فإنه يمكن القول أنه لا يشترط لوجود الجريمة أن يكون الدخول إلى النظام مقيدا لوجود حماية فنية.[1]

وكذلك يذهب أنصار هذا الرأي في الفقه الفرنسي دائما وفي تعزيز وجهة نظرهم إلى قياس جريمة الدخول غير المشروع على جريمة السرقة، بحيث أن المال يتمتع بالحماية الجنائية من السرقة سواء كان في حماية صاحبه أو لم يكن، فالجريمة تمت

[1] – خثير مسعود، مرجع سابق، ص ص، 112، 113.

بغض النظر عن الصعوبة التي يتلقاها الجاني، وأنه لا يمكن للجاني أن يدفع بعدم تحوط صاحب المال فتمت سرقته.[1]

وبناءا على ما تقدم فإن نظام الحماية الفنية لا يدخل عنصرا في جرائم المعطيات، فهذه الأجهزة تقوم بالاعتداء على نظام المعالجة الآلية للمعطيات سواء كان محميا بنظام الأمان، أو لم يكن محميا فالحماية الجنائية إذا عامة على كل الأنظمة.[2]

وإضافة إلى هذه النتيجة يقال أن الوقاية خير من العلاج وبالتالي نحن نرى أنه لابد من الحماية الفنية رغم أن المشرع لم يشترطها، لأنه كما نوضع الأوراق التي تحمل أسرار في خزانة ويقفل عليها بإحكام فإنه في المقابل لابد من تأمين النظام المعلوماتي للحفاظ على الأسرار الموجودة بداخله لأنه ليس من المعقول أن تخزن فيه أسرار من دون حماية فنية تحميها.

[1] – أيمن عبد الله فكري، جرائم نظم المعلومات دراسة مقارنة، دار الجامعية الجديدة للنشر، الإسكندرية، ب ط، 2007، ص 333، كذا أنظر رشيدة بوبكر، مرجع سابق، ص 168.

[2] – محمد خليفة، مرجع سابق، ص 137– 138.

المبحث الثالث: ماهية الجريمة المعلوماتية وأساليب ارتكابها وأطرافها

في إطار التصدي للسلوكات الإجرامية المستحدثة والمتمثلة في الجرائم المعلوماتية والتي تفطنت لها التشريعات العربية والغربية واستحدثت لها نصوصا، وحرص مجلس أوروبا على التصدي للاستخدام غير المشروع للحاسبات وشبكات المعلومات، وتجلى ذلك في اتفاقية بودابست الموقعة غفي 23 نوفمبر 2001 المتعلقة بالجرائم المعلوماتية، إيمان من الدول العميقة التي حدثت بسبب الرقمية والتقارب والعولمة المستمرة للشبكات المعلوماتية[1].

واستنادا إلى ما سبق، فإن المعلوماتية هي علم المعالجة الآلية للمعلومات أي المعلومات التي تمت معالجتها بوسائل آلية، فانطلاقا من العلاقة الموجودة بين المعلومات والتقنية المستحدثة في معالجتها للقول بأن المعلوماتية هي المعلومات المعالجة آليا باستخدام الحاسبات الآلية وأنظمتها.

تعتبر الحاسبات الآلية من المخترعات الحديثة التي تؤثر على الإنسان كيانا ونشاطا ولذلك فإنها تثير موضوع الحماية منها، أي حماية الإنسان وضمان حقوقه وحرياته الأساسية في مواجهة الغزو الذي تفرضه تلك الحاسبات على جوانب من النشاط

[1] – مدحت محمد عبد العزيز إبراهيم، الجرائم المعلوماتية الواقعة على النظام المعلوماتي، ط1، دار النهضة العربية، القاهرة، 2015، ص ص، 28، 29.

الإنساني، حيث كانت تلك الحقوق والحريات إلى وقت قريب من المحرمات التي لا يجوز الاطلاع أو الاعتداء عليها.

إذن شيئا فشيئا أصبحت تظهر مشكلة الحاسبات الآلية والتي تتمثل في تحقيق التوازن بين مصلحة المجتمع في الاستعانة بهذه التقنية الحديثة ومصلحة الإنسان في حماية حياته الخاصة والحفاظ على أسراره سواء هو أو أي شخص اعتباري، حيث أن هؤلاء فعلا تضرروا من جراء استخدام التقنية الحديثة بأشكال إجرامية مختلفة أدت بالعديد من الخسارة الاعتبارية إلى الخسارة المادية والمعنوية على حد السواء.

إذن إن الملاحظ وبشكل جدي أن الوسائل التقنية الحديثة خاصة الحاسب الآلي وشبكة الإنترنت والهاتف المحمول – خاصة المزود بتقنية البلوثوت– وكذلك الكاميرات المزودة بها تلعب دورا رئيسيا في ارتكاب هذه الجرائم وبالتالي فقد حدث تطور نوعي ملحوظ في وسيلة ارتكاب الجريمة سواء تعلقت بالأموال أو الأشخاص أو الحياة الخاصة أو المال العام كلها أنماط ونماذج من الجرائم ترتكب حاليا عن طريق وسائل التقنية الحديثة.

وبخصوص العلاقة التي ترتبط الحاسب الآلي والجريمة المعلوماتية ولمزيد من التوضيح بخصوص اختيارنا للحاسب الآلي وتركيزنا عليه باعتباره الوسيلة الإلكترونية الأهم في ارتكاب الجريمة المعلوماتية، وخاصة فيما يتعلق بالاعتداء على السرية

المعلوماتية والسلامة والإتاحة فيما يتعلق بالبيانات، فلا يخفى على أحد مدى العلاقة الوثيقة بين استخدامات الحاسب الآلي وارتكاب الجريمة المعلوماتية[1].

وفي إطار ماهية الجريمة المعلوماتية سيتم دراستها من خلال تحديد مفهومها ، والتعرف على أطرافها ودوافع الحياة فيها.

المطلب الأول:

لبيان مفهوم الجريمة المعلوماتية ولكي يتم رسم الصورة العامة لهذا البناء المعرفي يجب أن نتطرق لكل جزيئاتها فلابد من تعريفها ، والتعرف على خصائصها.

الفرع الأول: تعريف الجريمة المعلوماتية

استخدمت من أجلها عدة مصطلحات للدلالة عليها وتحديد مفهومها، فهناك من يطلق عليها جرائم الحاسب الآلي وإساءة استخدام الحاسب الآلي، وهناك من يطلق عليها مصطلح جرائم الكومبيوتر أو الجرائم الإلكترونية، وهناك من يطلق عليها جرائم الحاسب الآلي والإنترنت، وهناك من يسميها بالجرائم المعلوماتية، لهذا قال البعض أنها جريمة مستعصية على التعريف ويستدلون في ذلك بالمحاولات العديدة التي بدلت لتعريفها،[2] فلا يوجد تعريف موحد على الصعيد الدولي للجريمة المعلوماتية بسبب الخلاف حول

[1] – محمد خليفة، مرجع سابق، ص 137– 138.

[2] – فتوح الشادلي وعفيفي كامل عفيفي، جرائم الكومبيوتر، منشورات الحلبي الحقوقية، بيروت، لبنان، 2003، ص 31.

العناصر المكونة لها ما جعل اللجنة الأوروبية الناظرة بمشاكل الجريمة المعلوماتية في المجلس الأوروبي، تترك لكل دولة من الدول المعنية، الحرية في وضع تعريف للجريمة المعلوماتية مما يتوافق مع نظام كل منها وتقاليده.[1]

هذا الخلاف حول تعريف الجريمة المعلوماتية، جعل بعض الدول تفضل عدم وضع تعريف لجرائم المعلوماتية في تشريعاتها، تحسبا للتطور العلمي والتقني المستمر، ولعدم إمكان حصر قاعدة التجريم في نطاق أفعال معينة قد تتغير أو تتبدل في المستقبل، واكتفت في قوانين متعاقبة بتجريم أفعال الجريمة المعلوماتية بعد أن تصنفها تبعا لأهدافها، في حين هناك مشرعين في دول أخرى قد نحوا آخر وأتوا على تعريف صريح للجريمة المعلوماتية، وعل هذا الأساس سنتعرض للتعريف الفقهي والتشريعي للجريمة المعلوماتية على النحو التالي:

فباعتبار المعلوماتية كموضوع للجريمة عرفها البعض أنها "كل فصل أو امتناع عمدي ينسأ عند الاستخدام غير المشروع للتقنية المعلوماتية ويهدف إلى الاعتداء على الأموال المادية أو المعنوية.[2]

[1] – رامي متولي القاضي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية، دار النهضة العربية، القاهرة، ط1، 2011، ص 25.

[2] – فتوح الشادلي، مرجع سابق، ص 32.

ويعرفها البعض أيضا أنها "كل فعل إجرامي متعمدة أيا كانت صلته بالمعلوماتية ينشأ عنه خسارة وتلحق بالمجني عليه أو مكسب يحققه الفاعل".[1]

وعرفتها منظمة التعاون الاقتصادي والتنمية بأنها "كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية"، ويعرفها البعض الآخر بأنها "سلوك غير مشروع يتعلق بالمعلومات المعالجة ونقلها"[2]

وعرفت أنها "جريمة تقنية تنشأ في الخفاء يقترفها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية، وتوجه للنيل من الحق في المعلومات وتطال اعتداءاتها معطيات الحاسب المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات"، وتبنى البعض تعريفا للجريمة المعلوماتية اقتراحاته مجموعة من خبراء منظمة التعاون الاقتصادي والتنمية كأساس للنقاش في اجتماع عقد بباريس سنة 1983 لبحث الإجرام المرتبط بالمعلوماتية مقتضاه لأنها "كل سلوك غير شرعي أو غير أخلاقي أ غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها".[3]

[1] – محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، 1984، ص 6.

[2] – فتوح الشادلي، المرجع نفسه، ص 32.

[3] – سامي علي حامد عياد، المرجع السابق، ص 43.

وهناك جانب من الفقه الجنائي من ذهب إلى تعريف الجريمة المعلوماتية بالنظر إلى اعتبار الحاسب الآلي كوسيلة لارتكاب الجريمة، إذ عرفها أنها "أشكال السلوك غير المشروع الضار بالمجتمع الذي يرتكب باستخدام الحاسوب"، وقد عرفها مكتب تقييم التقنية في الولايات المتحدة الأمريكية "أنها الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا"[1]، ويعرفها البعض الآخر بأنها "نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود"[2]

ويقصد بالجريمة المعلوماتية أيضا كل فعل غير مشروع يرد على الكومبيوتر أو يتم استعماله، ويعرفها البعض أنها "كل نشاط إجرامي يؤدي في النظام دور لإتمامه أو يقع على النظام نفسه.[3]

وتعرف كذلك الجريمة المعلوماتية أنها ذلك النوع من الجرائم التي تتطلب إلمام خاص بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعليها، كما تعرف بأنها "الجريمة التي يتم ارتكابها إذا قام شخص ما باستخدام معرفته

[1] – مدحت محمد عبد العزيز إبراهيم، مرجع سابق، ص 23.

[2] – عبد الفتاح بيومي حجازي، مرجع سابق، ص 17.

[3] – شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2007، ص 12.

بالحاسب الآلي بعمل غير قانوني"، وهناك من يعرفها أنها "أي عمل غير قانوني يستخدم فيه الحاسب كأداة، أو موضوع للجريمة".[1]

وكتعريف شامل للجريمة المعلوماتية إلى جانب التعاريف السابقة هناك من وضع تعريفا شاملا للجريمة الإلكترونية، يتمثل في تعريفها بأنها تتضمن كافة أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب أو الجرائم التي تلعب فيها البيانات التكنولوجية والبرامج المعلوماتية دورا رئيسيا، أو هي "أي فعل إجرامي يستخدم الحاسب الآلي في ارتكابه كأداة رئيسية أو نشأ غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه، أو أية جريمة يكون متطلبا لاختراقها توافر لدى فاعلها معرفة تقنية للحاسب".[2]

وهناك جانب من الفقه يعرف الجريمة المعلوماتية، كما تعرف أيضا أنها "استخدام غير مشروع للحاسبات والتي تتخذ صورة فيروس يهدف إلى تدمير الثورة المعلوماتية".[3]

أو هي "كل فعل أو امتناع من شأنه الاعتداء على الأحوال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة تدخل التقنية المعلوماتية، أو سلوك غير

[1] – عمر وعيسى الفقي، الجرائم المعلوماتية، جرائم الحاسب الآلي والإنترنت في مصر والدول العربية، المكتب الجامعي الحديث، ص 232.
[2] – رامي متولي القاضي، مرجع سابق، ص 24.
[3] – عبد الفتاح بيوميحجازي، مرجع سابق، ص 18.

مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها"[1] وهو التعريف الشامل حقيقة لمعنى الجريمة المعلوماتية بخلاف التعاريف السابقة.

ثانيا: التعريف التشريعي للجريمة المعلوماتية

رغم خلو بعض التشريعات من تعريف الجريمة المعلوماتية 1 إلا أن هناك البعض من التشريعات من أشار إلى تعريفها كما هو الشأن بالنسبة للمشرع الجزائري من خلال المادة 1/2 من القانون رقم 04/09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال[2] على "أنها كل الجرائم سواء المتعلق بالمساس بالأنظمة أو غيرها من الجرائم الأخرى التي ترتكب أو يسهل ارتكابها باستعمال منظومة معلوماتية أو أي نوع آخر من نظم الاتصال الالكتروني."

ويمكن أن أشير في هذا المقام أن المشرع الجزائري بداية بموجب القانون 15/04 المعدل والمتمم لقانون العقوبات قد عبر عن الجريمة المعلوماتية بالجرائم ضد الأنظمة المعلوماتية على أساس أنه قد قدر بذلك أن جوهر المعلوماتية هو المعطيات التي تدخل إلى الحاسب الآلي، فتحول إلى معلومات بعد معالجتها وتخزينها، فقام بحماية هذه المعطيات من أوجه عدة .لذلك آثر المشرع الجزائري استخدامه لمصطلح المساس بنظم المعالجة الآلية للمعطيات، ثم في مرحلة لاحقة اختار المشرع الجزائري للتعبير عن

[1] – رامي متولي القاضي، مرجع نفسه، ص 24.

[2] – مدحت محمد عبد العزيز إبراهيم، مرجع سابق، ص 31.

الجريمة المعلوماتية مصطلح الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بموجب القانون رقم 04/09 المتضمن الوقاية من هذه الجرائم ومكافحتها.

وأما عن المقصود بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وهو التعبير الذي استخدمه المشرع الجزائري للتدليل على الجريمة المعلوماتية.[1] فإنه وقبل صدور القانون رقم 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها كانت الجريمة المعلوماتية في النظام العقابي الجزائري تقتصر فقط على تلك الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات وهي وفقا لدلالة الكلمة تنصرف إلى المعلومات والنظام الذي يحتوي عليها بما في ذلك شبكة المعلومات وهذه الأفعال في الحقيقة ما هي إلا جزء من الظاهرة الإجرامية.

لأجل هذا فقد تبنى المشرع الجزائري حديثا بموجب القانون 04/09 تعريفا موسعا للجرائم المعلوماتية واعتبر أنها تشمل بالإضافة إلى جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات من المادة 394 مكرر إلى المادة 394 مكرر 07 أي جريمة أخرى ترتكب أو يسهل ارتكابها بواسطة منظومة معلوماتية أو نظام للاتصالات الإلكترونية وبذلك لم يعد مفهوم الجريمة المعلوماتية في التشريع الجزائري يقتصر على الأفعال التي تكون فيها المنظومة المعلوماتية محلا للاعتداء بل توسع

[1] – سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير في العلوم الجنائية، جامعة الحاج لخضر، باتنة، السنة الجامعية 2012-2013، ص ص 46 ، 47.

نطاقها لتشمل إضافة إلى ذلك تلك الأفعال التي تكون المنظومة المعلوماتية وسيلة لارتكابها[1] .

من خلال ما سبق من تعريفات نستنتج أن الوسيلة الأكثر استخدما للجريمة المعلوماتية هي الحاسب الآلي وما يسهلها ويزيد من خطورتها هو ارتباطه بالإنترنت ومنه نخلص إلى تعريف خاص بنا وهي أن الجريمة المعلوماتية هي " :كل فعل غير مشروع وغير قانوني يتم باستعمال الحاسب الآلي أو أي وسيلة معالجة آلية للمعطيات قام به شخص ما مستخدما معرفته وقدراته بالحاسب الآلي أو وسيلة المعالجة الآلية للمعطيات، واستخدام فيها الجهاز كأداة أو موضوع للجريمة ، سواء كان الجهاز مربوط بشبكات الاتصال أم لا."

الفرع الثاني: خصائص الجريمة المعلوماتية

وكما سبقت الإشارة أنه صاحب ظهور الحاسب الآلي تحديات جديدة للقانون الجنائي فظهرت طائفة من الجرائم المستحدثة التي اتخذت من الثورة المعلوماتية والتكنولوجية التي جاء بها الحاسب الآلي بايجابياته إذ لا يمكننا أن ننكر هذه الأخيرة بيد أن هذا الجانب المضيء سرعان ما تناوشته الظلمة، وذلك باستخدامه استخداما غير مشروع.

[1] – مدحت محمد عبد العزيز إبراهيم، مرجع سابق، ص 31.

وشكل ذلك انقلابا ربما يعطي تفسيرا لما نراه اليوم من النمو المتزايد والمطرد للجرائم الإلكترونية أو المعلوماتية، والتي اختلفت وتميزت عن الجريمة التقليدية في عدة نقاط سيرد التفاصيل فيها أدناه ولكن قبل ذلك لابد من الإشارة إلى ما يلي:

1- أن الاعتداء على الكيانات المالية للحاسوب يخرج عن نطاق جرائم الحاسوب لأن هذه الكيانات المادية محل صالح لتطبيق نصوص التجريم التقليدية الناظمة للجرائم الواقعة على الأموال.[1]

2- أن محل جرائم الحاسوب هو دائما المعطيات إما بذاتها أو بما تمثله وقد تكون هذه المعطيات مخزنة داخل النظام أو على أحد وسائط التخزين أو تكون في طور النقل أو التبادل ضمن وسائل الاتصال المدمجة مع نظام الحوسبة.[2]

3- أن المصلحة محل الحماية في هذه الجرائم هي الحق في المعلومات ككيان معنوي ذو قيمة اقتصادية عالية،[3] إذن فمحل جريمة الكمبيوتر هو دائما معطيات الكمبيوتر بدلالتها الواسعة (بيانات مدخلة، بيانات ومعلومات معالجة ومخزنة، البرامج بأنواعها، المعلومات المستخرجة والمتبادلة بين النظم).

[1] – سهيل محمد العزام، الوجيز في الجرائم الإنترنت ، الطبعة الأولى، دائرة مكتبة الجامعة الأردنية، 2009 ، ص 79.

[2] – سهيل محمد العزام، المرجع نفسه، ص 79.

[3] – سهيل محمد العزام، المرجع سابق، ص 79.

فنظرا لوقوع الجريمة المعلوماتية في غالبية الأحيان في بيئة المعالجة الآلية للبيانات حيث تكون المعلومات محل الاعتداء، ووقوع هذه الجريمة في بيئة المعالجة الآلية للبيانات يستلزم التعامل مع بيانات مجمعة ومجهزة لدخول الحاسب بغرض معالجتها الكترونيا بما يمكن المستخدم من إمكانية كتابتها في الحاسب الذي يتوفر فيه إمكانيات لتصحيحها وتعديلها ومحوها وتخزينها واسترجاعها وطباعتها وهذه العمليات وثيقة الصلة بارتكاب الجرائم ولابد من فهم الجاني لها كما تكون أيضا البرامج والبيانات محلا للاعتداء أو تستخدم وسيلة للاعتداء،[1] ومن هذا المنطلق تتميز الجرائم المعلوماتية عن نظيرتها التقليدية بالخصائص التالية:

أولا: أنها ترتكب من مجرم غير تقليدي وهي جرائم ناعمة:

يختلف المجرم مرتكب الجريمة المعلوماتية عن المجرم في الجرائم التقليدية ذلك لأن له سمات مختلفة عن غيره كما أن له طوائف وأنماط خاصة به، كما أن العوامل التي تدفعه لارتكاب الجريمة مختلفة عنه أيضا، فسمات هذا المجرم عموما هو أنه إنسان اجتماعي، أي أنه متوافق مع مجتمعه وغالبا ما تكون له مكانة معتبرة فيه ويحظى بالاحترام منه، كما أن هذا المجرم يمتلك المعرفة والمهارة والوسيلة الخاصة في هذا

[1] – فتوح الشادلي، مرجع سابق، ص 34.

المجال، أو عن طريق الخبرة والاحتكاك بالآخرين، كما أن هذا المجرم إنسان ذكي ويستغل ذكائه في تنفيذ جريمته ولا يستعين بالقوة الجسدية في ذلك إلا بالقدر اليسير جدا.

كما تعتبر الجريمة المعلوماتية جرائم ناعمة لا عنف فيها ولا وجود لجثث قتلى وآثار لدماء أو اقتحام من أي نوع، فإذا كانت الجرائم التقليدية تحتاج من مرتكبيها إلى قوة عضلية لتنفيذها فإن هذه الجرائم لا تحتاج إلى مثل تلك القوة العضلية وإنما تحتاج إلى قوة علمية وقدر من الذكاء ومهارة في توظيف ذلك، والجاني في سبيل ذلك لا يحتاج من الوقت إلا ثواني أو دقائق معدودات، ولا يحتاج من القوة العضلية غير تحريك الأنامل من على وسائل الإدخال وقد يتسبب بذلك في حصول خسائر فادحة رغم أن جريمته لا ترى بالعين فنعومة هذه الجريمة وما تدره من أرباح ومن إشباع الفضول عند البعض، جعلها من الجرائم المغرية للمجرمين[1].

ثانيا: جرائم خفية وعابرة للحدود وصعبة الاكتشاف والإثبات:

أ- **خفاء الجريمة:** تتسم الجريمة المعلوماتية بأنها مستترة خفية في أغلبها حيث أن المجني عليه لا يلحظها غالبا مع أنها قد تقع أثناء وجوده على شبكة الإنترنت ولكن لا يكون عالما بها ولا ينتبه إليها إلا بعد فترة من وقوعها وفي بعض الأحيان لا يكتشف

[1] – فتوح الشادلي، مرجع سابق، ص 35.

أمرها،[1] وقد يتم اكتشافها بالصدفة البحتة، إضافة إلى أنها ترتكب في الخفاء ولا يوجد لها أثر كتابي في أغلب الأحيان، مع العلم أن للجاني فيها قدرة عالية على تدمير ما قد يعتبر دليلا يمكن أن يستخدم لإدانته وذلك في أقل من ثانية واحدة، [2]وهذا ما جعل نسبة الجرائم المعلوماتية المكتشفة ضئيلة.

وتعتبر خفية أيضا لأن الجاني يتعامل مع نبضات إلكترونية غير مرئية لا يمكن قرائتها إلا بواسطة الحاسب كما أن توافر المعرفة الفنية لدى الجاني في مجال المعلوماتية يؤدي إلى صعوبة اكتشاف جريمته، وذلك بإتباعه لطرق وأساليب لا يفطن إليها المستخدم العادي للشبكة، ومن أمثلتها إرسال الفيروسات، سرقة البيانات الخاصة، التجسس وغيرها كما قد يدس بعض البرامج الخاصة وتغذيتها ببعض البيانات التي تؤدي إلى عدم شعور المجني عليه بوقوع هذه الجرائم.[3]

ب – جرائم عابرة للحدود :حيث أن الإنترنت وكما يشاهد الجميع ربطت العالم بشبكة الاتصال المتميزة والفعالة، قربت شعوب العالم بأجناسهم وثقافاتهم المختلفة من بعضهم بصورة لم تكن متاحة من قبل بأي وسيلة من وسائل الاتصال حتى كادت أن تلغي الحدود القائمة بين الدول بأن جعلت العالم قرية صغيرة.

[1] – محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت دراسة مقارنة، ط2، دار النهضة العربية، القاهرة، 2009، ص 38.

[2] – فتوح الشادلي، مرجع سابق، ص 35.

[3] – محمد عبيد الكعبي، مرجع سابق، ص 38.

واستخدام هده الشبكة الحديثة أدى إلى سلبيات تمثلت في انتشار الجريمة، وأصبحت الجرائم المستحدثة منتشرة بواسطة الإنترنت والمشكلات المصاحبة لها، مشكلة عالمية لا تعترف بالحدود الإقليمية للدول ولا بالزمان، ولا بالمكان، وأصبح العالم بأجمعه ساحة لتلك الجرائم.

وفي مجتمع الإنترنت تذوب الحدود الجغرافية بين الدول لارتباط العالم بالشبكة الواحدة، ومن الملاحظ أن أغلب الجرائم المرتكبة عبر شبكة الإنترنت يكون الجاني في دولة والمجني عليه في دولة أخرى، ومن ذلك على سبيل المثال اختراق أنظمة الحواسيب الآلية من خارج إقليم دولة المجني عليه.

معناه أنه يمكن أن تقع الجريمة من جان في دولة معينة على مجني عليه في دولة أخرى في وقت يسير جدا مكبدة أفدح الخسائر، لاسيما مع تعاظم الدور الذي تقدمه شبكة الإنترنت فإمكانية ارتكاب هذا النوع من الجرائم من خلال مسافات بعيدة قد تصل إلى دول وحتى قارات.

ج- صعوبة اكتشاف واثبات هذه الجرائم:

تقع هذه الجريمة على الكمبيوتر وشبكة الإنترنت ونظمها،[1] وهي جريمة ناعمة ترتكب دون عنف وفي الخفاء ولا أثر خارجي لها وممكن تدمير أي دليل عليها في ثانية واحدة أو عدة ثوان.

وذلك أيضا لإحجام المجني عليهم عن الإبلاغ عن هذه الجرائم في حال اكتشافها لما يؤدي إليه هذا الإبلاغ من عواقب وخيمة في مجتمع الأعمال الذي ينتمون إليه وحتى لا تهتز ثقة جمهور المتعاملين معهم .وقد يحاول الضحية حتى تضليل المحققين حتى لا يكتشفوا هذه الجرائم، إضافة إلى أنه يجب أن يكون لهؤلاء المحققين إحاطة واسعة بالتكنولوجيا الحديثة حتى يتمكنون من اكتشاف وإثبات هذه الجرائم.

فتتميز الجرائم المعلوماتية أيضا عن سائر الجرائم التقليدية بصعوبة إثباتها، ويرجع ذلك إلى عدة أسباب، من أهمها:[2]

[1] – فريد منعم جبور، حماية المستهلك عبر الإنترنت ومكافحة الجرائم المعلوماتية (دراسة مقارنة)، ط1، منشورات الحلبي الحقوقية، بيروت، لبنان، 2010 ،

[2] – محمد عبد الرحيم سلطان العلماء، جرائم الإنترنت والاحتساب عليها، بحوث مؤتمر القانون والكومبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، المجلد الثالث، ط3، 2004، ص 877.

1- انعدام الآثار التقليدية للجريمة

أغلب المجرمين يتركون أثرا يؤدي إلى اكتشافهم والعثور عليهم ولو بعد حين من الزمن أما الجرائم المرتكبة بواسطة الإنترنت فلا تترك في الأغلب آثارا خارجية أو مادية تدل على الجريمة أو مرتكبها، فلا يوجد جثث لقتلى أو آثار لدماء.

2- عدم ترك هذه الجرائم لأي أثر خارجي بصورة مرئية والذي يمكن فهمه بالقراءة

أغلب البيانات والمعلومات التي يتم تداولها من حاسب آلي إلى آخر عبر الشبكة الإنترنت تكون في هيئة رموز مخزنة على وسائط تخزين ممغنطة بحيث لا يمكن للإنسان قراءتها أو إدراكها إلا بواسطة الحاسب الآلي ولا زالت الأجهزة المعنية في سبيل الجمع أو الكشف عن أدلة من هدا النوع لإثبات وقوع الجريمة والتعرف على مرتكبها تعاني الكثير[1].

3- إعاقة الوصول إلى الدليل بوسائل الحماية الفنية

الذين يرتكبون الجرائم الالكترونية أنفسهم بتدابير أمنية واقية تزيد صعوبة من صعوبة التفتيش عن الأدلة التي تؤدي إلى الإدانة ودلك باستخدام كلمات السر، أو دس

[1] – محمد عبد الرحيم، مرجع سابق، ص 875.

تعليمات خفية لتصبح بينها كالرمز أو تشفير التعليمات باستخدام طرق وبرامج تشفير البيانات المتطورة مما يجعل الوصول إليها غاية في الصعوبة.

4- سهولة إتلاف الدليل المادي وتدميره في زمن قياسي

يسهل غالبا على الجاني في ارتكاب الجرائم الالكترونية محو أدلة الإدانة في زمن قياسي بحيث لا تستغرق أكثر من ثوان معدودة، وذلك بتعريض البيانات المخزنة لديه على وسائط ممغنطة إلى مجال مغناطيسي قوي قادر على محوها في طرفة عين، أو تزويد الحاسب ببرامج من شأنها تدمير وتخريب البيانات في حال استخدامه من قبل شخص غير مرخص له.

ثالثا: هي جرائم فادحة الأضرار وذات أساليب سريعة التطور:

إن الاعتماد على الحاسب الآلي في إدارة مختلفة الأعمال في شتى المجالات ضاعف من الأضرار والخسائر التي تخلفها الجريمة المعلوماتية (الاعتداء على معطيات الحاسب الآلي).[1]

وتتميز الجرائم المعلوماتية خاصة جرائم الإنترنت بارتباطها بالتطور السريع الذي تشهده اليوم تكنولوجيا الاتصالات، مما يؤثر بدوره على مرتكب الجريمة وأسلوب ارتكابه

[1] – محمد خليفة، مرجع سابق، ص 38.

لها من خلال تبادل الأفكار والخبرات الهدامة مع العديد من المجرمين حول العالم عبر الشبكة الالكترونية وتطور التقنيات المستخدمة.[1]

كما تبرز ذاتية الجرائم المعلوماتية بصورة أكثر وضوحا في أسلوب ارتكابها وطريقتها، فإذا كانت الجرائم التقليدية تتطلب نوعاً من المجهود العضلي الذي قد يكون في صورة ممارسة العنف والإيذاء كما هوا لحال في جريمة القتل أو الاختطاف، أو في صورة الخلع أو الكسر وتقليد المفاتيح كما هو الحال في جريمة السرقة، فإن الجرائم المعلوماتية هي جرائم هادئة بطبيعتها لا تحتاج إلى العنف بل كل ما تحتاج إليه هو القدرة على التعامل مع جهاز الحاسوب بمستوى تقني يوظف في ارتكاب الأفعال غير المشروعة.

وتحتاج كذلك إلى وجود شبكة المعلومات الدولية(الإنترنت) مع وجود مجرم يوظف خبرته أو قدرته على التعامل مع الشبكة للقيام بجرائم مختلفة كالتجسس أو اختراق خصوصيات الغير كل ذلك دون حاجة لسفك الدماء.

الفرع الثالث: محل الجرائم المعلوماتية (موضوعها)

كان الحاسب الآلي آلة هامة في حياة الإنسان وله كل القدر من الأهمية والفائدة التي سبق ذكرها، فإن هذا الأخير عبارة عن جهاز ضعيف أمام الإنسان لأنه –أي

[1] – محمد عبد الرحيم، مرجع سابق، ص 875.

الحاسب الآلي– مصمم لتلقي الأوامر ولا يمكنه التمييز بين أمر وآخر، ولا يمكنه إدراك الغايات التي يصبو إلى تحقيقها الإنسان من خلال استعماله لهذا الحاسب، خاصة إذا كان مربوطا بشبكة الإنترنت التي ساهمت بشكل كبير في تسهيل ارتكاب الجريمة بواسطة هذا الجهاز الذي أسهم بايجابياته العجيبة في حياة الإنسان وسلبياته الخطيرة في هدمها.

فالإنسان هو الذي صنع الحاسب الذي قد يستعمله في أغراض مشروعة ومفيدة كما قد يستعمله في أغراض غير مشروعة وخطيرة، ولا يمكن للحاسب أن يميز بين هذا وذاك، وإنما يقوم بالوظيفة التي صنع من أجلها فهو بمكوناته المادية وغير المادية تحت سلطة الأوامر، من يجلس أمامه ويقوم باستخدامه حتى وإن كان مجرما وتسمى الجريمة المرتكبة في هذه الحالة جريمة كمبيوتر (جريمة معلوماتية)، وهي نوع جديد من السلوكيات المنحرفة التي يتعرض لها كل من الحاسوب ومكوناته من خلال أشخاص مؤهلين وذوي خبرة علمية وعملية في كيفية التعامل معه، أو مع تلك المعطيات أو البيانات أو المستخرجات، ومن هذا التعريف نتصور أنه قد تكون المكونات المادية أو المعنوية محل تلك الجريمة المعلوماتية، كما قد يتصور وقوع هذه الجريمة من خلال الاستخدام غير المشروع للحاسوب[1].

[1] – محمد عبيد الكعبي، مرجع سابق، ص 38.

والجدير بالذكر هنا أن العديد من الدارسين أكدوا أن الجرائم الواقعة على المكونات المادية للكمبيوتر تعتبر من قبيل الجرائم التقليدية وهو الموقف الغالب إذ أن الجديد في القانون الجنائي وفيما أثير من مشكلات حول المسؤولية الجنائية عن جرائم الكمبيوتر، إنما يتصل بالاعتداءات الموجهة إلى الكيانات غير المادية لنظام الكمبيوتر والتي عبر عنها بمعطيات الكمبيوتر (المعلومات)، إذا فإن وقوع الجريمة على المكونات المادية لا تثير مشكلة على أساس أنها تتمتع بالحماية الجزائية وفقا للقواعد العامة (قانون العقوبات) بخلاف المكونات المعنوية، رغم أن البعض يعتبرها ضمن جرائم الكمبيوتر ولكنه رأي غير متفق عليه والغالب هي جرائم تقليدية كما سبقت الإشارة.

إذن فموضوع الجريمة المعلوماتية أي محلها، يتمثل في المعطيات و المصلحة التي تهدرها والحق الذي تعتدي عليه هو الحق في المعلومات بذاتها، وبما تمثله من أموال أو أصول أو أسرار أو بيانات شخصية أولها قيمة بذاتها كالبرامج[1] .

فالمعلومات الالكترونية جديرة بالحماية حتى عن المعلومات الورقية، فتظهر جدارة المعلومات المبرمجة آليا بالحماية الجنائية عن المعلومات التي تحتويها الملفات الورقية من ضعف النوع الأول من المعلومات ومن أهميته في آن واحد، فالمعلومات المعالجة آليا ضعيفة داخل النظام عنها داخل الملفات الورقية .هذه الأخيرة يمكن إخفاؤها بسهولة

[1] – محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية. بدون طبعة، 2004، ص 65.

عن المعلومات داخل النظام .كما أن المعلومات المعالجة آليا تتميز بالضخامة والتنوع، ومنها ما يتعلق بالحياة الخاصة للأفراد .كل هذه العبارات دعت مشرعي كثير من البلاد إلى استحداث صور من التجريم لحماية المعلومات داخل الكمبيوتر من الاطلاع عليها، بينما لا يوجد مثيل لتلك النصوص بالنسبة للمعلومات المسجلة داخل الملفات الورقية.[1]

;رغم أن الدخول إلى النظام يعتبر أمرا بسيطا إلا أن الأضرار الناتجة عنه تعتبرا أمرا خطيرا، وتختلف طبعا الدوافع في ارتكاب هذا النوع من الإجرام تتباين بين المدادية والتنافسية وغيرها.

المطلب الثاني: دوافع مرتكبي الجريمة المعلوماتية وأطرافها

حيث أن الجريمة المعلوماتية أضافت شكلا جديدا من المجرمين و الضحايا، وحيث اصطلح على تسمية المجرم فيها بالمجرم المعلوماتي كما توسعت دائرة المتضررين من هؤلاء الجناة، و من خلال هذا المطلب نحاول التفصيل في كل من دوافع مجرمي المعلوماتية (فرع أول) و أطرافها (فرع ثان).

[1] – Marise CREMONA JONATHAN HERRING, criminal law, ibid,p234.

الفرع الأول: دوافع مرتكبي الجريمة المعلوماتية

إذن الدافع يشكل أحد الركائز في جميع الجرائم وبالنسبة للجرائم المعلوماتية فهي لا تختلف في وضعها العام عن التقليدية فثمة دوافع عديدة لمرتكبي جريمة المعلوماتية تحركهم لارتكاب أفعال الاعتداء المختلفة المشكلة لما يسمى بالجريمة المعلوماتية وتختلف هذه الدوافع من إنسان لأخر وتتمثل هذه الدوافع أساسا فيما يلي:

أولا: السعي إلى تحقيق الكسب المالي

يعتبر هذا الدافع أكثر الدوافع التي تؤدي إلى تحريك بالجناة إلى ارتكاب هذا النوع من الجرائم على وجه الخصوص وغيرها ذلك لأن حجم الربح الكبير الممكن تحقيقه من بعضها يتيح تعزيز هذا الدافع.

فقد تدفع الحاجة البعض إلى تحقيق الثراء السريع عن طريق إتاحة الاطلاع على معلومات معينة أساسية وذات أهمية خاصة لمن يطلبها، ولذلك تتعدد الأساليب اللازمة للوصول إلى هذا الهدف المنشود2 ، حيث أنه قد تطلب بشأن تلك المعلومات مبالغ طائلة ولكن لا تعتبر كذلك بالنظر إلى الخسائر التي ستلحق أصحابها لوتم إفشاؤها[1].

[1] – محمد عبيد الكعبي، مرجع سابق، ص 38.

ثانيا: الانتقام من رب العمل وإلحاق الضرر به

هناك أثار سلبية في سوق العمل من جهة وفي البناء الوظيفي من جهة أخرى، وقد لوحظ أن العاملين في قطاع التقنية أو المستخدمين لها في نطاق قطاعات العمل الأخرى ويتعرضون على نحو كبير لضغوطات نفسية ناجمة عن ضغط العمل والمشكلات المالية، ومن طبيعة العلاقات العمل المنفرة في حالات معينة، هذه الأمور قد تدفع إلى النزعة نحو تحقيق الربح لكنها في حالات كثيرة مثلث قوة محركة لبعض العاملين لارتكاب جرائم الكمبيوتر باعثها الانتقام من النشأة أورب العمل،[1] أي أن الحقد على رب العمل الدافع المحرك لارتكاب الجريمة.

ثالثا :الرغبة في قهر النظام والتفوق على تعقيد وسائل التقنية

وهناك دافع أقوى من شهوة الحصول على الربح وهو الرغبة في قهر النظام رغم أن السعي إلى تحقيق الربح يظهر دافعا أكثر تحريكا للمجرمين الكمبيوتر إلا أن الدافع إلى قهر النظام أيضا تجسدت لدينا نسبة معتبرة من تلك الجرائم الالكترونية خاصة ما يعرف بأنشطة المتطفلين، وهؤلاء ليسوا على جانب كبير من الخطورة الإجرامية وإنما هم غالبا يفضلون تحقيق انتصارات تقنية ودون أن يتوافر لديهم أية نوايا سيئة.[2]

[1] – محمد محمود المكاوي، الجوانب الأخلاقية والاجتماعية والمهنية للحماية من الجرائم المعلوماتية (جرائم الكمبيوتر والإنترنت)، الطبعة الأولى، المكتبة العصرية للنشر والتوزيع ، مصر، 2010 ، ص51

[2] – محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية. بدون طبعة، 2004، ص 65.

رابعا: دوافع سياسية وتجارية

وهي عموما محرك أنشطة الإرهاب الإلكتروني فكثيرة هي المنظمات في عصرنا الحالي والتي تتبنى بعض الآراء والأفكار السياسية أو الدينية أو الإيديولوجية، ومن أجل الدفاع عن هذه الآراء تقوم بأفعال إجرامية ضد معارضيها.[1]

فمثلا هناك العديد من عمليات الاختراق تعود لأسباب عقائدية، حيث يقوم بعض المجموعات التي تتبنَّى فكرة الإصلاح، بعملية رقابة أخلاقية أو اجتماعية أو دينية، فتتجسّس على المواقع التي تقدِّم خدمات أو معلومات تتعارض مع قناعاتها، وتعمل على كشف أسرارها أو حتى تدميرها، فهناك بعض المواقع أخذ على عاتقه مهمة التجسّس على مواقع حكومية وكشف الأسرار الدبلوماسية والعسكرية.

أما عن دوافع الحصول على المعلومات التجارية بمختلف الأشكال فهي عموما دوافعها المنافسة.[2]

الفرع الثاني: أطراف الجريمة المعلوماتية

من خلال ما سبق فإن الجريمة المعلوماتية هي جرائم نتجت عن التزاوج بين انفجار المعلومات وتطور وسائل الاتصال، فهي نوع جديد من السلوكيات المنحرفة التي

[1] – نسرين عبد الحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف الإسكندرية، 2008، ص 45.

[2] – http://www.lebarmy.gov.lb/article.asp?ln=ar&id=27286 يوم الاطلاع على الموقع: 2020/08/15

يتعرض لها كل من النظام المعلوماتي ومكوناته من البيانات أو معطيات من خلال أشخاص مؤهلين وذوي خبرة علمية أو عملية في كيفية التعامل معه أو مع تلك المعطيات أو البيانات أو المستخرجات، فهي كأي جريمة لابد لها من فاعل (جان) وواقع عليه الفعل (مجني عليه) وسيتم التفصيل فيهما كالتالي:

أولا: الجاني في الجريمة المعلوماتية

بالإضافة إلى الشروط العامة الواجب توفرها في مرتكب الجريمة المعلوماتية من سلوك منحرف (فعل) وعلم وإرادة في نتائج هذا السلوك، ينبغي أن يكون هذا الشخص على درجة معينة من العلم والخبرة في شؤون عالم الحاسوب وتقنية المعلوماتية،[1] وهذا يعني أنه لا يتصور أن يكون الجاني في الجريمة المعلوماتية إلا شخصا طبيعيا ذا أهلية وقدرة على أن يكون محلا لتوقيع العقوبة وهو الأمر الذي لا يتصور حدوثه إلا بالنسبة للشخص الطبيعي دون الشخص المعنوي، كما لا يتصور أن يكون الجاني هنا إلا شخصا ذا خبرة ودراية في علم الحاسوب سواء أكان مستخدما أو مبرمجا أو مجرد هاو أو محترف لجرائم الحاسوب وتقنية المعلومات، حيث تتوفر لدى الجناة مرتكبي جرائم المعلوماتية أو معظمهم مجموعة من السمات أو الخصائص، التي تميزهم عن غيرهم من

[1] – عامر محمود الكسواني، التجارة عبر الحاسوب، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2008 ، ص 180-181.

الجناة أ المتورطين في أشكال الانحراف والإجرام الأخرى وعلى هذا الأساس يمكن أن نلخص السمات التي يختص بها الجناة في الجريمة المعلوماتية وبإيجاز كالتالي:[1]

1- المهارة اللازمة عن طريق الدراسة، والخبرة المكتسبة في تكنولوجيا المعلومات والمعرفة الكاملة بمحيط الجريمة وظروفها والوسيلة التي يتزودون بها والقدرة على ابتكار الأساليب اللازمة والسلطة المباشرة أو غير المباشرة في الوصول إلى المعلومات والحصول على الشيفرة.[2]

2- ارتفاع مستوى الذكاء، حيث يعتبر الذكاء من أهم صفات مرتكب الجرائم المعلوماتية لأن ذلك ينتج منه المعرفة التقنية لكيفية الدخول إلى أنظمة الحاسب الآلي وارتكاب مختلف أشكال الجرائم.

3- خشية الضبط وافتضاح الأمر، لما يترتب على ذلك من ارتباك مالي وفقد للمركز والمكانة.[3]

[1] – أيمن عبد الحفيظ، إستراتيجية مكافحة جرائم استخدام الحاسب الآلي، الناشر المؤلف، 2003 ، ص 24.

[2] – فريد منعم جبور، مرجع سابق، ص 189.

[3] – محمد عبد الله أبوبكر سلامه، مرجع السابق، ص 98.

4- يفرق معظم مرتكبي جرائم المعلوماتية لاسيما الهواة منهم تفرقة واضحة بين الإضرار بالأشخاص العاديين الذي يعتبرونه غاية في اللاأخلاقية والإضرار بمؤسسة أوجهة في استطاعتها اقتصاديا تحمل نتائج تلاعبهم وهو ما لا يجدون غضاضة في تقلبه.[1]

ثانيا :المجني عليه في الجرائم المعلوماتية

إذا كان الغالب الأعم بأن مرتكب الجريمة المعلوماتية لا يتصور أن يكون إلا شخصا طبيعيا، فإن المجني عليه هنا هو بالغالب الأعم شخص معنوي كالبنوك والشركات الكبرى والمؤسسات الحكومية والوزارات والمنظمات والهيئات المالية الضخمة، وغيرها من الأشخاص الاعتبارية التي تعتمد في انجاز أعمالها على الحواسيب.[2]

وبالنسبة للأشخاص العاديين، فمن غير المستبعد أن يكونوا هم أيضا ضحية الجرائم المعلوماتية خاصة الذين يحفظون أسرارهم وأعمالهم وشؤونهم داخل الحاسوب خاصة الأشخاص الذين يكون لهم منصب سياسي رفيع أو رجل أعمال مرموق أو صاحب شهرة عالمية في قطاع من القطاعات الاقتصادية أو الاجتماعية أو العسكرية.

وعلى الرغم من إمكانية تعرض الجميع للجريمة المعلوماتية سواء أكانوا أشخاصا معنوية أو طبيعية إلا أننا يمكننا الجزم بأن معظم الجرائم المعلوماتية ترتكب من أجل

[1] – محمد عبد الله أبوبكر سلامه، مرجع السابق، ص 98.

[2] – عامر محمود الكسواني، مرجع سابق، ص 98.

أمرين لا ثالث لهما وهما :المال والمعلومات، وبالتالي يمكننا الجزم أيضا بأن الغالبية العظمى من المجني عليهم في الجرائم المعلوماتية هم إما مؤسسات مالية كالبنوك والمصارف وشركات الصرافة وإما شركات المعلومات يصرف النظر عن نوع هذه المعلومات وقيمتها إذ قد تكون بالغة الأهمية كالمعلومات العسكرية والمخابراتية وقد تكون معلومات رياضية أو اجتماعية بسيطة .

المطلب الثالث: تصنيف جناة الجريمة المعلوماتية

اتفق الباحثون على أن أفضل تصنيف لمجرمي التقنية هو التصنيف القائم على أساس أغراض الاعتداء، ومن بين هذه التصنيفات لمجرمي التقنية هو تصنيفهم إلى ثلاثة طوائف وهي المخترقون، المحترفون والحاقدون[1].

الفرع الأول: المخترقون

كانت حقبة الستينات هي البداية في تاريخ ما يطلق عليهم المخترقون وقد تم تصميم برنامج UNIX الذي كان يعد أسرع البرامج في تلك الحقبة من الزمن، وكان من أشهر هؤلاء المخترقون (دينيس) و(ريتشي) و(كين تومسون) وبعد أن تم بنجاح إنتاج الكمبيوتر الشخصي بدأ عمل هؤلاء المخترقون في اكتشاف كيفيات عمل هذا الجهاز، وماهية البرامج التي ثبت عليه وكيفية اختراقه وتعتبر الفترة الزمنية من عام 1979 وعام

[1] – محمد منير الجنيهي، ممدوح محمد الجنيهي، امن المعلومات الالكترونية ، دار الفكر الجامعي الاسكندرية، 2005 ، ص 29.

1989 هي العصر الذهبي لهؤلاء المخترقون. أما عام 1983 فشهد القبض على أول عصابة من نوعها تتهم باختراق. أجهزة الحاسب الآلي والمفاجأة أن أعضاء العصابة كانوا من المراهقين والتي أطلق عليها فيما بعد عصابة "414" ووجه إليها اتهامات باختراق 60 جهاز كمبيوتر من بينها معمل يقوم بتطوير الأسلحة النووية الأمريكية،[1] وانتهت تلك المجموعات إلى مجموعتين فقط هم : مجموعة "LOD" ومجموعة "MOD" وسيتم التفصيل في هاتين المجموعتين في الفرع الخاص بالهاكرز، فالمخترقون هم أشخاص لهم القدرة على التعامل مع أنظمة الحاسب الآلي والشبكات بحيث تكون لهم القدرة على تخطي أي إجراءات أو أنظمة حماية اتخذت لحماية تلك الحسابات أو الشبكات فتشمل هذه الفئة نوعين من المخترقين أو ما يسمون بالمتطفلين إذ تم تصنيفها إلى نوعين الهاكرز، والكراكرز.

أولا: الهاكرز

الهاكر هو اللفظ العربي للكلمة الانجليزية (hacker) وهي تحمل عدة معان، إلا أننا في هذه الدراسة نحن معنيون بمعنى واحد وهو المخترق أو الهاتك.

فالهاكر هو شخص بارع في استخدام الحاسب الآلي وبرمجته، ولديه فضول في استكشاف حاسبات الآخرين وبطرق غير مشروعة، فالهاكرز وكما يدل اسمهم هم

[1] – محمد منير الجنيهي، مرجع نفسه، ص 29.

متطفلون يتحدون إجراءات أمن نظم الشبكات، لكن لا تتوفر لديهم في الغالب دوافع حادة أو تخريبية وإنما يطلقون من دوافع التحدي وإثبات الذات، وتتألف هذه الطائفة أساسا من المراهقين وشباب (طلبة وتلاميذ ثانويات) وشباب عاطل عن العمل، وهو شخص يتمتع بتعليم لغة البرمجة وأنظمة التشفير الجديدة، ويستمتع أيضا بعمل البرامج أكثر من التشغيل وهو شخص يؤمن بوجود أشخاص آخرين يستطيعون القرصنة ويستطيع أن يصمم ويحلل البرامج أو أنظمة التشغيل.[1]

إذن هم أشخاص لهم قدرة فائقة على اختراق الأجهزة والشبكات أيا كانت إجراءات وبرامج وتدابير الحماية التي تم اتخاذها إلا أنهم لا يقومون بأي من الإجراءات التي تؤدي من تم اختراق جهازه أو شبكته،[2] وقدرتهم على اختراق كافة الشبكات تمكنهم من الإبحار في عالم البيانات دون أهمية لحواجز كلمات المرور أو الشفرات.[3]

وقد صنفت إحدى أهم شركات حفظ أمن المعلومات في أمريكا الهاكرز بأنهم ثلاث نماذج:

1- المتشردون وهم عادة ما يكونون كالأطفال في أعمالهم.

[1] – عبد الصبور عبد القوي على مصدي، الجريمة الالكترونية، دار العلوم للنشر والتوزيع، ص 55 ، الطبعة الأولى، 2008، ص ص، 40،41.

[2] – منير محمد الجنيهي، مرجع سابق، ص 28.

[3] – رشدي محمد علي محمد عيد، مرجع سابق، ص 74.

2- المستغلون أو ذو القبعة السوداء وهم الذين يعملون من أجل الربح الشخصي أومن أجل الثأر وتأكيد مواقف سياسية.

3- ذو القبعات البيضاء وهم الذين يعملون من أجل أغراض البحث.

وقد ضايق الهاكرز الجيش الأمريكي عندما تصاعدت الأزمة في الخليج، لقد قال وزير الدفاع الأمريكي بأن الهاكرز استطاعوا الدخول إلى مناطق محظورة واستطاعوا تثبيت مفاتيح كي تمكنهم من الوصول للمعلومات في وقت لاحق. وقد أعلن مكتب التحقيقات الفيدرالي بأن مخترقي أنظمة الكمبيوتر هم الأكثر خطورة على الولايات المتحدة وأن أمريكا تواجه تهديدات كبيرة بسبب الهجوم على بنيتها الإلكترونية مما يسبب خطر أكبر حتى من أي مواجهة محتملة.

فقال رئيس المركز الوطني لحماية البنية التحتية في أمريكا وهو المخول إليه الحماية من التجسس الالكتروني بأن خارقي أنظمة الكمبيوتر يرون في نظام دفاع حكومة الولايات المتحدة هو الامتحان الأخير لهم وأقصى تحدي لاختبار مهاراتهم. وأضاف بأن كثير من الحوادث كان السبب فيها هم الشباب الصغار وهؤلاء كان أثر اختراقهم تافه ولكن حذّر من الأعداء ذو المهارات العالية لأن عملهم خطير.[1]

[1] – منير محمد الجنيهي، ممدوح محمد الجنيهي، مرجع سابق، ص 32.

ثانيا :الكراكرز

الكراكرز أو المقتحم هو شخص يقوم بالتسلل إلى نظم الحاسوب للاطلاع على المعلومات المخزنة فيها أو لإلحاق الضرر أو العبث بها أو سرقتها، ولقد تم استعمال هذا المفهوم الجديد سنة 1985 من طرف الطائفة الأولى طائفة الهاكرز للرد على الاستعمال السيئ للصحفيين لمصطلح الهاكرز .ولقد استفادة هذه الطائفة كثيرا من التقنيات التي طورتها فئة الهاكرز وبدؤوا يستخدمونها استخداما سيئا في اعتداءات تتم على ميولات إجرامية، فالمقتحمين يتميزون بصفة وهي تبادلهم للمعلومات فيما بينهم.[1]

ويطلق على هذه الفئة أيضا اسم القراصنة المخادعين وهؤلاء يحدثون أضرارا كبيرة على الصناعات وعلى أنظمة المعلومات لأنهم يؤلفون نوادي لتبادل المعلومات فيما بينهم وهي الميزة التي سبق وأشرنا إليها وهم يقسمون أيضا على أساس جرائمهم إلى:

1- المخادعون:

وهم أشخاص يتمتعون بقدرات عالية باعتبارهم من المتخصصين في المعلوماتية، ومن أصحاب الكفاءات وتنص جرائمهم في أغلبها على الأموال، والتلاعب في حسابات

[1] – نسرين عبد الحميد نبيه، مرجع سابق، ص 41.

المصارف والمؤسسات المالية والاقتصادية ولديهم القدرة الفائقة على إخفاء الأدلة التي من الممكن أن تختلف عن جرائمهم.[1]

2- الجواسيس:

وهؤلاء مهمتهم خلاف مهمة الفئة السابقة، إذ أن مهمتهم استخبارية، تقتصر على جمع المعلومات لمصلحة الجهات التي يعملون لحسابها، سواء كانوا يعملون لمصلحة دولهم أو لمصلحة بعض الأشخاص أو الشركات التي تتنافس فيما بينها، ومن مقتضيات عملهم أن لا يتركوا دليلا عن عملهم. لذلك فهم يتمتعون بالصفات التي يتمتع بها أعضاء الفئة السابقة من كونهم أشخاص من أصحاب الكفاءات ويتمتعون بقدرة عالية على التعامل مع الحاسب الآلي، إلى جانب قدرتهم على طمس الأدلة التي تتخلف عن جرائمهم.[2]

ويعرف الجاسوس "بأنه الشخص الذي يقوم بمجموعة من الأعمال المنجزة لصالح بلد أجنبي تهدف إلى إيقاع الضرر بسلامة بلد آخر، وتكون غالبا معلومات سرية عن الجيوش أو أجهزة المخابرات وسواها، وذلك بطرق ملتوية ومخالفة للقانون، مما يعرضه

[1] – محمد حماد مرهج الهيثي، جرائم الحاسوب، ط1، دار المنهج للنشر والتوزيع، عمان، الأردن، 2006.

[2] – محمد حماد مرهج الهيثي، مرجع سابق، ص 137.

لعقوبات قاسية.[1] "كما ورد تعريف للجاسوس في القانون الدولي العام أنه "هو الشخص الذي يعمل في خفية، أو تحت ستار مظهر كاذب في جمع أو محاولة جمع معلومات عن منظمة الأعمال الحربية لإحدى الدول التجارية بقصد إيصال هذه المعلومات لدولة العدد".[2]

والملاحظ على هادين التعريفين هو اقتصار التجسس على الأسرار العسكرية فقط بينما مفهوم التجسس يتعدى ذلك إذا ما تعلق الأمر بمعلومات الكترونية سرية فلا تقتصر على العسكرية فقط بل تتعدى ذلك لكل أنواع المعلومات السرية الالكترونية كما سيرد التفصيل أدناه في المبحث الخاص بجريمة التجسس الالكتروني.

الفرع الثاني: المحترفون والحاقدون

تعتبر فئة المحترفين أخطر طوائف مجرمي المعلوماتية حيث تهدف اعتداءاتهم إلى تحقيق الكسب المادي لهم وللجهات التي كلفتهم وسخرتهم لارتكاب جرائمهم كما تهدف اعتداءات بعضهم إلى تحقيق أغراض سياسية والتعبير عن موقف فكري أو نظري أو فلسفي، وإلى تحقيق جانب المعرفة التقنية المميزة والتنظيم العالي .ويتصف هؤلاء الطائفة بالتكتم، فلا يتبادلون المعلومات بشأن أنشطتهم بل يطورون معارفهم الخاصة

[1] – القاموس القانوني الثلاثي، قاموس قانوني موسوعي، شامل ومفصل عربي –فرنسي–انجليزي، موريس نخلة وآخرون، منشورات الحلبي الحقوقية، سوريا، 1992 ، ص 61.

[2] – علي صادق أبوهيف، القانون الدولي العام، الطبعة السابعة، منشأة المعارف الإسكندرية، 1965 ، ص846

ويحاولون قدر الإمكان عدم كشف طرقهم التقنية لارتكاب جرائمهم، وبشأن أعمارهم فأشارت الدراسات إلى أنهم الشباب الأكبر سنا مقارنة بالطائفة الأولى فتتراوح أعمارهم ما بين 25 و 40 سنة.[1]

أما عن الحاقدون، فهم طائفة يغلب عليها عدم توافر أهداف وأغراض الجريمة المتوفرة لدى الطائفتين المتقدمتين فهم لا يسعون إلى إثبات القدرات التقنية والمهارة وفي نفس الوقت لا يسعون إلى مكاسب مادية أو سياسية. إنما يحرك أنشطتهم الرغبة بالانتقام والثأر كثأر لتصرف صاحب العمل معهم أو لتصرف المنشأة المعنية معهم عندما لا يكونوا موظفين فيها، ولهذا فإنهم ينقسمون إما إلى مستخدمي النظام بوضعهم موظفين أو مشتركين أو على علاقة ما بالنظام محل الجريمة، وإلى غرباء عن النظام تتوفر لديهم أسباب الانتقام من المنشأة المستهدفة في نشاطهم.

ولا يتسم أعضاء هذه الطائفة بالمعرفة التقنية الاحترافية، ومع ذلك يشقى الواحد منهم في الوصول إلى كافة عناصر المعرفة المتعلقة بالفعل الذي ينوي ارتكابه، وتغلب على أنشطتهم من الناحية التقنية استخدام تقنيات الفيروسات والبرامج الضارة وتخريب النظم أو إتلاف كل بعض معطياته أو نشاط إنكار الخدمة تعطيل النظام أو الموقع المستهدف إن كان من مواقع الانترنت .وليس هناك ضوابط محددة بشأن أعمارهم، كما لا

[1] – نسرين عبد الحميد نبيه، مرجع سابق، ص 42.

تتوفر عناصر التفاعل بين أعضاء هذه الطائفة، ولا يفاخرون بأنشطتهم بل يعمدون على إخفائها وهم الطائفة الأسهل من حيث كشف الأنشطة التي قاموا بارتكابها لتوفر ظروف وعوامل تساعد على ذلك.[1]

هذه إذن أصناف مجرمي المعلوماتية والذين يسلكون خطورة تكمن خطورتهم في قدرتهم على اختراق الأنظمة التقنية والفنية التي توضع لحماية المعلومات، وفي كونهم أيضا ممن يعملون داخل المؤسسات وممن يعملون في مجال إدارة وتشغيل الحاسب الآلي، وتكمن خطورتهم في أن الذي يعمل في المؤسسة قد يجعل أي نظام من أنظمة الحماية التي تستخدمه المؤسسة عديم القيمة والنفع، لأنه على دراية به وبأسلوب عمله، ذلك يشجعهم على ارتكاب جرائمهم أولا وسهولة وصولهم إلى ما يبغون كونهم ممن يتعاملون مع الحاسب الآلي ثانيا، الأمر الذي لا يجعل الشكوك تحوم حولهم لأي سبب وكون فرصهم أكبر من غيرهم سواء بالدخول إلى المعلومات السرية أو الاطلاع على الأسرار التجارية فيسهل عليهم ارتكاب جرائمهم، وإخفاء الأدلة التي تدينهم مما يشكل صعوبة في اكتشافهم، وفي ذلك تكمن خطورتهم.[2]

وبشكل عام فإن المجرم المعلوماتي تكون غايته البحث عن معلومات يمكنه استخدامها كوسيلة لتنفيذ جرائمه وتتمثل عموما مميزاته بأنه:

[1] – نسرين عبد الحميد نبيه، مرجع سابق، ص 43.

[2] – محمد حماد مرهج الهيتي، مرجع سابق، ص 14.

- يتميز المجرم المعلوماتي بقدرته العالية والفنية في مجال تقنية الحاسب الآلي.
- قدرتهم العالية على التحرك عبر حدود الدول دون قيود بفضل قدرتهم على اختراق أنظمة الحاسب الآلي في مختلف البلدان عبر ما توفره لهم شبكة الاتصالات العالمية للانترنت.
- إن مرتكبي هذه الجرائم قد يكون الدافع إليها غرض شخصي كالتيار الفكري بين مرتكبيها لاسيما تعتمد على مقدار الإلمام بتقنية الحاسب الآلي، ويكون مجال التياري بينهم هو قدرة مجرم معلوماتي ما دون غيره على اختراق أنظمة الحماية التي يتمتع بها برنامج معين.
- في الكثير من الأحيان تتركز نشاطاتهم الإجرامية على الاعتداء على الحقوق المالية للأفراد والشركات والمؤسسات المالية والاقتصادية، فهم مجرمون يسببون أضرارا اقتصادية ومالية باهظة دولية ومحلية هذا ما تكشف عنه معظم الإحصائيات الجنائية في هذا الإطار وهؤلاء المجرمون دوافعهم مختلفة كما سبق الشرح. إذن الدافع في الجريمة المعلوماتية يختلف من جريمة لأخرى، حسب الحق الذي تنال منه الاعتداء أو المصلحة التي تتعرض لها فمثلا الدافع الذي يدفع الجناة لارتكاب جرائمهم عند المؤسسات والشركات المالية والاقتصادية الغالب فيه هو الإضرار بهذه الشركات والحصول على نفع مادي سواء بالمتاجرة بأسرارها الصناعية أو الاعتداء على حقوقها في الإنتاج أو الاعتداء على ذمتها المالية، ولكن دوما كما يقال الأمور تقاس بالغالب

لأن الغالب أن المجرم المعلوماتي من خلال جرائمه يسعى لتحقيق الكسب المادي رغم أن هناك دوافع كالانتقام وغيره وسيتم التفصيل في الجرائم المعلوماتية خاصة ما يتعلق منها بالاعتداء على الأسرار المعالجة آليا[1].

فالجرائم المعلوماتية هي التي تستهدف المعلومات، فهي أنماط السلوك الإجرامي التي تطال المعلومات المخزنة أو المعالجة في نظام الكمبيوتر أو المتبادلة عبر الشبكات، لهذا هي ترتكب بوسائل معلوماتية تتماشى مع التطور المستمر للتقنيات المستحدثة.

[1] – محمد حماد مرهج الهيثي، مرجع سابق، ص 137.

ملخص:

تطرقنا من خلال دراستنا لعنوان البحث فيما يخص الحماية الجنائية للمعطيات الشخصية عبر الأنظمة المعلوماتية في فصله الأول إلى الإطار المفاهيمي لنظام المعلوماتي في الجزائر من خلال قانون (04-15) وفي مبحثه الأول، أما في المبحث الثاني تطرقنا لأهمية نظام المعالجة الآلية للمعطيات للحماية الفنية وفي المبحث الثالث تطرقنا إلى الآلية من خلال الأساليب ارتكاب الجرائم المعلوماتية وأطرافها.

الفصل الثاني:

الإطار القانوني للإجراءات المتابعة والتحقيق والعقوبات المقررة لاعتداءات الماسة بالأنظمة المعلوماتية

يعد التطرق لأركان أنظمة المعالجة الآلية للمعلومات والجزاءات المقررة لها، سوف نعالج في هذا الفصل الآليات القانونية في مفهوم أصول التحقيق الجنائي في الجرائم الإلكترونية بما فيه جمع الأدلة والتفتيش وجمع الاستدلالات، وطرق متابعتها بما فيها الانتقال والمعاينة. وذلك تماشيا مع مواد القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الذي يسمح باستعمال وسائل قانونية جديدة تتلاءم وخصوصية هذا النوع من الجرائم إضافة إلى الأشخاص المخولين قانونا لكيفية إتباع الجريمة (ضباط الشرطة القضائية) والأقطاب الجزائية المتخصصة.

نقسم هذا الفصل إلى ثلاثة مباحث ، نتناول في المبحث الأول بعنوان إجراءات المتابعة والتحقيق في إجراءات الجرائم الماسة بأنظمة المعلوماتية.

والمبحث الثاني بعنوان القمة القانونية لدليل الرسمي في مجال الاثبات الجنائي.

والمبحث الثالث بعنوان الجزاءات والعقوبات المقررة لتجريم الاعتداء الماسة بالأنظمة المعلوماتية.

المبحث الأول: إجراءات المتابعة والتحقيق في الجرائم الماسة بأنظمة المعلوماتية

يقوم ضباط الشرطة القضائية والنيابة العامة بإجراءات المتابعة فور تلقي بلاغ أو دعوة عن وقوع جريمة معلوماتية مع التحقيق في هذه الجرائم وكل ما لهم صلة بالموضوع محل البلاغ، بجميع الاستدلالات من خلال الانتقال والمعاينة، التفتيش وتلقي المراسلات ...، وهذا ما سيتم عرضه في المطلبين التاليين:

المطلب الأول: من حيث إجراءات المتابعة

إن لضباط الشرطة القضائية دور فعال في ضبط أدلة الجرائم ومرتكبيها وكشف كل ما يتعلق بها حال وقوعها.

أما بالنسبة للجرائم المستحدثة فإنها تلقي المزيد من الأعباء على عاتق هذه السلطة وكذلك الأمر بالنسبة للسلطات القضائية، وذلك نظرا لضعف خبرة كلا منهما في مواجهة هذه الجرائم.

فمن المتصور أن يجد ضباط الشرطة القضائية أنفسهم غير قادرين على التعامل بالوسائل الاستدلالية والإجراءات غير التقليدية من هذه النوعية من الجرائم وقد يفشل جهاز الضبط القضائي في تقدير أهمية الجريمة نظرا لنقص الخبرة والتدريب ولهذه

الأسباب كانت من أولويات السياسة الوطنية لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال تكوين وتأهيل سلك ضباط الشرطة القضائية وأعوانهم.[1]

فعلى مستوى الدرك الوطني الذي باشر منذ سنة 2004 في عمليات تكوين مستخدمين من أجل إنشاء مركز وطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، فبموجب هذا العمل فإن الكثير من إطارات الدرك الوطني استفادوا من تكوين خاص في جامعات سويسرا وأمريكا، لهذا سواء في الجانب التقني للإعلام الآلي (أو القانوني) الجرائم المتصلة المعلوماتية (وكذلك تم التكوين في مؤسسات وطنية مثل مركز الدراسات التي عرض تكوينا في الأمن المعلوماتي في إطار التكوين كل سنة cerist والبحوث في الإعلام العلمي والتقني هذا البرنامج التكويني يهدف إلى تطوير كفاءات إطارات سلك الدرك الوطني، حتى تكون أكثر عملية في مجال مكافحة الجرائم المعلوماتية.[2] كما أن إطارات الدرك الوطني تساهم في عدة متقلبات وطنية ودولية تنصب موضوعاتها في إطار الجرائم المتصلة بالمعلوماتية بينما مصالح الأمن الوطني هي الغائبة عن مجالات تكريس مكافحة هذه الجرائم ما عدا ما يتم تنظيمه من معارض وملتقيات تتعلق بالموضوع وكذلك المشاركة والمساهمة في ملتقيات ومؤتمرات وطنية

[1] – عبد الفتاح بيومي حجازي، المرجع السابق، ص 232.

[2] – Hadjira Bouder : orientation de la politique pénale de prévention et de lutte contre la criminalité liées au TIC en Algérie, centre de recherche sur l'information scientifique et technique, CERIST 03, www.alexalaw.com, 01/05/2014, 22h 43.

ودولية تتناول بالأساس حقوق المؤلف في البيئة الرقمية. كما أن الدرك الوطني الفرنسي أنشأ منذ سنة 1998 إدارة مكافحة الجرائم المعلوماتية ضمن المصلحة التقنية للأبحاث القانونية والوثائقية، كل هذه الترسانة من الهيئات والمؤسسات لمكافحة الجرائم المعلوماتية بمختلف أشكالها ما هي إلا دليل على خطورة وتشعب هذا النوع الجديد من الإجرام وما يجب على السياسة الجنائية الجزائرية أن تتبعه، لأنه يلاحظ تباطؤ كبير في مجالات هذه الجرائم، وإفلات الكثير من المجرمين من العقاب خاصة فيما يتعلق بالاعتداء على الأشخاص والأموال التي تتم بواسطة شبكة الإنترنت وكذلك ما وصلنا إليه من تبادل الصور التي تحمل في طياتها خدش للحياء العام، وصور أشخاص أبرياء التقطت لهم تلك Bluetooth الهواتف المحمولة عبر الصور بعلمهم أو بدون علمهم ولكن وظفت تلك الصور لتكون أفعال إجرامية يعاقب عليها القانون، ولأنه لا توجد سياسة وقائية تحسيسية فإن فاعلي هذه الجرائم يتمادون في ارتكاب جرائمهم بدون متابعات قضائية تحد من إجرامهم لهذا فإن التدريب الجيد لعناصر الأمن والدرك الوطنيين والحملات التحسيسية للمواطنين ستحد من انتشار هذه الجرائم، وفي حالة وقوعها فإن المجرمين ينالون عقابهم لإمكانية الوصول إليهم عبر إجراءات قانونية تتسم بالشرعية.[1]

[1] – Hadjira Bouder, Opcit. www.alexalaw.com, 02/05/2014, 15h 00.

إن النيابة العامة في قضايا الجرائم المتصلة بالجريمة المعلوماتية، ولاسيما بعد اللجوء الواسع والمتزايد إلى شبكات الرقمية في حياة المواطنين، بينما يتطلب الأمر مظاهر تقنية وقانونية لمعالجة هذه القضايا، وعلى هذا فإن حتمية المعرفة ولو في حدها الأدنى لمعالجة فعالة في هذه المواد التي تجتاح المجال العقابي.

ومنذ سنة 2003 وفي إطار إصلاح العدالة، قامت وزارة العدل بإطلاق برنامج تكوين خاص بالقضاة هدفه رفع مستوى أداء القضاة، ويواكب التطور القانوني الجاري الخاص بجرائم المعلوماتية لأجل هذا تم إجراء أولًا دمج مادة الجريمة المعلوماتية في برنامج تكوين طلبة المدرسة الوطنية للقضاء على شكل ملتقيات ينشطها خبراء العديد من دورات التكوين في مختلف مجالات الجرائم المتصلة بتكنولوجيات الإعلام والاتصال منظمة بالخارج لصالح القضاة.

المطلب الثاني: من حيث إجراء التحقيق

من الصعب التحقيق في الجرائم المعلوماتية بسبب تعقيداته مما يستوجب الإلمام بأمور تقنية بحثة، تختلف عن الطرق العادية في مجال التحقيق وتوجيه الأسئلة والاستفسارات بحيث يجب أن تكون مقنعة وذات مصداقية وهذا ما يجعلها ذات طبيعة خاصة، وهذا ما سنتناوله في ما يلي:

أولا: الانتقال والمعاينة

من خصائص الجريمة المعلوماتية أنها قد تخلف آثار مادية إلى لزوم وقت طويل نسبيا لاكتشافها ما يعطي الفرصة لمرتكبي هذه الجرائم أن يضروا أو يتلفوا أو يعبثوا بالآثار المادية للجريمة إن وجدت وهو الأمر الذي يولد الشك في دلالة الأدلة المستقاة من المعاينة في الجريمة المعلوماتية.

وفي كل الأحوال فإنه عند تلقي البلاغ عن وقوع إحدى الجرائم المعلوماتية وبعد التأكد من البيانات الضرورية في البلاغ يتم الانتقال إلى مسرح الجريمة المعلوماتية ويتعين مراعاة ما يلي:[1]

1- ضرورة وجود معلومات مسبقة عن مكان الجريمة من حيث عدد الأجهزة المطلوب معاينتها وشبكاتها.

2- وجود خريطة توضح الموقع الذي ستتم معاينته وتفاصيل المبنى أو الطابق موضوع البلاغ، عدد الأجهزة والخزائن ويحدد ذلك من خلال مصادر سرية لجهات الأمن.

3- تحديد الأجهزة المحتمل تورطها في الجريمة المعلوماتية حتى يتم تحديد كيفية التعاون معها فنيا قبل المعاينة.

[1] – د عبد الفتاح بيومي، مرجع سابق، ص 317.

4- تأمين الأجهزة والمعدات التي سيتم الاستعانة بها في عملية المعاينة سواء كانت أجهزة أو برامج.

5- إعداد الفريق المتخصص الذي يتولى المعاينة من الخبراء ورجال الضبط والأمن.

6- تحديد البيانات والمهام والاختصاصات المطلوبة من كل عضو في فريق المعاينة على حدى، وذلك حتى لا تتداخل الاختصاصات.

7- إعداد خطة المعاينة موضحة بالرسومات مع تمام المراجعة التي تكفل تنفيذها على الوجه الأكمل.

8- أن تتم هذه العملية وفق مبدأ المشروعية وفي إطار ما تنص عليه القوانين الجنائية.

9- تأمين عدم انقطاع التيار الكهربائي لأن معاينة الأجهزة وما بها من برامج وشبكات وأنظمة تشغيل لا جدوى منها في ظل عدم وجود التيار الكهربائي.

عند معاينة مسرح الجريمة يرى الفقه الجنائي ضرورة وضع عدة ضوابط في معاينة مسرح الجريمة المعلوماتية وهذه الضوابط هي:

- تحديد أجهزة الحاسب الآلي الموجودة في مكان المعاينة وتحديد موقعها بأسرع فرصة ممكنة وفي حالة وجود وذلك لأجل تعطيل الاتصالات لمنع تخريب الأدلة الموجودة

serveurشبكة اتصالات وجوب البحث على خادم الملفات ومحوها، ويراعي تصوير الأجهزة الموجودة خاصة الأجهزة الخلفية منها.

- ضرورة وضع حراسة كافية على مكان المعاينة، ومراقبة التحركات داخله بل رصد الاتصالات الهاتفية من وإلى مسرح الجريمة مع إبطال مفعول أجهزة الهاتف النقال التي قد تساعد عن طريق تقنية معينة في تدمير أدلة الجريمة المعلوماتية متى تم توصيلها بالأجهزة محل المعاينة.
- ملاحظة الطريقة المعد بها النظام المعلوماتي والآثار التي يخلفها ومعرفة السجلات الإلكترونية التي نزود بها شبكة المعلومات لمعرفة موقع الاتصال ونوع الجهاز المتصل عن طريق الدخول إلى النظام أو الموقع أو الدخول معه في حوار وبروتوكولات الاتصال عبر الإنترنت وهو ما يعرف اختصارا ip.[1]
- كما يتعين كذلك ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن تحليل البيانات ومقارنتها والوصول منها إلى الدليل.
- عدم نقل المواد المعلوماتية خارج مسرح الجريمة إلا بعد التأكد من خلو المحيط الخارجي للكمبيوتر من مجالات القوى المغناطيسية التي قد تسبب في محو البيانات ولن يتأتى ذلك عن طريق خبراء الكمبيوتر.

[1] – يعرف الـip وهو اختصار الكلمة Internet Protocol أنه وسيلة لنقل البيانات من كمبيوتر مربوط بشبكة الإنترنت إلى كومبيوتر آخر على نفس الشبكة.

- التحفظ على محتويات سلة المهملات وما فيها من أوراق ممزقة وشرائط وأقراص ممغنطة وغير سليمة أو محطمة ورفع البصمات التي قد تكون عليها، وكذلك التحفظ على مستندات الإدخال والأوراق المطبوعة لجهاز الكمبيوتر والتي قد تكون ذات صلة بالجريمة.
- ضرورة قصر المعاينة على الباحثين والمحققين الذين لديهم كفاءة علمية وخبرة فنية في مجال المعلوماتية واسترجاع البيانات[1].

ثانيا: التفتيش وضبط الأشياء:

فيما يخص إجراءات التفتيش والحجز فتناولتها المادة 47 المعدلة في فترتها 3 و4 من قانون الإجراءات الجزائية، والتي تكون في محل سكني وفي كل ساعة من ساعات الليل أو النهار بناء على إذن مسبق من وكيل الجمهورية، ويمكن لقاضي التحقيق أن يقوم بأي عملية تفتيش أو حجز ليلا أو نهارا وفي أي مكان على امتداد الإقليم الوطني، أو يأمر ضباط الشرطة القضائية المختصين بذلك أو القاضي المنتدب لذلك وإذا وجدت أثناء التحري في جريمة متلبس بها أو تحقيق في هذه الاعتداءات إن كان هذا الشخص موقوفا للنظر أو محبوسا لسبب آخر يمكن أن يجرى التفتيش دون حضوره ودون الموافقة المسبقة من وكيل الجمهورية أو قاضي التحقيق وبحضور شاهدين

[1] – د عبد الفتاح بيومي، مرجع سابق، ص 317.

مسخرين أو ممثل يعينه صاحب المسكن وهذا لدواعي المحافظة على النظام العام. وقد نصت المادة 05 من قانون 09-04 المتعلق بمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها عن حالات اللجوء للتفتيش نظم المعلوماتية وهما الحالتين المتعلقتين بالوقاية من الأفعال الموصوفة بجرائم الإرهاب والتخريب والجرائم الماسة بأمن الدولة، وكذلك حالة توافر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.[1] فالتفتيش هنا وخلافا للتفتيش التقليدي عن الأدلة التي تثبت وقوع الجريمة ونسبتها إلى المتهم، إنما هي حالة إجراء تفتيش وقائي قد تسفر عنه أدلة يمكن أن تكون إثبات لتخطيط مسبق يراد به ارتكاب جرائم ذات خطورة على الأمن الداخلي للدولة، وكما نعلم فإن الأحكام العامة للتفتيش تقتضي بأنه "الأصل في القانون أن الإذن بالتفتيش هو إجراء من إجراءات التحقيق لا يصح إصداره إلا لضبط الجريمة، جناية او جنحة واقعة بالفعل وترجع نسبتها إلى متهم معين وأن هناك من الدلائل ما يكفي للتصدي لحرمة مسكنه أو حرمته الشخصية.[2] وكذلك الأمر في حالة التحري في الجنحة المتلبس بها (المادة 44 من قانون الإجراءات الجزائية).

[1] – طارق إبراهيم الدسوقي، الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة، مصر، ص 396.

[2] – أحمد مسعود مريم، رسالة ماجستير: آليات مكافحة جرائم تكنولوجيا الإعلام والاتصال في ضوء القانون 09-04، جامعة قاصدي مرباح، ورقلة، 2013/2012، ص 90.

كما نصت المادة 64 من ق.إ.ج التي تحيل أحكام المواد 44 إلى 47 من ق.إ.ج فيما يخص التحريات الأولية التي يجريها ضابط الشرطة القضائية كما أن الدستور نص على وجوب أن يتم التفتيش مكتوب صادر من السلطات القضائية المختصة المادة 40 من دستور 1966.

كما نصت أيضا المادة 5 والمادة 2 على إمكانية الدخول إلى منظومة معلوماتية موجودة على جهاز آخر متصل بالجهاز الأول لكن في مكان آخر مختلف تماما عنه داخل الدولة ومتصلان فيما بينهما بشبكة اتصالات أين كانت، يمكن الدخول إلى هذه المنظومة سواء كان الجهاز الثاني ملك للمتهم أو لشخص آخر فلا فرق، ما دامت هناك دلائل على إمكانية وجود المعطيات المبحوث عنها في ذلك النظام، وعليه فإن التفتيش في هذه الفرضية:

1- وجود دلائل وأسباب تدعوا للاعتقاد بأن الكشف عن المعطيات يكون بالبحث في المنظومة الثانية[1].

[1] – د عبد الفتاح بيومي، مرجع سابق، ص 317.

2- إعلام السلطات القضائية لمن يفرض المشرع إذن ثاني يسمح بهذا التفتيش وإنما مجرد إعلام السلطة القضائية التي تولت أمر هذا التفتيش (وكيل الجمهورية، قاضي التحقيق بحسب الحالة).

ثالثا: إجراءات اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

المواد من 65 مكرر5 إلى 65 مكرر10 يجوز لوكيل الجمهورية المختص أو قاضي التحقيق أن يأذن كتابيا في أجل 4 أشهر قابلة للتجديد بـ: اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية، مع إمكانية تسخير كل عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية مكلفة بالمواصلات السلكية واللاسلكية للتكفل بالجوانب التقنية مع ضرورة تحرير محضر عن كل عملية[1].

- وضع الترتيبات التقنية، دون موافقة المعنيين، من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط صور في أماكن خاصة ويسمح هذا الإذن بالدخول للمحلات السكنية أو غيرها في أي وقت ودون علم رضا صاحب المسكن ويجلب أن يتضمن كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها، والأماكن المقصودة

[1] - أحمد مسعود مريم، رسالة ماجستير، نفس المرجع، ص 92.

بالجريمة التي تبرر اللجوء لهذه التدابير ومدتها، وإذا ما اكتشفت جرائم أخرى غير التي التي وردت في الإذن فإن ذلك لا يكون سببا في بطلان الإجراءات العارضة كما يصف أو ينسخ ضابط الشرطة القضائية المأذون له المراسلات والصور أو المحادثة المسجلة أو المفيدة في إظهار الحقيقة في محضر يودع بالملف.[1]

رابعا إجراءات التسرب

المواد 65 مكرر 11 إلى 65 مكرر 18 قانون إجراءات جزائية.[2]

عندما تقتضي الضرورة التحري والتحقيق فيف الاعتداءات الماسة بأنظمة المعالجة الآلية لأنظمة المعلومات يقوم الضابط أو عون الشرطة القضائي تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية وبموجب إذن مكتوب ومسبب من وكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم، مع إمكانية استعمال هوية مستعارة وارتكاب الأفعال التالية دون اعتبارها تحريضا على ارتكاب الاعتداءات.

اقتناء أو حيازة أو نقل أو تسليم، أو إعطاء مواد أو منتوجات أو وثائق أو معلومات متحصل عليها من ارتكاب الاعتداءات. ويجب أن يذكر في الإذن الجريمة التي

[1] – أحمد مسعود مريم، رسالة ماجستير، نفس المرجع، ص 92.

[2] – انظر المواد 65 مكرر 11 إلى 65 مكرر 18، قانون إجراءات جزائية.

تبرر اللجوء إلى هذا الإجراء وهوية ضابط الشرطة القضائية التي تتم العملية تحت مسؤوليته، ويحدد كذلك مدة عملية التسريب التي لا يمكن أن تتجاوز 4 اشعر إلا في حالة التمديد من طرف القاضي الذي رخص بها والذي يمكنه أن يأمر في أي وقت بوقفها قبل انقضاء الفترة المحددة، وقد أقر ق.ا.ج عقوبات صارمة ضد من يكشف هوية ضابط أو عون الشرطة القضائية المتسرب في أي مرحلة من مراحل الإجراءات طبقا للمادة 65 مكرر16 من ق.ا.ج.

المبحث الثاني: القيمة القانونية للدليل الرقمي في مجال الإثبات الجنائي

لقد توجس كل من الفقه والقضاء خيفة من الدليل الرقمي لإمكانية عدم تعبيره عن الحقيقة نظرا لما يمكن أن تخضع له طرق الحصول عليه من التعرض والتزييف والتحريف والعبث، وهو ما يثير مسألة مشروعية الأخذ به، إذ يشترط الدليل الجنائي بوجه عام أن يكون مشروعا من حيث وجوده ومن حيث الحصول عليه[1].

كما يثير أيضا مسألة مصداقية أو حجية الدليل الرقمي في تعبيره عن الحقيقة التي تهدف إليها الدعوى الجزائية لاسيما إذا أخذنا بالاعتبار الصعوبات التي تصاحب استخلاصه، فضلا عن التطور في مجال المعلوماتية الذي قد يتيح العبث بهذا النوع من

[1] – د عبد الفتاح بيومي، مرجع سابق، ص 212.

الأدلة مما يجعل مضمونها مخالفا للحقيقة وعلى ذلك فكيف نضمن مصداقية هذه الأدلة وتكون لها الحجية في الإثبات، وما مدى اقترابها نحو الحقيقة؟ وهل مفهوم الحجية التي يجب أ يتمتع بها الدليل الجنائي يتعارض مع الطبيعة الخاصة للدليل الرقمي.

إن مجرد دليل يثبت وقوع الجريمة ونسبتها إلى شخص معين لا يكف للتعويل عليه، إذ يلزم أن تكون لهذه الأدلة قيمة قانونية، وقيمة الدليل الجنائي تتوقف على مسألتين رئيسيتين: الأولى هي مشروعية الدليل والثانية هي حجية الدليل على الوقائع المراد إثباتها.

المطلب الأول: مشروعية الدليل الرقمي

تعرف المشروعية بأنها التوافق والتقيد بالأحكام القانون في إطاره ومضمونه العام، فهي تهدف إلى تقرير ضمانة أساسية وجدية للأفراد لحماية حرياتهم وحقوقهم الشخصية ضد تعسف السلطة ومن التطاول عليها في غير الحالات التي رخص فيها القانون بذلك، من أجل حماية النظام الاجتماعي وبنفس القدر تحقيق حماية مماثلة للفرد ذاته.[1]

[1] – هلالي عبد الله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، ط2، دار النهضة العربية، 2008، ص 104.

لذلك فإنه لصحة الإجراءات التي تقوم بها التي تقوم بها جهة التحقيق أن تغلف بمبدأ المشروعية من أجل أن تثمر على دليل صحيح وسليم يعول عليه القضاء في أحكامه.

فلاشك أن مبدأ شرعية الجرائم الذي يستقيم عليه بنيان القانون الجنائي الموضوعي ينعكس على قواعد الإثبات الجنائي ويفرض خضوعها هي الأخرى لمبدأ المشرعية، والتي تستلزم عدم قبول أي دليل يكون البحث عنه أو الحصول عليه قد تم بطريقة غير مشروعة، وتعد مسألة قبول الدليل الجنائي بصفة عامة الخطوة الأولى التي يتخذها القاضي الجزائي تجاهه وذلك بعد التنقيب عنه قبل إخضاعه لتقديره، وقبول الدليل على هذا النحو يتسع ويضيق تبعًا للمبادئ التي تقوم عليها أنظمة الإثبات السائدة.

والحقيقة أن مشروعية الدليل هي مشروعية وجود مشروعية حصول

الفرع الأول: مشروعية وجود الدليل الرقمي

تقتضي مشروعية وجود الدليل الرقمي أن يكون المشرع قد قبل هذا الدليل ضمن أدلة الإثبات الجنائي.

أولا: المقصود بمشروعية الوجود: ويقصد بمشروعية وجود الدليل الرقمي أن يعترف المشرع بهذا الدليل من خلال تصنيفه في قائمة الأدلة القانونية التي يجيز القانون فيها

للقاضي الاستناد إليه وتكوين عقيدته، ولعل المعيار الذي يتحدد على أساسه موقف القوانين فيما يتعلق بسلطة القاضي الجزائي في قبول الدليل الرقمي يتمثل في طبيعة نظام الإثبات السائد في الدولة، إذا تختلف النظم القانونية في موقفها من حيث الأدلة التي يمكن قبولها في الإثبات[1].

ثانيا: موقف المشرع الجزائري من الدليل الرقمي: لقد عرفت التشريعات الإجرائية الجزائية نظامين رئيسيين هما:

– نظام الإثبات المفيد وفيه يقوم المشرع بتحديد أولوية الإثبات حصرا وكذا القوة الإثباتية لكل دليل من الأدلة بناء على قناعة المشرع بها. وهو ما يعرف بنظام الأدلة القانونية، إذ لا يكون لقناعة القاضي الجزائي في هذا النظام أي دور في تقدير الأدلة أو البحث عنها، فتحدد للقاضي الأدلة التي يجوز له قبولها واللجوء إليها في الإثبات ولا سبيل للاستناد إلى أي دليل لم ينص عليه القانون صراحة ضمن أدلة الإثبات.

– نظام الإثبات الحر الذي يقوم على أساس حرية الإثبات فلا يقوم المشرع بتحديد الأدلة بل يكون للقاضي دور إيجابي في البحث عن الأدلة وتقدير قوتها الثبوتية حسب قناعتها بها، فلا يلزمه القانون بأدلة للاستناد إليها في تكوين قناعته فله أن يبني هذه القناعة على

[1] – أحمد مسعود مريم، رسالة ماجستير: آليات مكافحة جرائم تكنولوجيا الإعلام والاتصال في ضوء القانون 09-04، جامعة قاصدي مرباح، ورقلة، 2013/2012، ص 90.

أي دليل وإن لم يكن مخصوصا عليه، بل إن المشرع في مثل هذا النظام لا يحفل بالنص على أدلة الإثبات فكل الأدلة تساوي قيمتها الإثباتية في نظر المشرع، والقاضي هو الذي يختار بين ما يطرح عليه وما يراه صالحا للوصول إلى الحقيقة وهو في ذلك يتمتع بمطلق الحرية لقبول الدليل أو رفضه إذا لم يطمئن إليه، فلا يتدخل المشرع في تحديد القيمة الإقناعية للدليل ولذلك فالقاضي في مثل هذا النظام يتمتع بدور إيجابي في مجال الإثبات في مقابل انحصار دور المشرع.[1]

وعلى هذا الأساس واسترشادا بما سبق ذكره فإن النظم القانونية التي تتبنى نظام الأدلة القانونية لا يمكن في ظلها الاعتراف للدليل الرقمي بأية قيمة إثباتية ما لم ينص عليه صراحة ضمن قائمة أدلة الإثبات، ومن ثم فإن خلو القانون من النص عليه سيهدر قيمته الإثباتية مهما توافرت فيه شروط اليقين، فلا يجوز للقاضي أن يستند إليه لتكوين قناعته.[2] وتطبيقا لهذا الفهم نص قانون الإثبات في المواد الجنائية البريطاني على قبول الدليل الرقمي وحدد قيمته الإثباتية تجاوبا واتفاقا مع طبيعة النظام القانوني في بريطانيا.[3]

[1] – هلالي عبد الله أحمد، مرجع سابق، ص 29.

[2] – طارق محمد الجملي، الدليل الرقمي في مجال الإثبات الجنائي، ورقة عمل مقدمة للمؤتمر المغاربي الأول حو المعلوماتية المنعقد في 2009/10/28.29 لأكاديمية الدراسات العليا طرابلس، ص 23.

[3] – الدول ذات الثقافة الأنجلوسكونية مثل بريطانيا والولايات المتحدة الأمريكية أخذت بنظام الإثبات القانوني.

ويمكن أن يعاب على نظام الإثبات القانوني أن من شأنه تقييد القاضي على نحو يفقده سلطته في الحكم بما يتفق مع الواقع فيحكم في كثير من الأحيان بما يخالف قناعته التي تكونت لديه من أدلة لا يعترف بها ذلك النظام بدأ ينحصر نطاقه حتى في الدول التي تعتبر الأكثر اعتناقا له.

ففي بريطانيا مثلا بدأت تخفف من غوائه حيث ظهر فيها ما يعرف بقاعدة الإدانة دون أدنى شك والتي مفادها أن القاضي يستطيع أن يكون قناعته من أي دليل وإن مفادها أن القاضي يستطيع أن يكون قناعته من أي دليل وإن لم يكن ضمن الأدلة المنصوص عليها متى كان هذا الدليل قاطعا في دلالته.

أما بالنسبة للنظم القانونية التي تعتمد نظام الإثبات الحر كما هو الحال عليه في القانون الجزائري (المادة 212 من قانون الإجراءات الجزائية) والقانون الفرنسي (المادة 427 قانون الإجراءات الجزائية الفرنسية) فإنه لا تثور مشكلة مشروعية الدليل الرقمي من حيث الوجود، على اعتبار أن المشرع لا يعتمد سياسة النص على قائمة لأدلة الإثبات فالأساس هو حرية الأدلة، لذلك فمسألة قبول الدليل الرقمي لا ينال منها سوى مدى اقتناع

القاضي به إذا كان هذا النوع من الأدلة يمكن إخضاعه لتقدير القاضي وهو ما سوف تناوله لاحقا عند الحديث على حجية الدليل الرقمي[1].

وفي هذا الصدد فإن المشرع الجزائري وكعيره من التشريعات المنتمية إلى نظام الإثبات الحر لا نجده قد أفرد نصوصا خاصة تحظر على القاضي مقدما قبول أو عدم قبول أي دليل بما في ذلك الدليل الرقمي، وهو أمر منطقي طالما أن المشرع الجزائري يستند لمبدأ حرية الإثبات حيث لم يتضمن قانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها أية أوضاع خاصة وترك الأمر للقواعد العامة ومنها أن الأصل في الأدلة مشروعية وجودها ومن تم فإن الدليل الرقمي سيكون مشروعا من حيث الوجود اصطحابا للأصل، ومن جهة أخرى فإنه وطبقا لمبدأ الشرعية الإجرائية فلا يكون الدليل مقبولا في عملية الإثبات إلا إذا كان مشروعا ذلك أن القاضي لا يقدر إلا الدليل المقبول ولا يكون كذلك إلا إذا كان مشروعا بأن تم البحث عنه والحصول عليه وفقا الطرق مشروعة.

[1] – أحمد مسعود مريم، رسالة ماجستير: آليات مكافحة جرائم تكنولوجيا الإعلام والاتصال في ضوء القانون 09-04، جامعة قاصدي مرباح، ورقلة، 2013/2012، ص 90.

الفرع الثاني: مشروعية الحصول على الدليل الرقمي:

إنه من الضروري أن يتم رسم ضوابط وأطر معينة يتعين أن تمارس في نطاقها عملية البحث عن الأدلة وتحصيلها والتحقيق فيها، بحيث لا تنحرف عن الغرض الذي يبتغيه المشروع من ورائها وهو الوصول إلى الحقيقة الفعلية في الدعوى وهي الهدف الأسمى لقانون الإجراءات الجزائية[1].

أولا: المقصود بمشروعية الحصول على الدليل الرقمي: إنه من المقرر أن الإدانة في أي جريمة لابد وأن تكون مبنية على أدلة مشروعة تم الحصول عليها وفق قواعد الأخلاق والنزاهة واحترام القانون من طرف الجهة المختصة بجمع الدليل الجزائي بما يتضمنه من أدلة مستخرجة من وسائل إلكترونية، ولا يكون مشروعا إلا إذا التنقيب عنه أو الحصول عليه أو كانت عملية تقديمه إلى القضاء أو إقامة أمامه بالطرق التي رسمها القانون، فمتى ما تم الحصول على الدليل خارج هذه القواعد القانونية فلا يعتد بقيمته مهما كانت دلالته الحقيقية وذلك لعدم مشروعيته، وعلى هذا الأساس فإن إجراءات جمع الأدلة الرقمية المتحصلة من الوسائل الإلكترونية إذا خالفت القواعد الإجرائية التي تنظم كيفية الحصول عليها فإنها تكون باطلة، وبالتالي بطلان الدليل المستمد منها ولا تصلح لأن تكون أدلة تبنى عليها الإدانة في المواد الجنائية. وفي إطار مشروعية الأدلة الرقمية نجد

[1] – علي حسين محمد الطوابلة، المرجع السابق، ص 99.

أن قانون الإجراءات الجنائية الفرنسي رغم أنه لم يتضمن أي نصوص تتعلق بمبدأ الأمانة والنزاهة في البحث عن الحقيقة إلا أن الفقه والقضاء كانا بجانب هذا المبدأ سواء في جانب التنقيب عن الجرائم التقليدية أم في مجال التنقيب في الجرائم المعلوماتية، ويشير رأي فقهي فرنسي إلى أن القضاء قد قبل استخدام الوسائل العلمية الحديثة في عملية البحث والتحري عن الجرائم تحث تحفظ أن يتم الحصول على الأدلة الجنائية ومن بينها الأدلة الرقمية بطريقة شرعية ونزيهة.[1]

وقد قضى في هولندا أنه إذا كانت بيانات الحاسوب المسجلة في ملفات الشرطة غير قانونية فذلك يؤدي إلى نتيجة مؤداها ضرورة محو هذه البيانات وعدم إمكانية استخدامها كدليل جنائي يسبب مبدأ استبعاد الأدلة غير القانونية. ومن قبيل الأدلة غير المشروعة الحصول على دليل رقمي من خلال إجراء مراقبة الاتصالات دون أن يكون محلا لإذن من السلطة القضائية المختصة أو اتخاذ ترتيبات تقنية من أجل تفتيش منظومة معلوماتية تؤدي إلى المساس بالحياة الخاصة للغير أو ممارسة الإكراه المادي أو المعنوي في مواجهة المشتبه فيه من أجل فك شفرة نظام من النظم المعلوماتية أو

[1] – علي حسن محمد الطوابلة: التفتيش الجنائي على نظم الحاسوب والإنترنت، عالم الكتب الحديثة، الأردن، ص 186.

التحريض على ارتكاب الجريمة عن طرف الضبطية.[1] ويعد من الطرق غير المشروعة أيضا استخدام التدليس أو الغش أو الخداع في الحصول على الأدلة الإلكترونية.

ولقد صادقت لجنة الوزراء التابعة للمجلس الأوروبي في 1981/01/28 على اتفاقية خاصة بحماية الأشخاص في مواجهة مخاطر المعالجة الآلية للبيانات ذات الطبيعة الشخصية، ومن المحاور المهمة التي تناولتها الاتفاقية ضرورة أن تكون البيانات المضبوطة صحيحة وكاملة ودقيقة ومستمدة بطرق مشروعة وعدم إنشائها أو استعمالها في غير الأغراض المخصصة لها، كما أن للشخص المعني الحق في التعرف والاطلاع على البيانات المسجلة المتعلقة به وتصحيحها وتعديلها ومناقضتها ومحوها إذا كانت باطلة.[2]

ولقد وضعت الدساتير والقوانين الإجرائية نصوصا تتضمن ضوابط لشرعية الإجراءات الماسة بالحرية، ومن تم مخالفة هذه النصوص في استخلاص الدليل يضع هذا الدليل بلا مشروعية والقول بذلك يهدر قيمته، فمشروعية الدليل تتطلب صدقه في مضمونه وأن يكون هذا المضمون قد تم الحصول عليه بطرق مشروعة تدل على الأمانة والنزاهة من حيث طرق الحصول عليه.

[1] – علي حسين محمد الطوابلة، المرجع السابق، ص 189.

[2] – مشار إليه لدى رشيدة بوبكر، مرجع سابق، ص 492.

والحقيقة أن مشروعية الدليل تعد قيدا وخطا فاصلا بين حق الدولة في توقيع العقاب بضمان أمن واستقرار المجتمع من جهة، وبين ضمان حقوق الأفراد وحرياتهم من جهة أخرى لذلك السؤال المطروح في هذا الإطار ما هو موقف القضاء من الدليل غير المشروع وما هي قيمة الإثبات الجنائي؟

ثانيا: موقف القضاء من الدليل غير المشروع

إن هذا التساؤل يقود إلى بحث قيمة كل من دليل الإدانة ودليل البراءة لمعرفة قيمتهما في الحالتين:

– فبالنسبة لدليل الإدانة فإن الأمر يقتضي من أجل كسر قرينة البراءة التي يتمتع بها المتهم أن تكون الأدلة التي يؤسس عليها حكم الإدانة مشروعة.[1] ويستوي في ذلك إن كانت أدلة تقليدية أو مستخلصة من الوسائل الإلكترونية وأي دليل تم الحصول عليه بطريقة غير مشروعة أو بوسيلة مخالفة للقانون يعتبر غير مقبول في عملية الإثبات لأنه إذا ما سمح بقبول أدلة وليدة من إجراءات باطلة أدى ذلك إلى إهدار الضمانات التي كفلها القانون لحماية حقوق المواطن وكرامته، وترتيبا على ذلك فإنه لا يجوز للقاضي القبول بدليل رقمي تم الحصول عليه من إجراء التسرب جرى القيام به دون مراعاة

[1] – جميل عبد الباقي الصغير، أدلة الإثبات الجنائي، والتكنولوجيا الحديثة، دار النهضة العربية القاهرة، 2002، ص 111.

الشروط الشكلية والموضوعية للإذن بمباشرة هذا الإجراء، أو كان الدليل متحصلا عليه عن طريق إكراه المتهم المعلوماتي من أجل فك شفرة الدخول إلى النظم المعلوماتية أو كلمة السر اللازمة للدخول إلى ملفات المعلومات المختزنة أو القيام بإجراء التنصت أو المراقبة الإلكترونية عن بعد دون مسوغ قانوني، ويكون الدليل المتحصل عليه وفق الطرق السابقة باطلا وعدم إنتاج الآثار القانونية المترتبة عليه[1].

والقاعدة أن الإجراء الباطل يمتد بطلانه إلى الإجراءات اللاحقة له مباشرة وهو الرأي الراجح الذي أخذ به الشرع الجزائري بنص المادة 191 من قانون الإجراءات الجزائية التي نصت على أنه تنظر غرفة الاتهام في صحة الإجراءات المرفوعة إليها وإذا تكشف لها سبب من أسباب البطلان قضت ببطلان الإجراء المشوب به وعند الاقتضاء ببطلان الإجراءات التالية له كلها أو بعضها، وقد أوصى المؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات في مجال حركة إصلاح الإجراءات الجنائية وحماية حقوق الإنسان، بمجموعة من التوصيات منها التوصية رقم 18 التي تنص على أن كل الأدلة التي تم الحصول عليها عن طريق انتهاك حق أساسي للمتهم والأدلة الناتجة عنها تكون باطلة ولا يمكن التمسك بها أو مراعاتها في أي مرحلة من مراحل الإجراءات، وقد

[1] – أحمد مسعود مريم، رسالة ماجستير، نفس المرجع، ص 70.

أشار هذا المؤتمر إلى ضرورة احترام مبدأ المشروعية عند البحث عن الدليل في الجرائم المعلوماتية في بيئة تكنولوجيا المعلومات وإلا ترتب عليها بطلان الإجراء[1].

أما إذا كان الدليل الرقمي غير المشروع دليل براءة فإن الأمر فيه اختلاف ويمكن رد ذلك إلة ثلاث اتجاهات:

– الأول يرى أن المشروعية لازمة في كل دليل سواء كان دليل لإدانة أو براءة، وإثبات البراءة كالإدانة لا يكون إلا من دليل تم الحصول عليه من خلال سبل مشروعة ولا يصح أن يفلت إثبات البراءة من قيد المشروعية الذي هو شرط أساسي في أي تشريع.

– والاتجاه الثاني يرى أن المشروعية لازمة في أدلة الإدانة دون البراءة لأن الأصل في الإنسان البراءة ولا حاجة لإثباتها.

– أما الاتجاه الثالث أن أدلة البراءة غير المشروعة يمكن الأخذ بها وقبولها في حالات دون أخرى طالما أنه تم الحصول عليها بوسائل لا تصل إلى حد الجريمة وإنما تتضمن مخالفة قاعدة إجرائية إذ يمكننا في هذه الحالة الاستناد إلى هذه الأدلة.

[1] – أحمد مسعود مريم، رسالة ماجستير، نفس المرجع، ص 92.

والراجح من بين هذه الاتجاهات هو الاتجاه الذي يقصر المشروعية على دليل الإدانة دون البراءة لأن عدم قبول دليل البراءة بحجة أنه غير مشروع يؤدي إلى نتيجة خطيرة وهي إمكانية إدانة بريء وهو ما لا يستقيم عدلا ولا منطقا.

المطلب الثاني: حجة الدليل الرقمي في إطار نظرية الإثبات الجنائي

إن مسألة تقييم الدليل الجنائي في إثبات الواقعة الجرمية هي مسألة موضوعية محضة، للقاضي أن يمارس سلطته التقديرية فيها، لأجل هذا فالسائل في الفقه الجنائي أن القاضي الجزائي له الحرية في تقدير الأدلة الجنائية وتكوين قناعته، وأن يبني حكمه على أي دليل متى اطمأن إليه وحتى ولو كان هذا الدليل مستمدا من محاضر جمع الاستدلالات.

ولا يشترط أن يكون الدليل الذي يستند إليه القاضي صريحا دالا على الواقعة المراد إثباتها بل يكفي أن يكون استخلاصها استنتاجا من الظروف والقرائن وترتيب النتائج على المقدمات، وأدلة الدعوة تخضع في كل الأحوال لتقدير القاضي مادام الدليل غير مقطوع بصحته.[1] ويترتب على ذلك أن الأدلة الجزائية لا تحظ أمام القاضي الجزائي بقوة حاسمة

[1] – أشرف عبد القادر قنديل، النظرية العامة للبحث الجنائي وأثرها في عقيدة القاضي، دار الجامعة الجديدة، ص 235.

في الإثبات، وعلى هذا الأساس فكما يصح للقاضي أن يؤسس اقتناعه على أي دليل يصح له أن يصدره.

المبحث الثالث: الجزاءات والعقوبات المقررة لجرائم الاعتداءات الماسة بالأنظمة المعلوماتية:

لقد نصت المادة 13 من الاتفاقية الدولية للإجرام المعلوماتي بموجب أن تكون العقوبات المقررة نتيجة ارتكاب الجرائم المعلوماتية رادعة ومتضمنة لعقوبات سالبة الحرية، كما نصت على وجوب تطبيق عقوبات الشخص المعنوي بناء على مبدأ له مساءلة الشخص المعنوي الوارد في المادة 12 من نفس الاتفاقية.

وباستمرار نصوص المواد الخاصة بجرائم المساس بأنظمة المعالجة الآلية للمعطيات الواردة في قانون العقوبات الجزائري، من المادة 394 مكرر إلى غاية المادة 394 مكرر7نجد أن المشرع الجزائري قد تبنى هذا المبدأ في تقريره للجزاءات الواجبة على هذا النوع من الجرائم فسن العقوبات تطبق على الشخص الطبيعي وعقوبات تطبق على الشخص المعنوي وذلك ما سنتناوله فيما يلي:

المطلب الأول: العقوبات المطبقة على الشخص الطبيعي

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

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

أولا: جريمة الدخول والبقاء :

أ/ الدخول والبقاء بالغش (الجريمة البسيطة): العقوبات المقررة هي 3 أشهر إلى سنة حبس و 50.000 دج إلى 100.000 دج غرامة (المادة 394 مكرر) .

ب/ الدخول والبقاء بالغش (الجريمة المشددة): تضاعف العقوبة إذا ترتب عن هذه الأفعال حذف أو تغيير لمعطيات العقوبة 06 أشهر إلى سنتين وغرامة من 50.000 دج إلى 150.000 دج إذا ترتب عن الدخول أو البقاء غير المشروع تخريب لنظام اشتغال المنظومة (المادة 394 مكرر/02-03).

[1] – أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة، ط1، 2008، ص 127.

ثانيا: جريمة التلاعب بالمعطيات

نصت عليها المادة 394 مكرر1، قانون العقوبات الجزائري. بالحبس من 6 أشهر إلى 03 سنوات وعقوبة الغرامة التي تتراوح من 500.000 دج إلى 2.000.000 دج والملاحظ أن عقوبة التلاعب بالمعطيات تفوق جريمة الدخول والبقاء وغير المصرح بهما سواء كانت هذه الأخيرة في صورتها البسيطة أو المشددة، لأن في صورتها البسيطة لا تؤدي إلى أضرار معينة تلحق بالمعطيات أو بنظام معالجتها وحتى في صورتها المشددة، وإن أدت إلى نفس النتائج التي تؤدي إليها جريمة التلاعب بالمعطيات وهي إزالة المعطيات أو تعديلها، فإن العقوبة المقررة لجريمة التلاعب تبقى أكبر لأنها جريمة عمدية يتوافر لدى مرتكبيها القصد الجنائي بينما لا يتوافر هذا القصد لدى مرتكب جريمة الدخول أو البقاء المشددة.[1]

ثالثا: جريمة التعامل في معطيات غير مشروعة

تعاقب المادة 394 مكرر2 من قانون العقوبات الجزائري على جريمة التعامل في معطيات غير مشروعة بعقوبة الحبس من شهرين إلى 3 سنوات وبالغرامة المالية من 1.000.000 دج إلى 5.000.000 دج بهذا يكون ترتيب هذه الجريمة من حيث عقوبة

[1] – د/ نائلة قورة: جرائم الحاسب الآلي الاقتصادية، دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية، 2004، ص 228.

الحبس هو الثاني بين جريمتي الدخول والبقاء غير المصرح بهما سواء في صورتها البسيطة أو المشددة بين جريمة التلاعب بالمعطيات (غير أن حدها الأدنى يقل عن كلتا الجريمتين).

ذلك أن حدها الأقصى يزيد عن الحد الأقصى لجريمة الدخول أو البقاء في صورتيهما (سنة وسنتين) وتتساوى مع الحد الأقصى لجريمة التلاعب بالمعطيات (03 سنوات).

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

الفرع الثاني: العقوبات التكميلية

نصت المادة 394 مكرر6 من قانون ع.ج. العقوبات التكميلية، التي يمكن الحكم بها إلى جانب العقوبات الأصلية وحاء فيها مع الاحتفاظ بحقوق الغير حسن النية، يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها في هذا القسم، علاوة على إغلاق المحل أو مكان الاستعمال

[1] – محمد خليفة، مرجع سابق، ص 219.

إذا كانت الجريمة قد ارتكبت بعلم مالكها ويستخلص من نص هذه المادة العقوبات التكميلية التالية:

أولا: مصادرة الأجهزة والوسائل والبرامج المستخدمة: وذلك مع الاحتفاظ بحقوق الغير حسن النية، وتجدر الإشارة إلى أن المشرع نص فقط على مصادرة الأجهزة والبرامج والوسائل المستخدمة فقط، وأغفل مصادرة الوسائل الموجهة لارتكاب الجريمة من المعطيات المخزنة أو المعالجة أو المرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها جرائم المساس بأنظمة المعالجة الآلية للمعطيات المنصوص عليها في الفقرة الأولى من المادة 394 مكرر 2 قانون العقوبات الجزائري، حيث أن عبارة "المستخدمة" الواردة في نص المادة 394 مكرر 6 الخاصة بالعقوبات التكميلية تفيد صيغة الماضي وهذا ما نصت عليه المادة 394 مكرر 6 من قانون.ع.ج التي تنص على العقوبات التكميلية، وفي فقرتها الثالثة على المصادرة فنجد أنها تناولت مصادرة الشيء الذي كان موجها للقيام.

ثانيا: إغلاق المواقع التي تكون محلا للجريمة من جرائم الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات.[1]

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

ثالثا: إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها وأضاف المشرع شرط علم المالك إذا كان على سبيل المثال الجاني مستأجرا للمحل المالك المؤجر له، ويعلم خطورة الأفعال التي يقوم بها الجاني، كغلق نادي الإنترنت الذي ترتكب فيه هذه الجرائم مع علم مالك أو مسير النادي بالأفعال الخطيرة التي يقوم بها زبونه، ولكن المشرع لم يحدد المدة القصوى لغلق المحل أو مكان الاستغلال، مما يطرح مشكلا في تنفيذ هذه العقوبة فمن جهة يعتبر إغلاق المحل أو أماكن كعقوبة تكميلية للشخص الطبيعي المسؤول جزئيا، ومن جهة أخرى لا يمكننا الرجوع إلى القواعد العامة للمسؤولية الجزائية للشخص المعنوي لتحديد المدى المدة، لأنه في هذه الحالة تقع المسؤولية الجزائية على عاتق الشخص الطبيعي فيوجد حسب رأينا في توقيع الجزاء، حيث توقيع جزاء خاص بالشخص المعنوي غلق المحل على الشخص الطبيعي[1].

– إن العقوبة التكميلية الواردة في المادة 394 مكر 6 قانون العقوبات الجزائري غير كافية في مواجهة الحالات العديدة التي يمكن أن يرتكبها الشخص الطبيعي فمثلا تنص المادة على العقوبة التكميلية الخاصة بالموظف العمومي المصرح له بالدخول على نظام الآلية للمعطيات لكنه يبتعد ذلك إلى ارتكاب جرائم أخرى متعلقة بالمنظومة المعالجة آليا، وكذلك الشيء بالنسبة للوظيفة المهنية فيما يخص المحامين أو الأطباء مثلا، وكذلك

[1] – د/ أحسن بوسقيعة، مرجع سابق، ص 448.

الوظيفة الاجتماعية إذا ارتكبت الجريمة عند تأدية الوظيفة أو بمناسبتها وهذا ما جاءت به أحكام المادة 323-05 من قانون العقوبات الفرنسي والتي نصت على تكميلية أخرى، ندعو المشرع الجزائري إلى الأخذ بها وهي كما يلي:

- المنع لمدة أقصاها 5 سنوات من الحقوق المدنية والسياسية.

- المنع لمدة أقصاها 5 سنوات من ممارسة الوظيفة العمومية أو النشاط المهني أو الاجتماعي إذا ارتكبت الجريمة أثناء تأدية الوظيفة أو بمناسبتها.

- مصادرة الشيء الذي استخدم أو الموجه لارتكاب الجريمة أو الشيء محل الجريمة الغلق لمدة أقصاها 5 سنوات للمؤسسات، أو لحد أو عدة مؤسسات المقاولة التي استعملت في ارتكابها الأفعال المجرمة.

- الحرمان لمدة أقصاها 5 سنوات من الصفقات العمومية.

- المنع لمدة أقصاها 5 سنوات في إصدار الشيكات بما فيها التي تسمح سحب الأموال من طرف الساحب لدى المسحوب له المرخص أو المرخص لهم بذلك. تقليل أو نشر الحكم أو القرار الصادر.[1]

[1] - د/ أحسن بوسقيعة، مرجع سابق، ص 449.

الفرع الثالث: الظروف المشددة

نصت المادة 394 مكرر 02-03 على ظروف تشدد به عقوبة جريمة الدخول والبقاء غير المشروع داخل النظام، ويتحقق هذا الظرف عندما ينتج عن الدخول و البقاء إما حذف أو تغيير المعطيات التي يحتويها النظام وإما تخريب نظام اشتغال المنظومة.

في الحالة الأولى تضاعف العقوبات المقررة في الفقرة الأولى من المادة 394 مكرر، وفي الحالة الثانية تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50.000 دج إلى 150.000 دج .

هذه الظرف المشدد هو ظرف مادي يكفي أن تقوم بينه وبين الجريمة الأساسية وهي جريمة الدخول والبقاء غير المشروع علاقة سببية للقول بتوافره.

نصت المادة 394 مكرر 3 على أن تضاعف العقوبات المقررة للجرائم الماسة بالأنظمة المعلوماتية وذلك إذا استهدفت الجريمة الدفاع الوطني والهيئات والمؤسسات الخاضعة للقانون العام[1].

[1] – أنظر نص المادة 394 مكرر 5، من قانون العقوبات الجزائري.

المطلب الثاني: العقوبات المطبقة على الشخص المعنوي

لقد كانت العقوبة إحدى أهم الحجج التي استند إليها المعارضون لمبدأ إقرار مسؤولية الشخص المعنوي حيث رأوا أنه لا يمكن تطبيقها على هذا الأخير خاصة تلك العقوبات السالبة والمقيدة للحرية، لكن وبعد اتساع تطبيق عقوبة الغرامة وابتكار عقوبات جديدة تتلاءم وطبيعة الشخص المعنوي لم لهذا الاعتراض محل، ولقد تضمنت المادة 18 مكرر من قانون العقوبات الجزائري بعد تعديله سنة 2004، أنواع العقوبات المطبقة على الشخص المعنوي في مواد الجنايات والجنح، وأول هذه العقوبات هي الغرامة التي تساوي من مرة إلى خمس مرات الحد الأقصى المقررة على الشخص الطبيعي، لكن المادة 394 مكرر 4، فهي غرامة ذات حد واحد أو حين الأخذ بالحد الأقصى لهذه العقوبات، وهو خمس مرات فيما يتعلق بجرائم المعطيات، وفيما يخص القانون الفرنسي فقد نصت المادة 323-6 من قانون العقوبات بأن الأشخاص المعنوية يمكن أن يحكم عليها بالمسؤولية الجنائية وفقا للشروط التي حدتها المادة 121-2 وإن العقوبات المقررة عليها هي:[1]

- الغرامة وفق ما تنص عليه المادة 131 -38.

- العقوبات المحددة في المادة 131-39.

[1] - أنظر نص المادة 121 وما يليها من قانون العقوبات الجزائري

– العقوبات المحددة في المادة 131–39 فقرة 2 بالنسبة للنشاط المهني الذي وقصت بمناسبة الجريمة.

وتنقسم العقوبات المقررة على الشخص في قانون العقوبات الجزائري وكذا الفرنسي بالنظر إلى طبيعة الحق الذي تمس أنواع:

– العقوبات الماسة بوجود الشخص المعنوي أو حياته وتتمثل في الكل.

– العقوبات الماسة بالذمة المالية للشخص المعنوي وتتمثل في الغرامة والمصادرة.

– العقوبات الماسة بالنشاط المهني للشخص المعنوي وتتمثل في إغلاق المؤسسة وكذا المنع من ممارسة النشاط المهني أو الاجتماعي.

– العقوبات الماسة بالسمعة وتتمثل في نشر الحكم وتعليقه.

– العقوبات الماسة بحق الشخص المعنوي في التعالم بحرية لتحقيق أهداف التي أنشئ من أجلها، وتتمثل في الحراسة القضائية والإقصاء من الصفقات العمومية ويضيف القانون الفرنسي المنع حتى الدعوة العامة للإخار وكذلك المنع من إصدار الشيكات.

– وهذه العقوبات في القانونين الجزائري والفرنسي ليست خاصة بجرائم المعطيات وإنما يمكن أن توقع على الجرائم التي يرتكبها الشخص المعنوي وليس هناك ما يميز جرائم المعطيات إلا عقوبة الغرامة المشددة.

المطلب الثالث: عقوبة جريمة الاتفاق والشروع الجنائي

نصت عليه المادة 11 من الاتفاقية الدولية للإجرام على تجريم التحضير للجرائم الماسة بالأنظمة المعلوماتية، وقد تبنى المشرع الجزائري مبدأ معاقبة الاتفاقية الجنائي بنص المادة 394 مكرر 5 من قانون العقوبات الجزائري إذ جاء فيها "أن كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو بعدة أفعال مادية ، يعاقب بالعقوبات المقررة بالجريمة ذاتها ".

وإن الحكمة التي ارتآها المشرع من تجريم الاشتراك في مجموعة أو في اتفاق بغرض الإعداد لجريمة من الجرائم الماسة بالأنظمة المعلوماتية هو أن مثل هذه الجرائم تتم عادة في إطار مجموعة، كما أن المشرع أراد توسيع نطاق العقوبة فأخضع الأعمال التحضيرية للعقوبة المقررة للجريمة التي تم التحضير لها إذا تمت في إطار اتفاق جنائي،

بمعنى أخر أن الأعمال التحضيرية المرتكبة من طرف شخص منفرد غير مشمولة بالنص.[1]

ويعاقب المشرع الجزائري على الاشتراك في الاتفاق الجنائي بعقوبة الجريمة التي تم التحضير لها فإذا تعددت الجرائم التي يتم التحضير لها تكون العقوبة هي عقوبة الجريمة الأشد.

وشروط المعاقبة على الاتفاق الجنائي بمن استخلاصها من نص المادة 394 مكرر 5 من قانون العقوبات الجزائري والتي هي:

– أما الشروع فنصت عليه المادة 11 من الاتفاقية الدولة لإجرام المعلوماتي وتبناها المشرع الجزائري في المادة 394 المكرر 7 من قانون العقوبات الجزائري والجرائم الماسة بالأنظمة المعلوماتية لها وصف جنحي ولا عقاب على الشروع في الجنح إلا بنص.

– نصت المادة 394 مكرر 7 قانون العقوبات الجزائري "يعاقب على الشروع في ارتكاب جنح المنصوص عليها في هذا القسم بعقوبات المقررة لجنحة ذاتها"

[1] – أمال قارة، مرجع سابق، 130.

يبدو من خلال هذا النص رغبة المشرع في توسيع نطاق العقوبة تشمل أكبر قد من الأفعال الماسة بالأنظمة المعلوماتية، إذ جعل الشروع في إحدى الجرائم الماسة بأنظمة المعلوماتية معاقب عليه بنفس عقوبة الجريمة التامة.

ومن خلال استقراء نص المادة أن الجنحة الواردة بنص المادة 394 مكرر 5 من قانون العقوبات الجزائري مشمولة بهذا النص، أي أن المشرع الجزائري بهذا المنطق يكون قد تبنى فكرة الشروع في الاتفاق الجنائي.[1]

[1] – أمال قارة، مرجع سابق، ص 133.

ملخص الفصل الثاني:

من خلال تطرقنا في الفصل الأول والذي تحدثنا فيه على الإطار المفاهيمي فالفصل الثاني تطرقنا إلى الإطار القانوني للإجراءات المتابعة والتحقيق والعقوبات المقررة للاعتداءات الماسة الأنظمة المعلوماتية.

حيث قسمنا هذا الفصل إلى ثلاث مباحث والتي تناولنا وعلى التناوب:

- إجراءات المتابعة والتحقيق في الجرائم الماسة بأنظمة المعلوماتية.
- القيمة القانونية للدليل الرقمي في مجال الإثبات الجنائي.
- والجزاءات والعقوبات المقررة لجرائم الاعتداء الماسة أنظمة المعلوماتية.

الخاتمة

خاتمة

بعد هذا العرض المتواضع لموضوع أنظمة المعالجة الآلية للمعطيات لاحظنا تشعب في الموضوع وصعوبة خصوصا ما يتعلق منه بخصوصية جرائم المعطيات من حيث الإجراءات ثم أن هذه الأخيرة من الجرائم الحديثة نسبيا التي تستلزم دراسات مستقبلية محاولة لوضع المبادئ العامة بكل ما يتعلق من جرائم ترتبط بالتطور الإلكتروني والمعلوماتي ووسائل الاتصال الحديثة، وهذا ما يتطلب تدخلا تشريعيا من أجل وضع حماية قانونية متكاملة وسد جميع الثغرات قانون العقوبات والتي تعد صالحة لمواكبة نظم المعلومات ولعل أبرز المشكلات التي أفرزتها الجريمة تتمثل في:

– من أبرز المشكلات التي أثارتها الجريمة المعلوماتية أن التحديات الإجرائية في ميدان التحري والتحقيق والمحاكمة من حيث الاختصاص والقانون الواجب التطبيق خاصة وأن الجريمة المعلوماتية كما سبق وأن وضحنا هي جريمة عالمية لا تعترف بالحدود الدولية والإقليمية.

وأنه رغم توفر النصوص القانونية الموضوعية فإن مكافحة جرائم المعلوماتية رهينة بالمعيقات الإجرائية التي أفرزتها هذه الجرائم، فبالنسبة لمرحلة التحري والتحقيق فإن أول معوق يواجه حسن سيرها هو غياب القدرات التأهيلية والوسائل الفنية التي تتيح سرع إدراك ما حصل وأن غياب التأهيل قد يؤدي إلى إتلاف الدليل على الجريمة.

فيكون الأثر إفلات مرتكبي هذه الجرائم من العقاب. هذا إضافة إلى قصور النصوص الإجرائية التقليدية للضبط والتفتيش لتلاءم الجرائم المعلوماتية التي تتميز بسهولة إخفاء الدليل.

وإلى حين انتهاء التحقيق تبدأ مشكلات المحاكمة وأولها الاختصاص المتعلق بمكان وقوع الجريمة أو بناء على معيار إلحاق الضرر. إضافة إلى القانون واجب التطبيق باعتبار أن الجريمة المعلوماتية جريمة عالمية عابرة للحدود.

لهذا يكون من الضروري الإسراع بسن قواعد إجرائية تتلاءم مع طبيعة الجريمة المعلوماتية حتى تكون القواعد الموضوعية المجرمة لها أكثر فعالية هذا من جهة، ومن جهة أخرى فإنه لابد من تكاثف الجهود الدولية والإقليمية في حقل جرائم المعلوماتية لتخطي العقبات التي تطرحها هذه الجرائم.

بعض الاقتراحات:

– ضرورة تدريب وتأهيل الضبطية القضائية من العاملين مع الإدعاء العام (النيابة) والقضاء على كيفية التعليل مع هذا النوع من الإجرام وتحقيق التعاون مع التقنيين من أصحاب الخبرة، وذلك بعقد دورات تدريبية بشكل دوري ودائم للاستفادة من خبراتهم وإرشاداتهم ابتداء من مرحلة الاستدلال وجمع الأدلة، وانتهاء بقرارات المحاكم.

– تدريس مواد الأنظمة المعلوماتية والجرائم التي قد تنشأ منها في كليات الحقوق والمعاهد القضائية.

– تفعيل دور الأسرة في متابعة الأبناء لوقايتهم من الآثار السلبية والمخاطر المترتبة عن الاستخدام غير الآمن لشبكات الإنترنت.

– التطور المستمر للتشريعات القائمة بما يحقق مرونتها ومواكبتها للتطورات المتسارعة في مجال تكنولوجيا المعلومات.

ضرورة التعاون الدولي لمواجهة الجرائم في البيئة المعلوماتية الإلكترونية وذلك من خلال الدخول في اتفاقيات ومعاهدات تجرم صور هذه الجرائم كلها وتبين كذلك الاختصاص المكاني في حال وقوعها، كما يمكن أن تنص هذه الاتفاقيات على تبادل الخبرات والمعلومات في المسائل المتعلقة بالجرائم المعلوماتية وهذا ما يجب أن يحدث بالنسبة للجزائر وضرورة انضمامها لاتفاقية بودابست 2001 لمكافحة الجريمة المعلوماتية.

قائمة المراجع

قائمة المراجــع:

1/ المراجع باللغة العربية

1- الكتب:

1- أيمن عبد الحفيظ، إستراتيجية مكافحة جرائم استخدام الحاسب الآلي، الناشر المؤلف، 2003.

2- أيمن عبد الله فكري، جرائم نظم المعلومات دراسة مقارنة، دار الجامعية الجديدة للنشر، الإسكندرية، ب ط، 2007.

3- خيثر مسعود، الحماية الجنائية لبرامج الكومبيوتر، دار الهدى للطباعة والنشر، عين مليلة، الجزائر، 2010.

4- رامي متولي القاضي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية، دار النهضة العربية، القاهرة، ط1، 2011.

5- رشدي محمد علي محمد عيد، الحماية الجنائية الموضوعية للمعلومات عبر شبكة الإنترنت، دار النهضة العربية، القاهرة، 2013.

6- رشيدة بوبكر، جرائم الاعتداء على نظام المعالجة الآلية في التشريع الجزائري المقارن، ط1، منشورات الحلبي الحقوقية، بيروت، لبنان، 2012.

7- سهيل محمد العزام، الوجيز في الجرائم الإنترنت ، الطبعة الأولى، دائرة مكتبة الجامعة الأردنية، 2009.

8- شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2007.

9- صليحة علي صداقة، الأبعاد القانوني والأخلاقي للمعلوماتية الصحية، دار المطبوعات الجامعية، الإسكندرية، 2017.

10- طارق إبراهيم الدسوفي، الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة، مصر، 2006.

11- طارق طه، مقدمة في نظم المعلومات الإدارية والحاسبات الآلية، الطبعة الثالثة، منشأة المعارف الإسكندرية، 2000.
12- طارق محمد الجملي، الدليل الرقمي في مجال الإثبات الجنائي، ورقة عمل مقدمة للمؤتمر المغاربي الأول حو المعلوماتية المنعقد في 28- 2009/10/29 لأكاديمية الدراسات العليا طرابلس.
13- عامر محمود الكسواني، التجارة عبر الحاسوب، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2008.
14- عبد الفتاح بيومي حجازي، مكافحة جرائم الكومبيوتر والإنترنت في القانون العربي النموذجي، ط1، دار النهضة العربية، الإسكندرية، 2009.
15- عبد الصبور عبد القوي على مصدي، الجريمة الالكترونية، دار العلوم للنشر والتوزيع، ط 1، 2008.
16- علي حسن محمد الطوابلة: التفتيش الجنائي على نظم الحاسوب والإنترنت، عالم الكتب الحديثة، الأردن.
17- علي صادق أبوهيف، القانون الدولي العام، الطبعة السابعة، منشأة المعارف الإسكندرية، 1965.
18- عمر وعيسى الفقي، الجرائم المعلوماتية، جرائم الحاسب الآلي والإنترنت في مصر والدول العربية، المكتب الجامعي الحديث.
19- فتوح الشادلي وعفيفي كامل عفيفي، جرائم الكومبيوتر، منشورات الحلبي الحقوقية، بيروت، لبنان، 2003.
20- فريد منعم جبور، حماية المستهلك عبر الإنترنت ومكافحة الجرائم المعلوماتية (دراسة مقارنة)، ط1، منشورات الحلبي الحقوقية، بيروت، لبنان، 2010.
21- محمد خليفة، الحماية الجنائية برامج الكمبيوتر، دار الهدى للطباعة والنشر، عين مليلة، الجزائر، 2010.

22- محمد عبد الرحيم سلطان العلماء: جرائم الانترنت والاحتساب عليها، بحوث مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، المجلد الثالث، ط3، 2004.

23- محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت دراسة مقارنة، ط2، دار النهضة العربية، القاهرة، 2009.

24- محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، الإسكندرية، 2004.

25- محمد محمود المكاوي، الجوانب الأخلاقية والاجتماعية والمهنية للحماية من الجرائم المعلوماتية (جرائم الكمبيوتر والإنترنت)، الطبعة الأولى، المكتبة العصرية للنشر والتوزيع ، مصر، 2010.

26- محمد مرهج الهيثي، جرائم الحاسوب، ط1، دار المنهج للنشر والتوزيع، عمان، الأردن، 2006.

27- محمد منير الجنيهي، ممدوح محمد الجنيهي، امن المعلومات الالكترونية ، دار الفكر الجامعي الإسكندرية، 2005.

28- نسرين عبد الحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف الإسكندرية، 2008.

29- هلالي عبد الله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، ط2، دار النهضة العربية، 2008.

2- الرسائل الجامعية:

1- أحمد مسعود مريم، رسالة ماجستير: آليات مكافحة جرائم تكنولوجيا الإعلام والاتصال في ضوء القانون 09-04، جامعة قاصدي مرباح، ورقلة، 2013/2012.

2- سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير في العلوم الجنائية، جامعة الحاج لخضر، باتنة، السنة الجامعية 2012-2013.

2/ المراجع الأجنبية:

1- Guillaume Champy, la fraude informatique, tome 1, presse universitaires d'Aix-Marseille, 1992.
2- Hadjira Bouder : orientation de la politique pénale de prévention et de lutte contre la criminalité liées au TIC en Algérie, centre de recherche sur l'information scientifique et technique, CERIST 03, www.alexalaw.com, 01/05/2014, 22h 43.
3- Hollande Alain ..Linant de Bellefont xavier, pratique du droit de l'informatique, edition Delmas (5 edition avril 2002, (France).
4- Lucas André, Jean Devreze, Jean Frayssinet, Droit de l'informatique et l'internet, collection themis (droit privé), 2001, (France).
5- Marise CREMONA JONATHAN HERRING, criminal law, ibid.
6- Valérie SEDALLIAN; Légiférer sur la sécurité informatique: la quadrature du cercle? 5décembre 2003.

3/ القوانين والاتفاقيات

أ- القوانين:

1- قانون الأونيسترال كان بموجب القرار الذي اتخذته الجمعية العامة للأمم المتحدة بناء على تقرير اللجنة السادسة (A/51). 628.
2-القانون رقم 575/2004 لجوان 2004 المتعلق بالثقة في الاقتصاد المعلوماتي، الميمم في 11 جويلية 2010 الفصل الثاني من الباب الأول تحت عنوان "حرية الاتصال في الشبكة" الفصل الثاني من الباب الثالث من هذا القانون.

3-القانون رقم 17/78 المؤرخ في 16 جانفي 1978 المتعلق بالحريات والمعلوماتية المعدل بموجب القانون رقم 2004/801 المؤرخ في 6 أوت 2004 الخاص بالمعالجة الآلية للمعلومات الرقمية.

ب/ الاتفاقيات:

1- المادة الأولى من الفصل الأول – المصطلحات- من اتفاقية بودابست .

2- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2012 عن الموقع الإلكتروني: http://www.lawjo.net/vb/showthread/php?26439

4/ القواميس:

1- القاموس القانوني الثلاثي، قاموس قانوني موسوعي، شامل ومفصل عربي – فرنسي–انجليزي، موريس نخلة وآخرون، منشورات الحلبي الحقوقية، سوريا، 1992.

5/ المواقع الإلكترونية:

1- http://www.droit.com/forum/Showthread.php?t=5955

2- http://www.mprog.org/coom p1.htm.

3- http://www.vercon.sci.eg/Matrials/14.html .

4- http://www.mproug.org/Ccom pL htm

5- http://www.lebarmy.gov.lb/article.asp?ln=ar&id=27286

فهرس المحتويات

فهرس المحتويات

فهرس المحتويات

ملخص

ملخص:

يتلاءم موضوع هذه الدراسة مع التطورات الحديثة الحاصلة في مجال المعلوماتية التي أصبحت تشكل أداة ارتكاب الجريمة مجالا لها، وذلك بإساءة استخدامها واستعمالها على نحو غير مشروع وقد سميت من خلالها، هذه الدراسة إلى الجانب الإطار المفاهيمي في فصله الأول وإطاره القانوني في فصله الثاني ومن خلال تحديد مفهوم المعلوماتية كشرط مفترض لقيامها، والتي تبين أنها تقوم أساسا على العلاقة بين المعلومات والتقنية الحديثة التي تستخدم في معالجة هذه المعلومات، لذلك كان من اللازم تعريف المعلومات وتوضيح خصائصها، وتناولنا أيضا أهم التعريفات الذي صاغها الفقه الجنائي للجريمة المعلوماتية وكذا الطبيعة القانونية الخاصة التي تميز هذه الجريمة من غيرها من الجرائم التقليدية، وكذا الخصائص التي يتميز بها المجرم المعلوماتي وأهم الطرائق والأصناف التي تنتمي إليها هذه الفئة من المجرمين، وما هي الأساليب والتقنيات المستعملة في ارتكاب الجريمة المعلوماتية وكذا الدوافع المحركة للمجرم المعلوماتي لارتكاب هذه الجريمة المعلوماتية وفي الأخير الجزاءات والعقوبات المقررة لجرائم الاعتداء الماسة للأنظمة المعلوماتية.

وفي الخاتمة تم تبيان أهم النتائج التي تم التوصل إليها ووضع بعض التوصيات والاعترافات التي من شأنها تفعيل وتنظيم الإجراءات المناسبة للتحقيق في الجرائم المعلوماتية.