الجرائم المعلوماتية واقعها في الجزائر واليات مكافحتها

أ/مزيود سليم – جامعة المدية

ملخص :

أدى زيادة اعتماد العالم اليوم على تكنولوجيا المعلومات في مختلف معاملاته اليومية وهذا في ظل المزايا التي وفرتها من اقتصاد للوقت، و خفض للتكلفة، وزيادة الأرباح لمنظمات الأعمال ؛ أفرزت له بالمقابل تحديا غير تقليدي وهو نوع جديد من الجرائم تستغل الوسائط الالكترونية التي تستعملها تكنولوجيا المعلومات والتي اصطلح على تسميتها بالجريمة المعلوماتية.

الكلمات المفتاحية: تكنولوجيا المعلومات والاتصال،الانترنت، جرائم الانترنت.

Abstract :

Resulted in increased adoption of today's world of information technology in various transactions daily and this in light of the advantages provided by the economy of the time, and reduce cost, increase profits for business organizations; produced his return challenge funky a new type of crimes exploiting electronic media used by information technology, which termed cybercrime crime.

Keywords : Information and communication technology, Internet, Internet crimes.

مدخل :

يشهد العالم الحالي منذ نهاية القرن العشرين وبداية القرن الحالي تغيرات واسعة النطاق، وذلك نتيجة التطورات الهائلة في مجال تكنولوجيا المعلومات وتكنولوجيا الإتصال والتي انعكست على كافة نواحي الحياة وقطاعاتها المختلفة بما فيها القطاع المالي والمصرفي.

ومع إتجاه المؤسسات إلى زيادة الإستثمار في التكنولوجيا وهذا لزيادة أرباحها من جهة والبيئة الأكثر التنافسية التي أصبحت تعيشها من جهة أخرى؛ خلفت أثرا سلبيا من خلال تعاظم تقديم الخدمات من خلال شبكة الإنترنت والتي اصطلح على تسميتها بالجريمة المعلوماتية.

لم تأمن المنطقة العربية بصفة عامة والجزائر بصفة خاصة من ظاهرة الجرائم المعلوماتية ففي ظل ازدياد عدد المتعاملين مع شبكة الانترنت ، ومع تنامي التعامل التجارة الالكترونية في الدول العربية واعتماد وسائل الدفع الحديثة بدأت تنمو هذه الظاهرة خاصة في ظل تأخر الآليات القانونية والبشرية والفنية في الدول العربية مقارنة بغيرها من دول العالم وهو ما سنحاول الوقوف عليه في هذه الورقة البحثية من خلال تناول العناصر التالية :

المحور الأول : مفهوم الجريمة المعلوماتية وصورها

المحور الثاني: تحديات الجرائم المعلوماتية

المحور الثالث : واقع الجرائم المعلوماتية وأثارها على مستوى العالم

المحور الرابع: واقع الجريمة المعلوماتية في الجزائر

المحور الخامس: اليات واتجاه مكافحة الجريمة المعلوماتية في الجزائر

المحور الأول : مفهوم الجريمة المعلوماتية وخصائصها.

1. مفهوم الجريمة المعلوماتية

لا تختلف الجرائم المعلوماتية في طبيعتها عن الجرائم التقليدية إلا أنها تعتمد على التقنيات الحديثة في استعمالها وفيما يلي مفهومها وخصائصها.

تعرف الجريمة عموما في نطاق القانون الجنائي بأنه سلوك الفرد عملا كان أو امتناعا يواجهه المجتمع بتطبيق عقوبة جنائية، أما المعلوماتية فهي مشتق من المعلومات والتي يعنى بها:

كل فعل أو امتناع عمدي ينشأ عن الإستخدام غير المشروع لتقنية المعلوماتية ويهدف إلى الإعتداء على الأموال المادية أو المعنوية[1].

وتعرف أيضا على أنها فعل أو امتناع عمدي ينشأ عن نشاط غير مشروع لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة في الحاسب ، أو التي تحوَل عن طريقه[2].

وقد عرفت منظمة التنمية و التعاون الاقتصادي **OCDE** الجريمة المعلوماتية على أنها : كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجاً بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية[3].

ويعد هذا التعريف أوضح تعريف أكثر شمولا مما سبق وهذا لمراعاة الإعتبارات التالية :

- تلاؤم هذا التعريف مع فكرة عالمية المعلومات والاتصالات، إذ انه تعريف مقبول ومفهوم على المستوى العالمي؛
- مراعاة التعريف للتطور المتلاحق لتكنولوجيا الحسابات الآلية بصفة خاصة، بحيث لا يقتصر على التكنولوجيا الراهنة، بل يسمح بإستيعاب ما قد يجد من صور للجريمة المعلوماتية نتيجة تطور المعلومات؛
- وأخيرا لما كانت الجريمة المعلوماتية يمكن أن تنطوي على أشكال مختلفة للسلوك الإجرامي فيجب أن يوضح التعريف خصوصية الجريمة المعلوماتية بحيث يبدو واضحا الدور الذي يقوم به الحساب الآلي والمعلومات في ارتكاب الجريمة.

2. خصائص الجريمة المعلوماتية.

تتميز الجريمة المعلوماتية بطبيعة خاصة تميزها عن غيرها من الجرائم التقليدية وذلك نتيجة لإرتباطها بتقنية المعلومات والحاسب الآلي مع ما يتمتع به من تقنية عالية وقد كان لظهور شبكة الإنترنت في إضفاء شكل جديد للجريمة المعلوماتية هو الطبيعة الدولية أو متعددة الحدود.

1.2. خصائص تشترك فيها مع بعض الجرائم.

أ- خطورة الجرائم المعلوماتية.

وذلك لمساسها بالإنسان في فكره وحياته، وتمس المؤسسات في اقتصادها والبلاد في أمنها القومي والسياسي والإقتصادي، ومن شأن ذلك أن يضفي أبعادا خطيرة غير مسبوقة على حجم الإضرار والخسائر التي تنجم عن ارتكاب هذه الجرائم على مختلف القطاعات والمعاملات.

ب- الطبيعة المتعدية الحدود.

من أهم خصائص التي تميز الجريمة المعلوماتية هي تخطيها للحدود الجغرافية ومن إكتسابها طبيعة متعددة الحدود ، فبعد ظهور شبكات المعلومات لم تعد الحدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالقدرة التي تتمتع بها الحاسبات الآلية في نقل وتبادل كميات كبيرة من المعلومات بين أنظمة يفصل بينها ألاف الأميال، قد أدت إلى نتيجة مؤداها إن أماكن متعددة من دول مختلفة قد تتأثر بالجريمة المعلوماتية وحجم المعلومات والأموال المستهدفة والمسافة التي قد تفصل الجاني عن هذه المعلومات والأموال.

وقد أثارت الطبيعة الدولية للجرائم المعلوماتية تساؤلا مهما يتعلق بتحديد الدولة التي يختص قضاؤها بملاحقة الجريمة، أم تلك التي أضرت مصالحها نتيجة لهذا التلاعب، كما أثرت هذه الطبيعة أيضا الشكوك حول مدى فاعلية القوانين القائمة في التعامل مع الجريمة المعلوماتية وبصفة خاص فيما يتعلق بجمع وقبول الأدلة.

2.2.خصائص تنفرد بها الجريمة المعلوماتية عن الجرائم الأخرى.

تختلف الجريمة المعلوماتية عن باقي أنواع الجرائم في :

أ- تتطلب لإرتكابها وجود كمبيوتر ومعرفة تقنية بإستخدامها.

حيث يعتبر الإستعانة بجهاز الكمبيوتر أساسا لإرتكاب الجريمة المعلوماتية وليس سرقة الجهاز أو إتلافه لأنه يدخل في نطاق الإعتداء أو سرقة الأموال المادية المنقولة، وترتكب الجريمة بتدمير برامج الكمبيوتر أو سرقتها أو العبث بالبيانات أو المعلومات المخزنة[4].

كما تعتمد هذه الجرائم على قمة الذكاء في ارتكابها ويصعب على المحقق التقليدي التعامل مع هذه الجرائم، إذ يصعب عليه متابعة الجرائم المعلوماتية والكشف عنها وإقامة الدليل عليها، فهي جرائم تتسم بالغموض وإثباتها بالصعوبة بمكان والتحقيق فيها يختلف عن التحقيق في الجرائم التقليدية، كما انه كلما تقدمت المعرفة التقنية كلما زادت احتمالية توظيف هذه المعارف بشكل غير مشروع وزيادة خطورة الجرائم المعلوماتية.

ب- صعوبة اكتشافها وإثباتها.

تتسم الجريمة المعلوماتية بأنها لا تترك أثرا بعد إرتكابها علاوة على صعوبة الإحتفاظ الفني بآثارها إن وجدت[5] ، فليس هناك أموال مادية منقولة تم إختلاسها وإنما هي أرقام تتغير في

السجلات، كما أن معظم الجرائم المعلوماتية تم اكتشافها بالمصادفة وبعد مرور وقت طويل إضافة انه لا يتم في الغالب الإبلاغ عن الجرائم المعلوماتية أما لعدم اكتشافها من طرف الضحية أو خوفا من التشهير به لذلك ما يرتكب فعلا من جرائم معلوماتية اكبر بكثير ما يصرح به.

ت– تميز مرتكب الجريمة المعلوماتية عن غيره من مرتكبي الجرائم الأخرى :

يتصف مرتكبوا الجرائم المعلوماتية بعدة صفات تميزهم عن غيرهم من المتورطين في أشكال الإجرام الأخرى والمتمثلة في:

– **المهارة:** المتطلبة لتنفيذ النشاط الإجرامي من ابرز خصائص المجرم المعلوماتي والتي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال، أو عن طريق الخبرة المكتسبة في مجال تكنولوجي المعلومات،أو بمجرد التفاعل الإجتماعي مع الآخرين. إلا أن ذلك لا يعني ضرورة أن يكون المجرم المعلوماتي على قدر كبير من العلم في هذا المجال، بل إن الواقع العملي قد اثبت أن بعض انجح مجرمي المعلوماتية لم يتلقوا المهارة اللازمة لإرتكاب الجريمة عن طرقي التعليم أو الخبرة المكتسبة من العمل في هذا المجال.

– **المعرفة:** فتتلخص في التعرف على كافة الظروف التي تحيط بالجريمة المراد تنفيذها وإمكانيات نجاحها واحتمالات فشلها، إذ أن المجرم المعلوماتي بإستطاعته أن يكون تصورا كاملا لجريمته، كون المشرح الذي تمارس فيه الجريمة المعلوماتية هو نظام الحاسب الآلي فالفاعل يستطيع أن يطبق جريمته على أنظمة مماثلة لتلك التي يستهدفها وذلك قبل تنفيذ جريمته.

– **الوسيلة:** فيراد بها الإمكانيات التي يتزود بها الفاعل لإتمام جريمته ففيما يتعلق بالمجرم المعلوماتي فإن الوسائل المتطلبة للتلاعب بأنظمة الحسابات الآلية هي في أغلب الحالات تتميز نسبيا بالبساطة وبسهولة الحصول عليها.

– **السلطة:** فيقصد بها الحقوق أو المزايا التي يتمتع بها المجرم المعلوماتي والتي تمكنه من ارتكاب جريمته، قد تتمثل هذه السلطة في الشفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات والتي تعطى الفاعل مزايا متعددة كفتح الملفات ومحو أو تعديل المعلومات التي تحتويها أو مجرد قراءتها أو كتابتها، وقد تمثل هذه السلطة في الحق في استعمال الحاسب الآلي أو إجراء بعض التعاملات، وقد تكون هذه السلطة غير حقيقية كما في حالة استخدام شفرة الدخول الخاصة بشخص آخر.

– **الباعث:** وراء ارتكاب الجريمة، الذي قد لا تختلف في كثير من الأحيان عن الباعث لإرتكاب غيرها من الجرائم الأخرى، فالرغبة في تحقيق الربح المادي بطريق غير مشروع يظل الباعث الأول وراء ارتكاب الجريمة المعلوماتية، ثم يأتي بعد ذلك الرغبة في قهر نظام الحاسب وتخطي حواجز الحماية المضروبة حوله، وأخيرا الانتقام من رب العمل أو احد الزملاء، حيث يفرق مرتكبي هذه الجرائم بين الإضرار بالأشخاص والأضرار بين بمؤسسة أو جهة في استطاعتها اقتصاديا تحمل نتاج أعمالهم.

3. مرتكبوا الجرائم المعلوماتية.

يمكن تصنيف مرتكبوا الجرائم المعلوماتية إلى الطوائف التالية[6]:

أ- المازحون Prankesters : الأشخاص الذين يرتكبون جرائم المعلوماتية بغرض التسلية والمزاح مع الآخرين بدون أن يكون في نيتهم إحداث أي ضرر بالمجني عليهم، ويتدرج تحت هذه الطائفة بصفة خاصة صغار مجرمي المعلوماتية.

ب- قراصنة الانترنت Hackers : فهي تضم الأشخاص الذين يهدفون إلى الدخول إلى أنظمة الحسابات الآلية غير المصرح لهم وكسر الحواجز الأمنية الموضوعة لهذا الغرض، وذلك بهدف إكتساب الخبرة ،أو بدافع الفضول أو بمجرد إثبات القدرة على اختراق هذه الأنظمة.

ت- القراصنة المجرمون Malicious hackers : هدفهم إلحاق خسائر بالمجني عليهم دون أن يكون الحصول على مكتسب مالية من ضمن هذه الأهداف، ويندرج تحت هذه الطائفة الكثيرون من مخترقي فيروسات الحاسبات الآلية وموزعيها.

ث- المنتقمون Personnel Problem solvers : فهم الطائفة الأكثر شيوعا بين مجرمي المعلوماتية، فهم يقومون بإرتكاب جرائم المعلوماتية التي تلحق بالمجنى عليهم خسائر ولا يستطيع حلها بالوسائل الأخرى بما فيها اللجوء إلى الجريمة التقليدية.

ج- ممتهنوا الإجرام Career criminals : وهم مجرمي المعلوماتية الذين يبتغون تحقيق الربح المادي بطريقة غير مشروعة بحيث ينطبق على أفعالهم الجريمة المنظمة،ا وعلى الأقل يشترك في تنفيذ النشاط الإجرامي أكثر من فاعل ،ويقترب المجرم المعلوماتي المنتمي إلى هذه الطائفة في سماته من المجرم التقليدي.

ح- المتطرفون Extreme advocates: فتدخل في عداداها الجماعات الإرهابية أو المتطرفة، والتي تكون بدورها من مجموعة من الأشخاص لديهم معتقدات وأفكار اجتماعية أو سياسية أو دينية ويرغبون في فرض هذه المعتقدات باللجوء أحيانا إلى النشاط الإجرامي،ويركز نشاكهم بصفة عامة في استخدام العنف ضد الأشخاص والممتلكات من اجل لفت الأنظار إلى ما يدعون إليه، وان اعتماد المؤسسة المختلفة داخل الدول على أنظمة الحسابات الآلية في انجاز أعمالها والأهمية القصوى للمعلومات التي تحتويها في اغلب الحالات قد جعل من هذه الأنظمة هدفا جذابا لهذه الجماعات.

خ- الإهمال **The criminality negligent** : و التي تضم واحدة من أهم المشكلات التي تتصل بإساءة استخدام الحسابات الآلية، ألا وهي الإهمال الذي يترتب عليه في مجال الحاسبات الآلية وفي اغلب الأحيان نتائج خطيرة قد تصل إلى حد القتل.

المحور الثاني: تحديات مكافحة جرائم المعلوماتية.

تكمن مخاطر الجريمة المعلوماتية مقارنة مع الجرائم العادية في التحديات التي تفرضها والمتعلقة بالآليات المناسبة لمكافحتها في ظل طبيعتها التي تعتمد على الانترنت وفيما يلي أهم هذه التحديات (13) (07).

أ- التحديات العامة.

وتتمثل في :

1. **الثقة في وسائل تكنولوجيا المعلومات والإتصال:** الذي يتجلى من خلال الإتصالات المستخدمة من خلال شبكة الإنترنت، والإعتماد الكبير عليها في كثير من الصناعات والخدمات، بشكل أصبحت مندمجة بشكل كلي في كل مظاهر الحياة.وقد أدت زيادة هذه الثقة في استخدام تكنولوجيا المعلومات والإتصال إلى مخاطر تعريض الأنظمة والخدمة إلى التخريب أو القرصنة.
2. **عدد مستخدمي تكنولوجيا المعلومات والاتصال:** في ضوء انتشار الإنترنت واستخدامها على مستوى العالم والذي قارب 2 مليار مستخدم سنة 2009، ومع زيادة عدد المستخدمين من سنة إلى أخرى ازداد عدد المستهدفين، خاصة في ظل صعوبة تحديد عدد مستخدمي الإنترنت بطريقة غير شرعية.
3. **توفر الأجهزة وسهولة الدخول:** والتي أصبح من خلالها عملية إجراء بريد الكتروني يستغرق وقت قصير فقط وهذا سبب نجاح الإنترنت، والتي لا بد أن يقابله وقت القصير للتحقيق أو جمع الأدلة، تختلف مع التحقيقات التقليدية التي تأخذ وقت أطول.
4. **التطور المستمر:** تتصف الإنترنت بأنها تخضع للتطور بإستمرار، ويتجلى هذا من خلال التطبيقات الجديدة التي تعرضها والتي مكنت من إنشاء جرائم جديدة .
5. **الإتصالات المجهولة:** إن طبيعة الخدمات التي تتم من خلال شبكة الانترنت والتي لا يتم التحقق من المعلومات الشخصية التي يجب إدراجها إما كخاصية عرضية للخدمة أو متعمدة لإخفاء طبيعة المستخدم، يمكن للمعتدين من إخفاء هوياتهم وإستخدام هويات وهمية، وكمثال على ذلك البريد الإلكتروني المجهول الذي يفيد المستخدم في خضوعه في نقاشات سياسية وفكرية، كما أنها قد تثير السلوكات ضد المجتمع لكنها تساعد من العمل بحرية أكثر.
6. **أنها تكنولوجيا التشفير:** إضافة إلى العوامل السابقة هناك عامل آخر قد يعقد من عملية التحقيق في الجرائم المعلوماتية وهو تكنولوجيا التشفير، والتي تحمي معلومات ضد أي شخص يريد الولوج أو الدخول وهذا من خلال كلمة سر، إضافة إلى البرامج تسمح للمستخدم من حماية الملفات ضد الدخول غير المسموح والتي تكون في الغالب تكون صعبة وتأخذ وقت طويل للإختراق إذا استطاع

المحققين من الدخول إلى البرنامج المستخدم في التشفير. والتي هي عبارة عن حل لمواجهة جرائم الإنترنت.

7. توفر المعلومات: تتوفر شبكة الانترنت على ملايين من واجهات الإنترنت والآنية حيث بإمكان أي شخص المساهمة والمشاركة في الشبكة، ويعد النجاح الكبير الذي شهدته الإنترنت إلى قوة محركات البحث التي تمكن من البحث في ملايين في صفحات الانترنت في ثواني، وقد ساعدت هذه الخاصية المعتدين أو المهاجمين في تنفيذ اعتدائهم من خلال المعلومات المتاحة على شبكة الانترنت وهذا بتوضيح طريق الاختراق مثلا.

8. غياب آليات الرقابة: تحتاج كل شبكات الإتصال والشبكات إلى إدارة مركزية وأدوات تقنية وهذا لضمان العملياتية، وهذا مالا يوجد على شبكة الانترنت حيث غياب أدوات الرقابة على شبكة الإنترنت تمكن المستخدم من التحايل بإستخادم شبكة الإتصال المجهولة.

9. لها خاصية البعد الدولي: بحيث يتم تبادل المعلومات من خلال الشبكة المعلومات على صعيد أكثر من بلد كما أن العديد من مزودي الخدمة عادة ما يكون خارج البلد الأصل، وكون المعتدين من بلدان مختلفة يفرض ضرورة تعاون كبير في عمليات التحقيق بين كل الهيآت القانونية والى مساندة كل السلطات في كل البلدان المشاركة، التي تواجه بالشروط الشكلية والوقت اللازم للتعامل مع قوانين الأجنبية.كما تؤدي عملية حذف البيانات المهمة لتعقب جرائم الانترنت معضلة بالنسبة لعملية التحقيق.

10. استقلالية المكان والحضور في موقع الجريمة: لا يحتاج مجرموا الإنترنت إلى التواجد في نفس الموقع المستهدف، حيث أن مكان المجرم يختلف في الغالب عن موقع الجريمة، كما أنها لا تكلف جهد ووقت كبير، إضافة إلى أنهم يتفادون الدول ذات التشريعات القوية في مكافحة جرائم الانترنت.

ب– التحديات التشريعية.

والمتمثلة في :

1. تحديات تحيين قوانين العقوبات: مع الأشكال الجديدة للجرائم التي أفرزتها روابط الحاسوب أو روابط شبكة الانترنت ، جرائم الانترنت برز تحدي أمام المشرعين بالإستجابة للتطورات الحاصلة في الانترنت وان يضمنوا فعالية وجود احتياطات خاصة الحاصلة في ظل التطور السريع في تكنولوجيا الشبكة. خاصة فيما يتعلق بتحيين قانون العقوبات لمتابعة الأشكال الجديدة من الجرائم المعلوماتية،حيث أن بعض البلدان لم تنتهي بعد من تعديل إجراءات مخالفات التي يقوم بها الجناة تحت القانون العقوبات.

فالتحدي الأساسي للأنظمة التشريعية العقابية هي فترة التأخير بين إدراك مخاطر سوء استعمال تكنولوجيا المعلومات من جهة ومتطلبات القانون التشريع المحلية وهذه التحديات تبقى مناسبة ومرتبطة بالموضوع دائما مع التطور الحاصل في تكنولوجيا الإنترنت، لذا فإن كثيرا من الدول تبذل مجهودا للتعامل مع تكنولوجيا المعلومات.

2. بروز جرائم جديدة: بالرغم من أن اغلب الجرائم المعلوماتية تشبه الجرائم التقليدية إلا في الأداة وهي استخدام تكنولوجيا المعلومات والاتصال وبالتالي فإن قانون الخاص لمكافحتها لا يختلف كثيرا قانون عن الجرائم التقليدية، إلا انه ظهرت بعض الأنواع الجديدة من الجرائم كالجرائم الاحتيال المالي وسرقة البيانات من خلال ممارسة الألعاب (online games) على الانترنت.

3. إستعمال تكنولوجيا المعلومات والإتصال والحاجة إلى أدوات تحقيق جديدة: يستعمل المهاجمين تكنولوجيات المعلومات والاتصال بطرق مختلفة لتحضير وتنفيذ مختلف اعتداءاتهم، لذا فإن الهيآت تحتاج أدوات مناسبة لتحقيق في جرائم الإنترنت في تطبيقها للقانون ، ذلك أن البعض منها تتناقض مع حق الإستعمال المشروع للإنترنت.

4.إقامة إجراءات الإثبات الرقمية: مع ارتفاع عدد الملفات الرقمية في ظل انخفاض تكلفتها و التطور في استعمال الرقمنة أصبحت كدليل جديد للمعلومات تستعمل في المحاكم وهذا بإستعمال تكنولوجيات المعلومات والاتصال في جمعها ومعالجتها واستعمالها كدليل، ومعالجة الأدلة الرقمية تعترضها تحدي واحد وهو الإجراءات الخاصة بها، وتعد عملية صيانة الأدلة الرقمية أكثر المظاهر تحدي للأدلة الرقمية،حيث أن الأدلة الرقمية تعد أدلة هشة وقابلة للتغيير أو الحذف.

وتعد الأدلة الرقمية أساسية في أي عملية تحقيق حول الجرائم المعلوماتية والتي يمكن تقسيم مراحلها إلى أربعة مراحل:

- الكشف عن الأدلة الوثيقة الصلة؛
- تجميع وحفظ الأدلة؛
- تحليل تكنولوجيا الإعلام الآلي والأدلة الرقمية؛
- تقديم الأدلة للعدالة.

المحور الثالث:واقع الجريمة المعلوماتية في العالم و أثارها.

تعد جرائم الانترنت احد مساوئ تطبيق تكنولوجيا المعلومات والإتصال حيث قدرت حجم خسائر جرائم الإنترنت في دراسة قام بها المركز الاستراتيجي والدراسات الدولية وشركة Mcafee بـ 500 مليار دولار في نهاية عام2012، مما يهدد صناعة التكنولوجيا في ميدان الأعمال للتفوق على ذلك على الخسائر من الاتجار بالمخدرات والمقدرة 274 مليار دولار [08].

وطبقا لمؤشرات Symantec لسنة 2012 فقد القطاع المالي يأتي في المرتبة الأولى من عمليات التصيد من خلال مواقع وهمية بنسبة 87 % تليها مواقع الأعمال بنسبة 12% ثم المواقع الحكومية بنسبة 3 %[09]. .

كما انه وفق الدراسة فإنه في كل ثانية يتعرض 18 شخص الى جريمة معلوماتية وقد بلغ عدد الافراد الذي تعرضوا الى الجرائم المعلوماتية 556 مليون شخص خلال 12 شهر الأخير.

هذا وقد بلغت حجم الخسائر المتعلقة فقط بالاحتيال على الزبائن من خلال العمليات الوهمية 21 مليار دولار في الولايات المتحدة الامريكية، 16 مليار دولار في أوربا، 465 مليار دولار في الصين ،8 مليار دولار في الهند، 2 مليار دولار في الهند.[10].

أما في الدول العربية فقد قدرت خسائر جرائم الانترنت بـ 600 مليون دولار بلغ حجم الخسائر المترتبة عن الجرائم المعلوماتية وفي الإمارات بقيمة 284 مليون دولار وبعدد 1.5 مليون شخص ضحية للجرائم،وفي السعودية بلغت خسائر البنوك السعودية من جرائم الانترنت بـ 2 مليار دولار[11].

رابعا:واقع الجريمة المعلوماتية في الجزائر وواقع مكافحتها في الجزائر.

بدأت تظهر ظاهرة الجريمة المعلوماتية في الجزائر إلى سنة 2005 أين سجلت ظاهرة واحدة فقط ومع تزايد انتشار الانترنت في الجزائر حيث وصل عدد المشتركين فيها إلى واتجاه إلى استعمال تكنولوجيا الاتصال بدأت ترتفع حجم الظاهرة حيث سجلت سنة 2009 88 شخصا متهما تتعلق بالجريمة المعلوماتية وتؤكد معطيات أمام ملتقى دولي حول الجريمة المعلوماتية أن هذا النوع من الجرائم لم ينتشر على نطاق واسع في الجزائر غير انه اخذ في التقدم وان المخالفات المسجلة تتعلق بالاطلاع غير الشرعي على البيانات قصد إتلافها والقرصنة ضد المواقع الرسمية والخاصة والدعاية المغرضة والإرهاب وسرقة المعلومات والتعدي على الحياة الشخصية وتستهدف الجريمة المعلوماتية 60% منها تستهدف الإدارات العامة والمؤسسات الصناعية ونسبة 20% الشركات الخاصة و11%الشركات الأجنبية و 6 الأشخاص.

المحور الخامس: آليات واتجاه مكافحة الجريمة المعلوماتية في الجزائر

لم تعرف الجزائر قوانين قبل 2004 تطبق بشكل خاص على نظام المعلوماتية أو على تكنولوجيات الإعلام والاتصال، ما عدا شبكة الاتصالات السلكية واللاسلكية ووسائل الإعلام السمعية.

ومراعاة لما شهدته الجزائر ويشهده العالم في الفترة الأخيرة وخاصة مع بداية الألفية الثالثة من تطورا كبيرا في مجال تكنولوجيات الإعلام و الاتصال التي تقوم بشكل اكبر على الاختراعات الجديدة

في مجال الإلكترونيك والمعلوماتية ،ولمسايرة هذا التطور التكنولوجي كان لابد للدول من إيجاد الإطار القانوني المناسب بوضع النصوص الملائمة المختلفة استعمالات الإعلام الآلي وفي نفس السياق وضع قوانين خاصة لمواجهة ما يسمى بالإجرام المعلوماتي أو الجرائم الالكترونية.

وقد تجسد ذلك في الجزائر بصدور القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون العقوبات الذي نص على حماية جزائرية للأنظمة المعلوماتية من خلال تجريم كل أنواع الاعتداءات التي تستهدف أنظمة المعالجة الآلية للمعطيات.

1. أسباب استصدار قانون مكافحة الجرائم المعلوماتية [12]

إن الثورة في مجال تكنولوجيا الإعلام والاتصال أدت بالجزائر إلى محاولة الاقتداء بأغلب دول العالم في هذا المجال.

كان لزاما سد فراغ القانوني الذي عرفه هذا المجال بصدور القانون رقم 15.04 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون العقوبات الذي نص على حماية جزائية لأنظمة المعلوماتية من خلال تجريم كل أنواع الاعتداءات التي تستهدف أنظمة المعالجة الآلية للمعطيات ويأتي هذا القانون لتعزيز نفس هذه القواعد ،من خلال وضع إطار قانوني أكثر ملائمة مع خصوصية الجريمة الافتراضية.

كما تكمن أهمية هذا القانون في كونه يجمع بين القواعد الإجرائية المكملة لقانون الإجراءات الجزائية وبين قواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة والتدخل السريع لتحديد مصدرها والتعرف على مرتكبيها.

وقد اخذ المشرع بعين الاعتبار الصعوبات التي تثيرها المصطلحات القانونية المتعلقة بهذه المادة ، لذلك تم اختيار عنونا " القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها" حتى لا يكون النص مرتبطا بتقنيات تشهد تطورا مستمرا بقدر ما يرتبط بالأهداف والغايات التي ترمي إليها هذا التكنولوجيا، كما أن التركيز على مجالي الإعلام والاتصال بين مقاصد النص الذي يهدف إلى جعل المتعاملين في مجال الاتصالات السلكية واللاسلكية شركاء في مكافحة هذا الشكل من الإجرام والوقاية منه.

2. مضمون القانون.

تضمن القانون رقم 09-04 المؤرخ في 5 غشت سنة 2009 مادة مقسمة على ستة فصول نلخصها فيما يلي [19] [13].

نص الفصل الأول على الأحكام العامة التي تبين الأهداف المتوخاة من القانون وتحدد مفهوم مصطلح التقنية الواردة فيه وكذا مجال تطبيق أحكامه، وفي الفصل الثاني نص القانون على مراقبة

الاتصالات الالكترونية حيث خصها بأحكام خاصة بمراقبة الاتصالات الالكترونية، وقد روعي في وضع هذه القواعد خطورة التهديدات المحتملة وأهمية المصالح المحمية.

والفصل الثالث تضمن القواعد الإجرائية، بمعنى النص على قواعد إجرائية خاصة بالتفتيش والحجز في مجال الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ،وذلك وفقا للمعايير العالمية المعمول بها في هذا الشأن ومع مراعاة ما تضمنه قانون الإجراءات الجزائية من مبادئ عامة.أما الفصل الرابع تطرق إلى التزامات المتعاملين في مجال الاتصالات الالكترونية ،وذلك من خلال تحديد الالتزامات التي تقع على عاتق المتعاملين في الاتصالات الالكترونية لاسيما إلزامية حفظ المعطيات المتعلقة ب حركة السير والتي من شأنها المساعدة في الكشف عن الجرائم ومرتكبيها، يهدف هذا القانون إلى إعطاء مقدمي الخدمات دورا ايجابيا ومساعدا للسلطات العمومية في مواجهة الجرائم وكشف مرتكبيها.

والفصل الخامس أشار إلى الهيئة الوطنية للوقاية من الإجرام المتصل بتكنولوجيا الإعلام والاتصال ومكافحته ،إذ نص القانون على إنشاء هيئة وطنية ذات وظيفة تنسيقية في مجال الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته ،وقد تمت الإحالة على التنظيم فيما يخص تحديد كيفيات تنظيم هذه الهيئة. وأخيرا وتعرض الفصل السادس على التعاون والمساعدة القضائية الدولية،إذ تناول قواعد الاختصاص القضائي والتعاون الدولي بوجه عام.

الخاتمة:

أدى التطور الهائل في تكنولوجيا المعلومات والإتصال وزيادة الترابط الإلكتروني والإعتمادية المتزايدة على التقنية إلى ظهور نوع جديد من المعاملات تسمى بالمعاملات الإلكترونية تختلف عن المعاملات التقليدية ؛ و بالمقابل أفرزت جرائم مستحدثة تعتمد على الوسائل التي أتاحتها تلك الثورة المعلوماتية خاصة الإنترنت والتي تدعى بجرائم الإنترنت أو جرائم إستخدام الحاسوب التي تتمثل في كل فعل أو إمتناع من شأنه الإعتداء على الأموال المادية أو المعنوية يكون ناتجاً بطريقة مباشرة أو غير مباشرة عن تدخل التقنية،

ويظهر مخاطر الجريمة المعلوماتية في التحديات التي تفرضها لمكافحتها في ظل طبيعتها التي تعتمد على الإنترنت، كالثقة المتزايدة في إستعمال تكنولوجيا المعلومات والاتصال وزيادة عدد مستخدمي شبكة الانترنت، وظهور جرائم جدد ، وإقامة إجراءات الإثبات الرقمية.

ولخطر هذا النوع من الجرائم والمحتمل إن يكون أن يكون كبيرا في ظل ضعف الجاهزية التقنية والتشريعية. قامت العديد من الدول منها الجزائر بإصدار قوانين خاصة أو تعديل قوانينها الجزائية لمواجهة الآثار السلبية التي خلفتها هذه التقنية العالية إضافة إلى الوسائل الفنية وتأهيل كوادر قادرة على التتبع والتحقيق في هذه الظاهرة.

الهوامش :

(1): عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون – دراسة مقارنة – ، منشورات الحلبي الحقوقية ، بيروت، 2003 ، ص 32.

(2): يونس عرب ، موسوعة القانون وتقنية المعلومات ، دليل أمن المعلومات والخصوصية ، جرائم الكمبيوتر والانترنت ، الجزء الأول، منشورات إتحاد المصارف العربية ، الطبعة الأولى،2001، ص 213.

(3) نادلة عادل محمد فريد قورة ، جرائم الحاسب الآلي الاقتصادية دراسة نظرية وتطبيقية، منشورات الحاتي الحقوقية، 2005، ص32.

(4): سميرة معاشي، ماهية الجريمة المعلوماتية، مجلة المنتدى القانوني، العدد السابع ، ص 282.

(05) www.itu.int ,International telecommunication union, understanding cybercrime for developing countries, April 2009. date de consultation : 17/05/2011

(6): جميل عبد الباقي الصغير،القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، الطبعة الأولى،1992، ص17.

(7): نائلة عادل محمد فريد رستم، مرجع سبق ذكره، ص 38.

(8) www.ic3.gov, Internet crime complate center, 2009 internet crime report ,date de consultation, 04/05/2011

(09) http://www.symantec.comdate de consultation, 01/09/2013

(10) www.mcafee.com/,date de consultation, 01/09/2013

(11) www.alwasat.com/,date de consultation, 01/09/2013

(12) احمد عمراني، الأزرق بن عبد الله، نظام المعلوماتية في القانون الجزائري واقع وأفاق، ، المؤتمر السادس لجمعية المكتبات والمعلومات السعودية حول البيئة المعلوماتية الآمنة : المفاهيم والتشريعات والتطبيقات، خلال الفترة 6-7 افريل 2010 ، الرياض، ص 15.

(13) قانون رقم09-04 المؤرخ في 05 أوت 2009 المتعلق بالقواعد الخاصة للوقاية من جرائم المتصلة بتكنولوجيا الإعلام والاتصال والوقاية منها ، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية رقم 47 المؤرخة في 16 أوت 2009، ص 05.