الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة منتوري قسنطينة

كلية العلوم الإنسانية والعلوم الاجتماعية

الرقم التسلسلي:..... قسم علم المكتبـــــــات

الشعبة:.....

رسالة مقدمة لنيل شهادة ماجستير في علم المكتبات تخصص " أنظمة المعلومات وإدارة المعرفة"

واقع شبكات المعلومات في ظل الإدارة الإلكترونية للمعلومات

دراسة حالة شبكة الصندوق الوطني للتقاعد لوكالة ميلة

إعداد الطالبة: تحت إشراف:

سعيدي سليمة د.قموح ناجية

... جوان **2008**...

شكر وتقدير

لك الحمد ربي على ما أنعمت ولك الفضل والمن على ما هديت ولك وحدك الشكر على ما وفقت إن التوفيق منك والهداية ترجع إليك والصلاة والسلام على نبيك ورسولك الكريم وآله وصحابته أجمعين.

أتقدم بخالص شكري لأستاذتي المشرفة "نجية قموح" على ما تحملته معي من مشاق هذا البحث إلى أن وصل إلى صياغته النهائية.

لك الحمد ربي على ما أنعمت ولك الفضل والمن على ما هديت ولك وحدك الشكر على ما وفقت إن التوفيق منك والهداية ترجع إليك والصلاة والسلام على نبيك ورسولك الكريم وآله وصحابته أجمعين.

أتقدم بخالص شكري لأستاذتي المشرفة "نجية قموح" على ما تحملته معي من مشاق هذا البحث إلى أن وصل إلى صياغته النهائية.

قائمة المحتويات

قائمة المحتويات..... 01
قائمة الجداول..... 07
قائمة الأشكال 08
المقدمة 09

الفصل الأول: اجراءات الدراسة

1-1. أساسيات موضوع البحث..... 16
1-1-1. أهمية الموضوع..... 16
1-1-2. أهداف البحث..... 17
1-1-3. إشكالية البحث..... 17
1-1-4. تساؤلات البحث..... 18
1-1-5. فرضيات البحث..... 19
1-1-6. الدراسات السابقة 19
1-2. إجراءات الدراسة الميدانية 21
1-2-1. منهج الدراسة 21
1-2-2. أساليب تجميع البيانات 21
1-2-2-1.إستمارة الاستبانة..... 22
1-2-2-2. المقابلة..... 22
1-2-3. حدود الدراسة الميدانية 22
1-2-3-1. الحدود الجغرافية 22
1-2-3-2. الحدود البشرية 22
1-2-3-3. الحدود الزمنية 23
1-2-4. العينـــــــة..... 23
1-2-4-1. تحديد المجتمع الأصلي للدراسة..... 23
1-2-4-2. اختيار العينة من المجتمع الأصلي 23
1-3. ضبط المصطلحات والمفاهيم..... 24
1-3-1. الهاكرز 24
1-3-2. الكراكرز 25
1-3-3. الجريمة المعلوماتية 25
1-3-4. الفيروسات 29
1-3-5. امن المعلومات 30

الفصل الثاني: الهاكرز أو قراصنة العصر

2-1.المجرم المعلوماتي:الماهية 35

2-1-1. الهــاكرز 35
2-1-1-1. تعريف الهاكرز..... 35
2-1-1-2. تطور الهاكرز 37
2-1-2. الكراكرز..... 39
2-1-2-1. تعريف الكراكرز..... 39
2-1-2-2.الكراكرز المحترفون 39
2-1-2-3. الكراكرز الهواة 39
2-1-3. الفرق بين الهاكرز والكراكرز..... 41
2-1-3-1. أوجه الشبه..... 41
2-1-3-2. أوجه الإختلاف..... 42
2-1-3-3. الفرق بين الهاكرز والمجرم التقليدي
..... 43
2-2. المجرم المعلوماتي :المميزات والتصنيفات 44
2-2-1. أنماط المجرمين المعلوماتيين 44
2-2-1-1.الدخـــــلاء..... 45
2-2-1-2. العابثيــن 47
2-2-1-3. المتسللين 48
2-2-2. مميزات المجرم المعلوماتي 49
2-2-2-1. المجرم المعلوماتي أنسان إجتماعي..... 48
2-2-2-2. المجرم المعلوماتي كإنسان ذكـــــــي..... 49
2-2-3. أسباب الإجرام المعلوماتي..... 51
2-2-3-1. غاية التعلم..... 52
2-2-3-2 تحقيق مكاسب مالية..... 52
2-2-3-3. الإنبهار بالتقنية 54
2-2-3-4. الدوافع الشخصية 54
2-3. منظمات الهاكرز، مؤتمراتهم، تموقعهم الجغرافي 55
2-3-1. منظمات الهاكرز..... 55
2-3-1-1. تعريف منظمات الهاكرز 56
2-3-1-2. أنواع منظمات الهاكرز 56
2-3-2. . مؤتمرات الهاكرز..... 57
2-3-2-1. مؤتمر ديفكون ***DEFCON***..... 58
2-3-2-2. مؤتمر هوب ***HOBE***..... 58
2-3-2-3. مؤتمر سمل كون ***SAMMLE CON***..... 58
2-3-3. جغرافية الهاكرز في العالم..... 58
2-3-3-1. الهاكرز في أمريكا..... 58

2-3-3-2. الهاكرز في أوروبا وآسيا 61
2-3-3-3. الهاكرز في الدول العربية 62

الفصل الثالث: الجريمة الإلكترونية

3-1. الجريمة المعلوماتية: الماهية..... 66
3-1-1. مفهوم الجريمة المعلوماتية 66
3-1-1-1. تعريف الجريمة المعلوماتية..... 66
3-1-1-2. ظهور الجريمة الإلكترونية..... 67
3-1-1-3. مميزات الجريمة الإلكترونية..... 68
3-1-2. الطبيعة القانونية للجريمة الإلكترونية..... 70
3-1-2-1. موضوع الجريمة الإلكترونية..... 70
3-1-2-2. خصوصية الجريمة الإلكترونية..... 71
3-1-2-3. الطبيعة القانونية الجريمة الإلكترونية..... 72
3-1-3. صعوبة الإثبات في الجريمة الإلكترونية..... 73
3-1-3-1. إثبات الجريمة الإلكترونية..... 74
3-1-3-2. المشكلات الإجرائية في الجرائم الحديثة..... 75
3-1-3-3. المعوقات التي تمنع من توقيع العقاب على مرتكبي الجرائم المعلوماتية..... 75
3-2. الجريمة المعلوماتية الأنواع 76
3-2-1. جرائم التعدي على البرمجيات والبيانات..... 76
3-2-1-1. تعريف برامج الحاسب..... 77
3-2-1-2. مفهوم قرصنة البرامج..... 77
3-2-1-3. صور القرصنة الشائعة..... 78
3-2-2. جرائم الأنترنت..... 80
3-2-2-1. تعريف جرائم الأنترنت..... 80
3-2-2-2. خصائص جرائم الأنترنت..... *81*
3-2-2-3. أهم جرائم الأنترنت..... *81*
3-2-3. جرائم الاعتداء على الخصوصية والسرية..... *84*
3-2-3-1. تعريف الحق في الخصوصية..... *84*
3-2-3-2. أثر التقنية على الحياة الخاصة..... *85*
3-2-3-3. أهم جرائم الاعتداء على الخصوصية..... *86*
3-3. . الإختراق..... *89*
3-3-1. ماهية الإختراق..... *89*
3-3-1-1. تعريف الإختراق..... *89*
3-3-1-2. ميكانيكية الاختراق..... *89*
3-3-1-3. أنواع الاختراق..... *92*

3-3-2. آثار الإختراق، أسبابه وطرقه..... 93
3-3-2-1. . آثـــار الإختراق..... 93
3-3-2-2. أسباب الإختراق ودوافعـــه 93
3-3-2-3. طـــــــــرق الاختـــــراق..... 96
3-3-3. برامج الإختراق وبرامج الحماية..... 97
3-3-3-1. تعريف برامج الإختـــــراق..... 97
3-3-3-2. أشهـــــر برامج الإختراق..... 98
3-3-3-3. أشهر برامج الحماية من الإختراق..... 99

الفصل الرابع: الفيروسات

4-1. الفيروسات: الماهيـــــة..... 104
4-1-1. ماذا نعني بالفيروس..... 104
4-1-1-1. ندة تاريخية عن الفيروسات..... 104
4-1-1-2. تعريف الفيروس. 105
4-1-1-3. لماذا سمي بالفيروس..... 106
4-1-2. خصائص الفيروس..... 108
4-1-2-1. القدرة على الاختفاء..... 108
4-1-2-2. الإنتشار..... 108
4-1-2-3. القدرة على الإختراق..... 109
4-1-2-4. القدرة على التدمير..... 109
4-1-3. دورة حياة الفيروسات وانتشارها..... 109
4-1-3-1. دورة حياة الفيروس..... 109
4-1-3-2. عوامل إنتشار الفيروسات..... 111
4-1-3-3. وسائل إنتقال الفيروس..... 111
4-2. أنواع الفيروسات وأشكالها..... 115
4-2-1. أنواع الفيروسات..... 115
4-2-1-1. قطاع التشغيل ***bootseetor*** 115
4-2-1-2. فيروسات الملفات..... 116
4-2-1-3. الفيروسات متعددة القدرة التحويلية..... 117
4-2-1-4. الفيروسات قطاع الإقلاع..... 117
4-2-2. أشكال الفيروسات..... 117
4-2-2-1. التحفي 117
4-2-2-2. البطيء..... 117
4-2-2-3. السريع..... 117
4-2-2-4. المتعدد الأشكال..... 118
4-2-2. أشهر الفيروسات..... 118

4-2-2-1. . أشهر فيروسات الحاسب..... 118
4-2-2-2. أشباه الفيروسات..... 119
4-3. آثار الفيروسات..... 122
4-3-1. أعراض الإصابة بالفيروس..... 122
3-3-1-1. نفص شديد في الذاكرة..... 122
3-3-1-2. تغيير عدد الملفات 122
3-3-1-3. عرض رسائل خطأ 122
4-3-2. الأضرار التي تترتب على الإصابة بالفيروس..... 124
3-3-2-1. ملء ذاكرة الحاسب بالنفايات..... 124
3-3-2-2. فقد ملفات من الذاكرة..... 124
3-3-2-3. تحطيم الفهرس الرئيسي..... 124
3-3-2-4. فقد قطاع التشغيل بالقرص..... 124
4-3-3. . أنواع دمار الفيروسات..... 125
4-3-3-1. الدمار التافه والثانوي..... 125
4-3-3-2. الدمار المعتدل 125

الفصل الخامس :أمن المعلومات بين التشريعات، التقنيات والأخلاق

5-1. أمن المعلومات : الماهية والأنواع..... 127
5-1-1. ماهية أمن المعلومات..... 127
5-1-1-1. تعريف أمن المعلومات..... 127
5-1-1-2. تطور مفهوم الأمن المعلوماتي..... 129
3-1-1-3. عناصر أمن المعلومات..... 130
5-1-2. . أنواع أمن المعلومات..... 131
5-1-2-1. العمليات الأساسية لأمن المعلومات..... 132
5-1-2-2. أنواع حماية أمن المعلومات. 133
5-1-2-3. حماية وحفظ ونقل المعلومات..... 134
5-1-3. طرق حماية المعلومات..... 136
5-1-3-1. التوقيع الإلكتروني..... 137
5-1-3-2. . تشفير البيانات..... 141
5-1-3-3. جدران النار..... 144
5-2. أمن المعلومات : الأخلاق..... 149
5-2-1. مجتمع المعلومات..... 149
5-2-1-1. مفهوم مجتمع المعلومات. 149
5-2-1-2. خصائص مجتمع المعلومات..... 150
5-2-1-3. ملامح وأبعاد مجتمع المعلومات..... 153
5-2-2. أخلاق مجتمع المعلومات 154

5-2-2-1. تعريف أخلاق أمن المعلومات..... 154
5-2-2-2. أهم المباذئ الاخلاقية في مجتمع المعلومات 155
5-2-2-3. الإفرازات الأخلاقيةالجديدة في مجتمع المعلومات..... 156
5-2-3. أخلاق الحاسب والأنترنت..... 158
5-2-3-1. الأنترنت : الماهية والخدمات..... 185
5-2-3-2.مخاطر الانترنت..... 162
5-3. أمن المعلومات والتشريعات. 164
5-3-1. التشريعات الخاصة بأمن المعلومات..... 164
5-3-1-1. تعريف التشريعات الخاصة بأمن المعلومات. 164
5-3-1-2. أنواع التشريعات الخاصة بأمن المعلومات. 165
5-3-1-3.قوانين الكمبيوتر 166
5-3-1-4. التشريعات الخاصة بالأموال الإلكترونية..... 167
5-3-2. الملكية الفكرية للمصنعات الرقمية 168
5-3-2-1. الملكية الفكرية للمصنعات الرقمية..... 168
5-3-2-2. المصنعات الرقمية الخاضعة للحماية..... 169
5-3-2-3. المعاهدات والقوانين الخاصة بالملكية الفكرية..... 170
5-3-3.المكافحة القانونية للجرائم الإلكترونية. 170
5-3-3-1. المعاهدات والمؤتمرات الدولية لمحاربة الجريمة المعلوماتية..... 172
5-3-3-2.على المستوى العالمي..... 172
5-3-3-3.على المستوى العربي. 173
الخاتمـــــة..... 174
قائمة المراجـــع 179
الملاحـــــــق..... 180

مقدمة

مقدمـــــــــة

إن المتأمل في المسيرة التاريخية لعالمنا المعاصر يلاحظ أن هناك تحولات جذرية إختلت فيها مفاهيم حضارية برمتها وأعيد النظر في الكثير من القضايا التي مثلت بالأمس القريب قيما ثابتة؛ وقد ألقت هده التحولات ظلالها على كافة القطاعات المجتمعية السياسية منها والإجتماعية، التجارية والصناعية فلم يعد العالم يسير بالحروب والطاقة والمال بل غدى يتحرك بالآحاد والأصفار الصغيرة بالقليل من البيتات؛ إن الحرب التي تدور في الخارج لم تعد تتعلق بمن يملك العتاد ويستحوذ على المال إنها تتعلق بمن يسيطر على المعلومات.

في مجتمع الفضاء السيبري ذلك النسق الهائل لترتيب وإتاحة كميات ضخمة من المعطيات في الحاسبات تحول العالم إلى بيت عنكبوت عير منظم الروابط عالم الشبكات, الصفر والواحد موصولة بطريقة إفتراضية وفضائية فائقة السرعة؛ عالم توحدت فيه البنى التحتية المعلوماتية على المستويات المحلية الإقليمية والدولية لتصبح بنية المعلومات كونية؛عصر وصلت فيه التطورات الرئيسة التي وصفها كاكو في"أعمدة العلم الثلاثة" المادة,الحياة, العقل (الذرة, ADN , الحاسب) إلى قمتها؛ عصرأصبح الخيال العلمي فيه واقعا بل أصبح من الصعب التفريق بين الواقع والخيال؛ واقع تغيرت فيه قواعد اللعبة السياسية تتشكل معالمه ويعاد تشكيلها يسرعة, عصر حروبه بلا جيوش ومعاركه بلا دماء أستبدل الرصاص فيه بالبيانات فلم تعد الدول والحكومات تخشي من بعضها البعض بقدر خشيتها من المنضمات والأفراد.

وقد أدت الثورة التي أحدثتها المعلومات في العقدين الأخيرين إلى قلب الموازين وإحداث تغييرات جذرية في المفاهيم وفي القواعد وفي علاقات الناس وإذا كان من عامل مشترك لكل هذه التحديات فإنه يمكن تلخيصه في كلمة واحدة هي المعلومات؛ ذلك المصدر الهام والناذر في عالم اليوم سلاح الهجوم وسلاح الدفاع؛ وقد أدت الأنترنت – تلك المجرة التي ترتبط فيها ملايير الحاسبات وملايين الموزعات — إلى زيادة هذا السيل الجارف من المعلومات إنتاجا وتوزيعا واستخداما مما أذى إلى ضرورة خلق قطاع للتحكم فيها وهو قطاع المعلومات الذي أصبح يمثل المصدر الرئيسي للدخل القومي للكثير من الدول المتقدمة ومورد إستراتيجي وحيوي في إقتصاديات هده الدول .

وفي خضم هذه التطورات العلمية والتقنية التي يشهدها هذا العصر كان لابد للمؤسسات الحكومية والخاصة بمختلف أوجه نشاطها أن تبادربوضع الخطط وترسم السياسات اللازمة لتطوير نظم المعلومات والإتصالات وترتبط بشبكات المعلومات المحلية والوطنية وحتى العالمية منها والإهتمام بتهيئة الكوادر الفنية المتخصصة في مجال المعلومات وشبكاتها لتأمين أليات من شأنها توفير المعلومات الصحيحة والدقيقة لمتخدي القرار من أجل ضمان إستمرارية المؤسسة من أجل الحصول على موطئ قدم في عالم البقاء فيه للأصلح.

وفي إطار هذا التوجه كانت فكرة هذه المذكرة التي تسعى إلى إلقاء الضوء على بعض جوانب تكنولوجيا شبكات تناقل البيانات، وتبيان الأهمية الكبيرة التي تكتسيها هذه الأخيرة بالنسبة للمنظمات

والمؤسسات المعاصرة؛ فعن طريق هذه الشبكات المعتمدة على الإتصالات المتقدمة وتكنلوجيا الحاسبات الآلية تقلصت المسافة بين العاملين داخل المنظمة وبين المنظمات بعضها ببعض على كافة المستويات المحلية، الوطنية والدولية حيث تساعد هده التقنية في تناقل البيانات داخل المنظمة مما يعد حتمية في الإدارة الحديثة للمعلومات

ومن بين الدوافع التي أدت إلى طرق باب هذا الموضوع هو محاولة إلقاء الضوء على هذا العالم المثير ـــ عالم الشبكات ـــ وكيفية حمايتها وحماية المعلومات السارية داخلها ومدى مساهمتها في إدارة المعلومات في ظل الإدارة الإلكترونية التي اكتسحت المؤسسات بهدف تحقيق الميزة التنافسية التي تعد ركيزة الإقتصاد العالمي الجديد ويمكن إيجاز هذه الدوافع في مايلي :

1. محاولة تسليط الضوء على بعض الجوانب الغامضة المتعلقة بالبيئة الإلكترونيةعامة وبيئة الشبكات خاصة من الناحيتين النظرية والتقنية، وأهم الفوائد التي يمكن أن تضيفها الشبكة للمؤسسة .
2. التعريف بمختلف متطلبات إنشاء شبكة وك ذلك أهم المعايير العالمية المعتمدة في بنائها وأشهر البروتوكولات المسيرة لها.
3. تبيان أهم الأخطار التي يمكن أن تواجهها شبكات المعلومات والميكانيزمات المعتمدة لضمان أمنها وحماية وسلامة معلوماتها .
4. توضيح أهم المفاهيم المتعلقة ببيئة العمل الإلكتروني والإدارة الإلكترونية للمعلومات.
5. توضيح أهمية الشبكات في إدارة المعلومات وتناقلها في إطار ما يعرف بالإدارة الإلكترنية للمعلومات .
6. الرغبة الشخصية في مثل هذه المواضيع التي تكتسي طابع الحداثة دات الإرتباط الوثيق يالتخصص.

وجائت الخطة المعتمدة للدراسة مكونة من مقدمة وخمسة فصول إضافة إلى خاتمة, ففي الفصل الأول – إجراءات الدراسة الميدانية – سيخصص لتحديد أساسيات الدراسة والمتمثلة في أهمية البحث وأهدافه الإشكالية المتبناة والتي ستكون بمثاب الخيط الموجه أثناء البحث وما يلحقها من التساؤلات الفرعية للبحث والفرضيات والتي تعد حلولا أولية للغشكالات المطروحة وإنتهاء بالإجراءات الميدانية للدراسة .

أما فيما يخص الفصل الثاني من هذه الدراسة فسوف يتم التطرق فيه بإسهاب إلى مفهوم شبكات المعلومات وذلك من خلال محاولة رصد أهم التعاريف التي تتناول هذا الموضوع وكذلك المراحل التاريخية والمفهومية التي مر بها المصطلح, وبما أن الشبكات أصبحت القلب النابض والعصب المحرك في المجتمع المعاصر فقد حاولنا إبراز الأهمية التي تكتسيها الشبكة في آداء الاعمال داخل المؤسسة إضافة إلى أهم انواع الشبكات, كما عرجنا على ذكر المتطلبات المادية والمالية والبشرية التي يتطلبها إنشاء شبكة وأشهر المعايير العالمية المطبقة وأنواع البروتوكولات المسيرة لها دون أن ننسى المراحل التي تمر بها أي شيكة معلومات أثناء تصميمها .

وكما أن هذا العالم الجديد أصبح يزخر بإنتصارات تنير درب البشرية فإن له كذلك جانبا مظلما, حيث فتح المجال فيه للعبث والجريمة في أحدث ثوب لها فقد أصبحت جرائم المعلومات وشبكاتها بلا حدود لذلك إرتاينا أن نخصص الفصل الثالث لتسليط ضوء على الأخطار التي تهدد بيئة الشبكات أنواع هذه الجرائم أهدافها والسيمات التي تميز المجرم المعلوماتي وكذا أهم الميكانزمات الدفاعية المتبعة لضمان حماية وأمن هذه الشبكات والبيانات السارية خلالها والحفاظ على سرية وموثوقية المعلومات,ثم سيتم التطرق في نهاية الفصل بصفة موجزة إلى بعض الجوانب القانونية والأخلاقية في البيئة الإلكترونية.

إن الثورة المعلوماتية التي تجتاح العالم والتي احدثت قفزة نوعية في نمط الحياة حيث لم يعد العالم محكوما بمن يملك الطاقة والمال كما في العصور الصناعية بل أصبحت المعلومات شريانه الذي يمده بالحياة، وقد جاء الفضاء السيبيري ليحول العالم إلى بيت متشعب الروابط وبالتالي فقد جعل الإنفجار المعلوماتي عظمة الدول وهيمنتها تقاس بما تملكه من عمالة فكرية وقدرة على التحكم في المعلومات؛ ومنه إرتأينا التطرق في هذا الفصل إلى هذه الثورة التي تعد عصب هذا العصر ألا وهي ثورة الأنفلوميديا وبروز قطاع المعلومات إلى الوجود ليحكم هذا السيل العاصف من المعارف، كما سيتم التطرق من خلاله إلى أهم إفرازات الثورة العلمية والمتمثلة في ثورة المعلومات – ذلك التزاوج بين تكنولوجيا الإتصالات وتكنولوجيا التخزين – حيث سنتطرق إلى مفهومها ومظاهرها واهم العوامل التي تساعد على إنتشارها والآثار التي أفرزتها على حياة الأفراد.

أدت التطورات الهائلة التي أفرزتها الفترة المعاصرة إلى إحداث تغييرات جذرية على كل المستويات داخل المجتمع مست جميع القطاعات الإثتصادية والسياسية وحتىالناحية الإجتماعية، حيث دخلت المعلومات حياة الأفراد واليومية بعد أن كانت حكرا على فئات محددة من المجتمع كالأوساط الأكاديمية والمراكز البحثية، ولهذا خصصنا المبحث الأخير من هذا الفصل للتطرق لمختلف الجوانب المتعلقة بمجتمع المعلومات مفهومه،خصائصه، ملامحه وفرازاته التي طفت إلى الوجود.

إن الإبداع الإداري ليس نتاج مصادفة وإنما هو نتيجة حتمية لأسس وقواعد تُتَبع،ومن اهم هذه القواعد المشاركة بالفكر وإتاحة المعلومات وقد تجلت خلال السنوات الأخيرة الأهمية الكبرى التي تلعبها المعلومات في الإقتصاديات المعاصرة، وضرورتها كمورد يضاهي أهمية أو يفوق الموارد المالية وأمام هذا الزحم الهائل من المعلومات واليانات أدى إلى خلق صعوبة الإستفادة منها فكان لزاما على المهتمين إيجاد آليات لإدارتها – جمعها تخزينها معالجتها من أجل إستخدامها بطريقة تضمن تقديم الخدمة المتميزة ومن هنا برز مفهوم إدارة المعلومات، ولهذا قمنا بتخصيص المبحث الأول من الفصل الأخير للتطرق إلى هذا المفهوم ماهيته، ظهوره، مراحل إدارة المعلومات وأهم ماقدمته من مزايا حتى تتمكن القيادات الإقتصادية من مواكبة المستجدات والتكي معها وتوظيفها بفعالية، ولقد خلق إنفجار المعلومات وسرعة إنتاجها وبثها صعوبة إدارتها بالطريقة التقليدية وبالتالي بروز التوجه والإنتقال من العمل الإداري التقليدي إلى تطبيق تقنيات المعلومات

والإتصالات في البناء التنظيمي وإستخدام التقنية الحديثة على رأسها شبكات الحااسب لربط الوحدات التنظيمية مع بعضها لتسهيل الحصول على المعلومات والبيانات لإتخاذ القرارات المناسبة وإنجاز الأعمال وهكذا ظهر مصطلح الإدارة الإلكترونية للمعلومات وبرز إلى الوجود، وهي عبارة عن منظومة إلكترونية متكاملة تهدف إلى تحويل العمل اليدوي العادي من الطريقة اليدويثة إلى إلى إدارة حاسوبية، وذلك بالإعتماد على نظم معلوماتية قوية تساعد في إتخاذ القرار بأسرع وقت وقل التكاليف وهذا ما سيتم تناةله في المبحث الثاني من هذا الفصل إلى مفهومها, عناصرها، ودواعي الإنتقال إليها؛ اما المبحث الإخير في هذا الفصل فسأتناول فيه أهم العمليات الخاصة بالمعلومات والتي تتم على مستوى الشبكات وكذلك الخدمات التي تقدمها الشبكة لعمال المنظمة والتسهيلات التي قدمتها تكنولوجيا الشبكات لتسهيل العمل الإداري وإضفاء الميزة التنافسية للأعمال .

وفي الأخير يتم وضع خاتمة أحاول من خلالها تجسيد لأهم النتائج المتوصل إليها في هذه الدراسة والتطرق إلى ممدى تحقق الفرضيات مع نتائج الدراسة الميدانية.

وختما أتمنى من المولى غز وجل أن أوفق في معالجة هذا الموضوع وأتوصل إلى تحقيق بعض أهداف البحث ليكون مساهمة في إثراء البحث العلمي .

أساسيات موضوع البحث:

يبدو واضحا اليوم أننا إزاء شكل جديد من أشكال التطور المجتمعي يعتمد في سيطرته ونفوده على المعلومات والمعرفة مثلما يعتمد على كفاءة إستخدامها في كل مجالات الحياة، حيث تعاظم دور صناعة المعلومات بوصفها الركيزة الأساسية في بناء الإقتصاديات الحديثة وبالموازاة مع ذلك يشهد العالم نموا كبيرا في استخدام شبكات المعلومات المبنية على الحاسب من خلال التزايد المستمر لاعدادها على المستويات الوطنية والإقليمية والدولية وذلك محاولة لتصدي لحجم المعلومات المتزايد إنتاجا, تخزينا, معالجة واستخداما.

أهمية الموضوع:

في عصر الإزدهار الإلكتروني في زمن قيام الحكومات الالكترونية، تبدل نمط الحياة وتغيرت معه اشكال الاشياء وانماطها وفي مقدمتها النظام الاقتصادي العالمي الجديد الذي تقوم دعائمه بدرجة عالية على التقدم العلمي والتكنالدراسة في مجال شبكات المعومات والادارة الالكلوجي والقدرة على استيعاب تدفق المعلومات والتمكن من استخدامها و تطبيقها في مجالانت التنمية المستدامة.

وامام هذه التحولات وجدت المؤسسات نفسها مجبرة على مسايرة االتقنية االعالمية واحدات تغييرات على هياكلها الادارية واساليب العمل واعادت هندستها بما يتماشا وذه النقلة المعلوماتية، وهذا ما ادى الى بروز الحاجة للاعتمادها على نطم وشبكات المعلومات فب ادارة اعمالها و وطائفها فب طل واقع الكتروني يفرض نفسه بقوة على ساحة الاعمال؛ وقد كان طهور الادارة الالكترونية كثمرة من ثمار ذا التطور التقني الدور الكبير لاعادت هيكلة هذه المؤسسات وادارة اعمالها.

وقد جاء هذا البحث محاولة لتسليط الضوء على بعض مفاهيم بيئة الشبكات فالمصطلح الاول هو مصطلح شبكات المعلومات مفهومها, اشكالها,متطلباتها وكيفية حمايتها؛ اماالمصطلح الثاني فهو مصطاح حديث وحيوي نتيجة التطورات الكبيرة التي يشهدها العالم منذ فترة إنتقاله غلى العمل الإلكتروني بعيدا عن التعاملات الورقية التقليدية ونقصد بالقول هنا الإدارة الإلكترونية للمعلومات وقد حاولنا من خلال هذا البحث تبيان العلاقة القائمة بين هذه المتغيرات .

كما ادت هذه التكنولوجيا الجديدة غلى ظهور عمل جديدة فرضتها التغيرات المجتمعية، وبروز ظرورة إيجاد آليات تتماشى مع عالم متسارع من أجل تقويم الآداء وتحسين الإنتاجية ,وأمام هدا الواقع ظهرت شبكات المعلومات التي تنمو وتنتشر في كافة القطاعات وداخل المؤسسات وعليه ارتأيت الخوض في غمار هدا العالم وتسليط الضوء على بعض خباياه وجوانبه المظلمة اضافة الى :

الشبكات في اداء الاعمال وفي ادارة المعلومات داخلها

الاهتمام الشخصي بالموضوع محل الدراسة الناتج عن حب الاطلاع على كل ماله علاقة بعالم الاعلام الالي عامة وعالم الشبكات خاصة.

أهداف البحث:

نهدف من وراء هده الدراسة في مجال شبكات المعلومات والادارة الالكترونية لتدفق المعلومات داخل المؤسسة الى :

- من الناحية النظلرية , محاولة تجميع مختلف جوانب الموضوع المشتتة في العديد من المراجع و جمعها في عمل واحد بغرض خدمة البحث العلمي
- معرفة ماتوصلت اليه التقنية في مجال التشابك وادارة المعلومات الالكترونية وكيفية توفير الحماية لها على الصعيد التقني و التشريع
- أما الجانب الميداني من الدراسة فيهدف الى الوقوف على واقع تطبيق تقنية التشابك داخل المؤسسات الجزائرية ومدى اطلاع المسؤولين عن الدور والاهمية التي يلعبها في ادارة الاعمال
- التأكيد على ضرورة مواكبة المؤسسات للركب الحضاري والتقنية المعاصرة
- التعرف على متطلبات الادارة الالكترونية للمعلومات
- ابراز اهم فوائد تطبيق الادارة الالكترونية عبر شبكة المعلومات
- الوقوف على اهم المعوقات والتحديات التي تنخلل البيئة الشبكية .

الإشكاليـــــــــــــة:

إننا امام عالم آخر ومشهد مختلف من مشاهد صراعات القرن عصر أحدثت المعلومات فيه أثرها العميق على البنيات الإجتماعية والإقتصادية والسياسية والاكثر من ذلك على المنضومات الإدارية والمناهج التسييرية؛ عالم تعد فيه المعلومات القوة الفاعلة والعصب المحرك لكل مناحي الحياة وأداة قياس التخلف والرقي، التطور والإنحطاط، وقد ساهمت الشبكات على رأسها الشبكة العالمية في قلب جميع الموازين وخلط أوراق العالم، وأمام هذه الإمكانيات الهائلة واللامحدودة للشبكات أصبحت لمعلومات بإختلاف أنواعها وكمياتها وأهدافها تحت أنامل الافراد.

وبإزدياد كم هذه المعلومات وسرعة تدفقها إزدادت الحاجة إلى تبادلها ونقلها من مكان امام هذا المشهد وجدت المؤسسات العمومية والخاصة نفسها في مواجهة شك عدم التأقلم والتكيف مع هدا المحيط المتسم بالتغيير مما طرح عليها عبء إعادة تغيير أساليب العمل وضرورة إيجاد آليات وميكانزمات من شأنها توفير المعلومات الصحيحة والدقيقة لمتخدى القرار من أجل ضمان استمرارية المؤسسة، وتعد نظم وشبكات المعلومات أهم وأبرز هذه الآليات التي تعتمد عليها الإدارة الحديثة، وقد أدركت المؤسسات في الدول المتقدمة

الدور الريادي الذي تلعبه هذه الشبكات في إدارة أعمالها فبادرت قياداتها بإدخال هذه التقنية وإدراجها ضمن سياساتها الإستراتيجية، وكذلك الحال بالنسبة لبعض الدول النامية التي سعى مسؤولوها إلى مواكبة التطورات الحديثة في الإدارة بإستخدام التكنولوجيا .

فإذا كان هذا حال المؤسسات في الدول المتقدمة فماهو واقع شبكات المعلومات في المؤسسات الجزائرية في ظل الإدارة الإلكترونية للمعلومات ؟

- وماهي أهم الأدوار التي تلعبها هذه الشبكات في إدارة الأعمال داخل المؤسسة ؟
- وهل أن المسؤولين داخل المؤسسات الجزائرية واعين بالأهمية التي تكتسيها هذه الشبكات ؟

تساؤلات البحث :

على ضوء الإشكالية المتبناة يمكن طرح مجموعة من الأسئلة التي أثارتها إشكالية البحث والتي يمكن من خلالها الألمام بالمحتوى العام للبحث واهم هذه التساؤلات :

- ماذا نعني بشبكات المعلومات نظريا وماهي حدود تطبيقها ميدانيا في المؤسسات الجزائرية ؟
- ماهي اهم الأخطار التي تواجه شبكات المعلومات وكيفية توفير الحماية لها ؟
- ماذا نعني بإدارة المعلومات وماهي أبعادها ؟
- ما المقصود بالإدارة الإلكترونية للمعلومات وما دواعي الإنتقال من إدارتها تقليديا إلى إدارتها إلكترونيا ؟
- ما هي الأدوار التي يمكن ان تلعبها شبكات المعلومات وفي الغدارة الالكترونية للمعلومات داخل المؤسسات وما القيمة التي تظفيها على إدارة الأعمال ؟

الفرضيـــــــات:

للإجابة على التساؤلات السالفة الذكر تمت صيغة مجموعة من الفرضيات كما يلي:

- تمتلك مؤسسة إتصالات الجزائر شبكة معلومات عالية الجودة .
- تلعب شبكة المعلومات التابعة لمؤسسة "إتصالات الجزائر" دورا مهما في إدارة المعلومات والأعمال داخل المؤسسة .
- المسؤولين بشركة "إتصالات الجزائر" واعين باهمية شبكة معلومات داخل المؤسسات
- تعترض شبكة المعلومات التابعة لمؤسسة "إتصالات الجزائر" بعض الصعوبات على المستوى الأمني .

الفصل الأول
إجراءات الدراسة

الفصل الأول: إجراءات الدراسة

-1 أساسيات موضوع البحث:

إن الثورة المعلوماتية التي تجتاح العالم والتي أحدثت قفزة نوعية في أسلوب ونمط الحياة من كل النواحي, فلم يعد العالم يسير بالطاقة كما في العصور الصناعية بل أصبحت المعلومات شريانه والمورد الذي يمده بالحياة؛ وقد جاء الفضاء السيبيري ليحول العالم إلى بيت عنكبوت متشعب الروابط والروافد، وبالتالي فإن الإنفجار المعلوماتي جعل عظمة الدول وهيمنتها تقاس بما تملكه من عمالة فكرية وقدراتها على التحكم في المعلومات.

1-1-1. أهمية الموضوع:

في عصر الإزدهار الإلكتروني وفي زمن قيام الحكومات الإلكترونية، زمن القرية الكونية، تبدل نمط الحياة وتغيرت معه أشكال الأشياء وأنماطها ومنه ولاشك أنماط المجرمين وكذا أنماط جرائمهم ؛ والتي قد يحتفظ بعضها بإسمها التقليدي مع تغير جوهري في طرق إرتكابها؛ إذن فإننا نقف اليوم على أعتاب حضارات جديدة وثقافات جديدة؛ حيث تضمحل وتزول كل الحواجز والحدود؛ ثقافات رسمت معالم لمصطلحات في بيئة تشابكت أطرافها وتداخلت؛ وهذا البحث محاولة لتسليط الضوء على بعض مصطلحات من هذه البيئة فالأول يرتكز حول مفهوم الهاكرز، الكراكر أو المجرم المعلومات إن صح التعبير والثاني حول الجريمة الإلكترونية أما المصطلح الثالث فيدور في فلك أمن المعلومات في أبعاده المختلفة؛ وفي بحثي هذا حاولت تبيان علاقة بين مختلف المتغيرات التي تطرقنا إليها.

إن إنتشار التكنولوجيا الحديثة وإستعمالاتها التي مست كل مناحي الحياة أفرزت العديد من التحولات والتغيرات والمخاطر والوسائل والتقنيات بشقيها الإيجابي والسلبي؛ فغدت على أعتابها البيئة الجديدة مسرحا للعديد من التناقضات والتحولات والتحديات على الصعيدين التقني والتشريعي، وعليه ارتأيت الخوض في غمار هذا العالم وإكتشاف خباياه وتسليط الضوء على بعض جوانبه بالإضافة إلى:

- حداثة الموضوع ومحاولة إستطلاع الواقع عن قرب لمعرفة مدى تمكن طلبة الإعلام الآلي – لإعتبارها الفئة الأكثر إطلاعا في هذا المجال – من حماية معلوماتهم وإطلاع طلبة الحقوق على المستجدات التشريعية في هذا الخصوص.
- الإهتمام الشخصي بالموضوع محل الدراسة النابع من حب إستطلاع على كل ماله علاقة بعالم الإعلام الآلـــي والتقنية الحديثة.

1-1-2. أهـــــــــــــداف البحث:

نهدف من وراء هذه الدراسة في مجال أمن المعلومات والجريمة الإلكترونية إلى:

- من الناحية النظرية محاولة تجميع مختلف جوانب الموضوع والمشتتة في العديد من المراجع وجمعها في عمل واحد بغرض خدمة البحث العلمي.
- معرفة ما توصلت إليه الدول الغربية التي تقود العالم في مجال أمن المعلومات سواء من الناحية التشريعية أو من الناحية القانونية، وواقع الدول العربية في ظل هذه التحولات.
- أما الجانب الميداني من البحث فيهدف إلى معرفة مدى إلمام طلبة الدراسات العليا بالمستجدات في عالم الجريمة.
- معرفة مدى إطلاع طلبة الإعلام الآلي بالتقنيات الحديثة والمستجدات في مجال حماية و أمن البيانات والمعلومات.
- أما الحقوقيين فقد حاول تقصي مدى مواكبتهم للتطورات الحاصلة في التشريعات والقوانين الحاصلة بالبيئة الإلكترونية.
- التنبيه إلى ضرورة التسلح بثقافة معلوماتية من أجل الحفاظ على معلوماتنا وخصوصيتنا داخل مجتمع المعلومات الذي نحن على أعتابه.

1-1-3. الإشكـــــــــالية:

إننا أمام عالم آخر ومشهد مثير من مشاهد صراعات القرن الذي نعيشه، عصر أحدثت فيه المعلومات أثرها العميق على البنيات الإجتماعية والعلمية والسياسية والأكثر من ذلك أثرها على المنظومات الأخلاقية؛ عالم تعد المعلومات فيه القوى الفاعلة والعصب المحرك لكل مناحي الحياة وأداة قياس التخلف و الرقي، التطور والانحطاط؛ وقد ساهمت الشبكات على رأسها الشبكة العالمية في قلب جميع الموازين وخلط أوراق العالم وأمام هذه الإمكانيات الهائلة واللامحدودة للأنترنت أصبحت المعلومات بإختلاف أنواعها وكمياتها وأهدافها تحت أنامل الأفراد.

وبإزدياد كم المعلومات وتدفقها، وإزدياد الحاجة إلى تبادلها ونقلها من مكان إلى آخر وطنيا وإقليميا وحتى دوليا، ومنه أصبح أمن هذه المعلومات وسريتها في خطر، وأصبحت عرضة للقرصنة والتحويل والتغيير والإتلاف، وقد كسرت عمليات الإختراق كل المساعي الرامية لحمايتها؛ وبهذا فتحت الأنترنت باب الخطر والجحيم على كافة الأصعدة المالية، الأخلاقية، والمصرفية ووقف العالم أمام هذا المشهد أعزل السلاح؛ وبالتالي لم يعد إنشغال الناس بتوفير المعلومات التي طالما كانت المطلب والهاجس الدائم لهم بقدر إنشغالهم بكيفية إيجاد وتوفير ميكانزمات لحماية معلوماتهم وخصوصياتهم التي قد تصبح في متناول أصغر فرد يلج العالم الإلكتروني.

إن هذه الوضعية التي يعيشها العالم جعلت كل الأفراد الفاعلة تتحرك لكل على مستواه لإيجاد حل لهذه المعضلة مما خلق تساؤلات حول أهم التحورات والتحولات التي طرأت على مسرح الجريمة والإجرام ؟ والكيفية التي يمكن من خلالها إحتواء هذه الظاهرة قانونيا وتقنيا ؟ وما هو الدور الذي يمكن أن تلعبه السلطة الأخلاقية في التقليل من وطأة الأزمة.

1-1-4. تساؤلات البحث:

على ضوء الإشكالية المتبناة يمكن طرح مجموعة من الأسئلة التي أثارتها مشكلة البحث والتي يمكن من خلالها الإلمام بالمحتوى العام للبحث وأهم هذه التساؤلات:

- هل أصبحت البيئة الإلكترونية أقل أمنا وعرضة لإنتهاكات الأفراد والجماعات؟
- هل أصبح الإجرام المعلوماتي في البيئة الجديدة ظاهرة لا مفر منها لابد من تضافر الجهود لمواجهتها ؟
- ها أصبحت خصوصيات الأفراد وأسرارهم تعرض على قارعة الطريق على يد المجرمين المعلوماتيين ؟
- هل هناك ضوابط تسير وتوجه التعامل في الفضاء السيبيري ؟
- إلى أي مدى يمكن إعتبار الأخلاق ضابطا وسلطة رادعة في التعامل مع الشبكة ؟.
- ما منبع هذه الأخلاق داخل الفرد، هل هي تربية الفرد أم عقيدته أم أعراف المجتمع الذي يعيش فيه ؟
- ماذا نحمي من معلوماتنا وما هي أهم المخاطر التي تواجهها ؟
- هل توفير الحماية ضرورة حتمية في دوامة العولمة التي نتخبط فيها ؟
- هل طلبة الحقوق على دراية بالتطورات الحاصلة في مجال التشريعات الدولية للحماية من الجريمة الإلكترونية ؟
- هل التشريع الجزائري يسعى لمواكبة التطورات الإجرامية بقوانينه الجنائية ؟

1-1-4. الفرضيـــــــــــات:

للإجابة على التساؤلات تمت صياغة مجموعة من الفرضيات كما يلي:

- إن غياب مواكبة التطورات الحاصلة في مسرح البيئة الإلكترونية من جرائم يؤدي إلى جعل الأفراد عرضة لهؤلاء المجرمين في أي وقت.
- يؤدي غياب الثقافة المعلوماتية في مجال حماية الأفراد لمعلوماتهم إلى زيادة عدد الجرائم مما ينتج عنه تخوف من إستعمال التكنولوجيا والإبتعاد عنها.
- إن غياب الوازع الأخلاقي لدى التعامل مع الشبكة يؤدي إلى إنحرافات أخلاقية وتصرفات غير مشروعة تنقص من مصداقية التعامل مع التكنولوجيا الحديثة.
- نقص أو غياب الأُطر القانونية المواكبة للتطورات الحاصلة يؤدي إلى خلق فجوات قضائية تساهم في الحد من إستعمال التكنولوجيا.

1-1-5. الدراسات السابقة:

إن العلم بناء متكامل وسلسلة متصلة الحلقات , والتجارب الحالية تعتبر همزة وصل بين التجارب السابقة والتجارب اللاحقة، والبحث العلمي الناجح هو الذي يبنى على الأبحاث والدراسات السابقة لتفادي

الأخطاء واستخلاص التجارب وضمان الحداثة وعدم التكرار؛ ومن خلال تفحصي للدراسات السابقة التي عالجت الموضوع المذكرة بتسليط الضوء على جانب أو أكثر من جوانبه، كونها مست من قريب أو من بعيد أمن المعلومات أو الجريمة الإلكترونية أو المجرم المعلوماتي أو التشريعات المتعلقة بالموضوع ومن أهم هذه الأبحاث والدراسات نذكر على سبيل المثال:

1- الدراسة الأولى:

بن ضيف الله فؤاد بعنوان "أمن المعلومات وحقوق التأليف الرقمية والتي تعتبر دراسة لها علاقة وطيدة بموضوع البحث حيث تطرقت إلى الجوانب المتعلقة بالمعلومات البيئة الإلكترونية أمن المعلومات داخل هذه البيئة وكذا الغوص في أغوار الملكية الفكرية وخاصة تلك المتعلقة بالمصنفات الرقمية وأهم التشريعات فيما يخص حمايتها.

2- الدراسة الثانية:

- المهندس حسام شوقي.حماية وأمن المعلومات على الأنترنت وهي دراسة شاملة تمس موضوع المذكرة وقد تطرق المؤلف بشيء من الإيجاز إلى مختلف الجوانب التي تعالج موضوع شبكة الأنترنت وتوفير الأمن سواء للبريد الإلكتروني أو المنسابة عبر الشبكة،كما تعرض للأختراق أساليبه وبرمجياته.

3- الدراسة الثالثة:

- منير محمد الجنبيهي.أمن المعلومات الإلكترونية وبإعتبار الكاتب محامي فهو على دراية بالجوانب القانونية ولهذا وفق إلى أبعد حد في معالجة أمن المعلومات من الناحية التشريعية وإيراد مختلف القوانين الدولية لمكافحة جرائم الحديثة كما تطرق إلى أهم المحاولات العربية في هذا المجال.

4- الدراسة الرابعة:

- البداينية دياب. الأمن وحرب المعلومات؛ وقد عالج المؤلف في كتابه العديد من القضايا التي تخ ص الأمن الوطني من منظور المعلوماتي وكيفية حماية الكيانات المعرفية في الفضاء الافتراضي، والذي أصبح عرضة لانتهاكات وأخطار لا متناهية؛ كما تطرق إلى خصائص المجرمين المعلوماتيين ، وأنواعهم ومختلف مميزاتهم؛ وأسبابهم للجريمة مما مس بشكل مباشر موضوع البحث.

أما عن الدراسات العالمية التي تناولت موضوع أمن المعلومات فقد أوردها الأستاذة فاتن بومفلاح في دراسة قدمتها بمناسبة المؤتمر الثاني عشر للأتحاد العربي للمكتبات العربية وأهمها [1]:

- دراسة "Rowley.j" الصادرة عام 1995 والتي تناولت الجوانب التي تهدد أمن المكتبات والمعلومات سواء في شكلها التقليدي أم في غيره بما في ذلك نظم الحاسبات الإلكترونية، وإستعرضت الدراسة السياسات الأمنية ومكوناتها كما تناولت تأثير التهديد وفقدان الأمن على المكتبات مشيرة إلى أنواع المخاطر التي تتعرض لها.

---

[1]- فاتن، حماية وأمن المعلومات في شبكة جامعة أم القرى.من كتاب الوقائع.مج2.الشارقة.ص554.

- عام1997 صدرت دراسة "Cervon.f" التي تناولت الجوانب المتعلقة بأمن شبكة المعلومات في نظام: "Illinois illinet online"بعد إدخال الفهرس المباشر، وقد أشارت الدراسة إلى المفاهيم المتعلقة بأمن المكتبات.

- في عام 1998 استعرضت دراسة أشرف الغنيمي الطرق المعتمدة لانتهاك أمن المعلومات في نظم الحاسب الآلي وأساليب الحماية منها.

1-2. إجراءات الدراسة الميدانية

1-2-1. منهج البحث:

لقد اعتمدت في هذا البحث على المنهج الوصفي بالنسبة للجانب النظري وهذا عند عرض مختلف العناصر المتعلقة بالمذكرة كالتعريفات الخاصة بالمجرمين المعلوماتيين وكذا الجريمة الإلكترونية وأنواعها كلا منهما، إضافة إلى إيراد مختلف عناصر أمن المعلومات سواء تعلق الأمر بالأمن من جانبه لتقني أو القانوني أوعلاقتة بالإطار الأخلاقي للأفراد؛ كما اعتمدنا المهج الإحصائي التحليلي بالنسبة للجانب التطبيقي (الجانب الميداني) وذلك بتفريغ إستبانة الدراسة ثم شرح النتائج المتحصل عليها.

1-2-2. أساليب تجميع البيانات:

كانت الإستبانة هي الأداة التي استخدمت أثناء البحث كأسلوب لتجميع البيانات، وتعتبر الإستبانة الأداة الأكثر فاعلية وملائمة لمثل هذ ه المواضيع وهذا لا يعني عدم تعرضي للعديد من المشاكل والعراقيل أهمها عدم العثور على أفراد عينة الدراسة باعتبار فترة آخر السنة الدراسية؛ وكذلك حداثة الموضوع وبالتالي عدم إستعاب الكثير من الطلبة لعديد من جوانب موضوع الدراسة خصوصا بالنسبة لطلبة الحقوق.

وأثناء تصميم استمارة الإستبانة، حاولت ترجمة إشكالية البحث الممثلة لموضوع الدراسة من خلال 25 (خمسة وعشرون) سؤالا، تحتوي الكثير من الأسئلة على أسئلة فرعية؛ وأغلبها كانت أسئلة مغلقة وذلك لمحاولة التحكم في مسار البحث وعدم خروج المبحوثين عن الإطار العام للدراسة أو الميل عن الإشكالية المتبناة.

وقد قمت بتوزيع أسئلة الإستمارة على عناصر البحث وفقا لأربع محاور على النحو التالي:

المحور الأول: المجرم المعلوماتي ؛ تدور أسئلة هذا المحور والتي بلغ عددها 04 (أربعة)أسئلة حول الأنماط الجديدة للمجرمين والذين أفرزتهم البيئة المعلوماتية الجديدة وأهم الفوارق التي يمكن أن تميز المجرم المعلوماتي عن نظيره المجرم التقليدي؛ وكذلك الأسباب التي تكون دافعا لارتكاب هذه الجرائم؛ كما تطرقت كذلك في هذا المحور إلى أهم المميزات التي تميز المجرمين المعلوماتين.

المحور الثاني الجريمة المعلوماتية : وكضرورة حتمية وإستكمالا للتسلسل المنطقي للموضوع وبعد الحديث عن المجرم المعلوماتي لابد من التطرق إلى الجريمة المعلوماتية, وهذا ما حاولن ا التركيز علية في المحور الثاني للإستبانة

والمكون من ستة (06) أسئلة تدور في فلك الجريمة المعلوماتية؛ بدآ بمميزاتها وأنواعها أهم الجرائم التي تصنف كجرائم معلوماتية.

المحور الثالث أوبئة الفضاء السيبيري آو الفيروسات : وفي هذا المحور حاولنا إلقاء نظرة حول الفيروسات والتي تعد أهم وأخطر الجرائم المهددة لأمن وسلامة الشبكات والأنظمة والتي يرتكبها الهاكر في الفضاء السيبيري.

المحور الرابع أمن المعلومات: وقد بلغ عدد الأسئلة خمسة عشرة (15) سؤالا, وقد صيغت الأسئلة بحيث عملت على تغطية عنصر أمن المعلومات من كافة جوانبه التقنية والأخلاقية وكذا تسليط الضوء على الجانب القانوني في الجزائر فيما يخص مجال الجرائم المعلوماتية.

2- المقـــــــــــابلة:

تم إجراء مقابلة مع المسؤولين عن الدراسات العليا لكل من قسمي الإعلام الآلي والحقوق وكان الهدف من هذه لمقابلة هو الحصول على العد د الإجمالي للطلبة المسجلين في الدراسات العليا وقد أدى كلا المسؤولين تعاونا وتجاوبا.

1-2-3. الحدود الجغرافية للدراسة الميدانية:

1-2-3-1. الحدود الجغرافية

يشمل الحيز المكاني (الجغرافي) قسم الحقوق بالمركب الجامعي تيجاني هدام وقسم الإعلام الآلي بجامعة منتوري قسنطينة.

1-2-3-2. الحدود البشرية للدراسة الميدانية:

وتشمل على أفراد مجتمع الدراسة والمتمثلة أساسا في طلبة الحقوق والإعلام الآلي المسجلين في الدراسات العليا لجامعة منتوري قسنطينة للموسم الدراسي 2005-2006 والبالغ عددهم 150 طالب بالنسبة لطلبة الحقوق و 38 بالنسبة لطلبة الإعلام الآلي وقد تم الحصول على المعلومات بإجراء مقابلة مع المسؤولين عن الدراسات العليا لكلا القسمين؛والأعداد المعطاة موضحة في الجدول رقم: 01 صفحة ؟؟؟؟؟؟؟

1-2-3-3. الحدود الزمنية:

تتمثل المدة الزمنية في الوقت أو المدة التي تم استغراقها في الدراسة الميدانية بداية من تحديد موضوع الدراسة واختيار العينة المراد بحثها واختيار الوسيلة والأداة التي سيتم تجميع البيانات بواسطتها إلى غاية تحليل ووضع هذه النتائج في جداول وأشكال بيانية وهي المدة التي قاربت 05 أشهر, وقد استغرقت فترة توزيع واسترجاع الإستمارات شهريين مند أول مقابلة وإلى غاية إسترجاع آخر إستمارة

1-2-4. العينـــــــــــة:

عند إختيارنا لمجتمع الدراسة راعينا في ذلك ملائمة مجتمع الدراسة وكذلك العينة لموضوع البحث؛ من أجل الوصول إلى نتائج ذات مصداقية وواقعية.

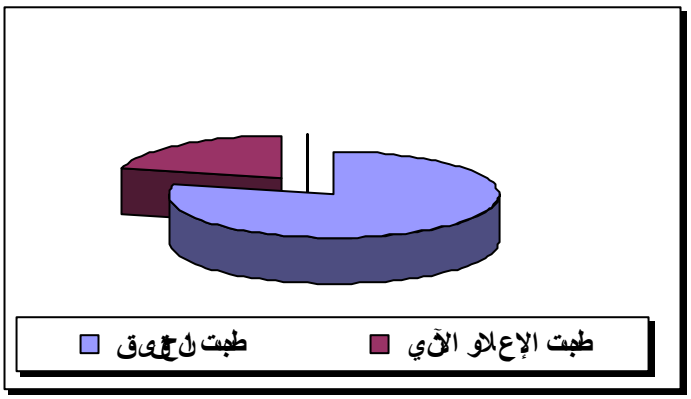
1-2-4-1. تحديـــد المجتمع الأصلي للدراســـــة:

يتكون مجتمع الدراسة من طلبة الدراسات العليا لكل من قسمي الحقوق والإعلام الآلي جامعة منتوري قسنطينة والذي بلغ عددهم (لموسم 2005- 2006) 150 بالنسبة للحقوقيين و 38 بالنسبة للإعلام الآلي أي بمجموع 188 طالب.

1-2-4-2. اختيار العينة من المجتمع الأصلي:

يتكون مجتمع الدراسة من طلبة الدراسات العليا لقسم الإعلام الآلي وقسم الحقوق والبالغ عددهم حوالي 188 طالب موزع على السنتين الأولى والثانية المبرمجة للدراسة.

وقد قمنا بإختيار نسبة 20 % لكلا القسمين، حيث قدرت عدد الإستمارات الموزعة 30 إستمارة على طلبة الحقوق و 08 إستمارات لطلبة الإعلام الآلي بنسبة 20 % كذلك.والإحصائيات المتبناة موضحة في الجدول رقم 02 صفحة ؟؟؟؟؟؟؟ أما عن عينة الدراسة حسب الأقسام فهي موضحة في الجدول رقم 03 صفحة؟؟؟؟؟؟؟ وهذا ما يوضحه الشكل البياني التالي:



الشكل رقم: 01 عينة الدراسة حسب الأقسام

1-3. ضبـــــــــــط المصطلحات والمفاهيم:

قبل البدا لابد من الإشارة إلى أهم المصطلحات الواردة في البحث:

1-3-1. الهاكـــــرز:

أطلقت هذه الكلمة أول ما أطلقت في الستينيات لتشير إلي المبرمجين المهرة القادرين على التعامل مع الكمبيوتر ومشاكله بخبرة ودراية حيث أنهم وكانوا يقدمون حلولا لمشاكل البرمجة بشكل تطوعي في الغالب. بالطبع لم تكن الويندوز آو ما يعرف بالـ Graphical User Interface أو GUI قد ظهرت في ذلك الوقت ولكن البرمجة بلغة البيسيك واللوغو والفورتوران في ذلك الزمن كانت جديرة بالأهتمام؛ ومن هذا المنطلق غذى العارفين بتلك اللغات والمقدمين العون للشركات والمؤسسات والبنوك يعرفون بالهاكرز وتعني الملمين بالبرمجة ومقدمي خدماتهم للآخرين في زمن كان عددهم لا يتجاوز بضع ألوف على مستوى العالم أجمع. لذلك فإن هذا الوصف له مدلولات إيجابية ولا يجب خلطه خطأ مع الفئة الأخرى الذين يسطون عنوه

على البرامج ويكسرون رموزها بسبب إمتلاكهم لمهارات فئة الهاكرز الشرفاء. ونظرا لما سببته الفئة الأخيرة من مشاكل وخسائر لا حصر لها فقد أطلق عليهم إسما مرادفا للهاكرز ولكنه يتداول خطأ اليوم وهو(الكراكرز Crackers).

كان الهاكرز في تلك الحقبة من الزمن يعتبرون عباقرة في البرمجة فالهاكر هو المبرمج الذي يقوم بتصميم أسرع البرامج والخالي في ذات الوقت من المشاكل والعيوب التي تعيق البرنامج عن القيام بدورة المطلوب منه. ولأنهم كذلك فقد ظهر منهم إسمان نجحا في تصميم وإرساء قواعد أحد البرامج المستخدمة اليوم وهما" دينيس ريتشي" و"كين تومسون" اللذان نجحا في أواخر الستينيات في إخراج برنامج اليونيكس الشهير إلي حيز الوجود[2].

1-3-2. الكراكـــــرز:

الكراكرز هن أشخاص موهوبين متخصصين بفك شرفيرات حقوق الملكية للبرامج وكل أنواع " السوفت وير" وأغلبهم على دراية كبيرة بلغات برمجة عدة.

كلمة الكراكر cracker مشتقة من الكلمة الإنجليزية "to cracker" ومعناها الكسر أو التكسير؛ ومعناها العام هو التخريب والعبث والتحطيم وهي عبارة عن إسم إختاره لأنفسهم مجموعة من المخربين المهرة القادرين على إختراق أي شبكة أو أي جهار حاسب، فهم لا يقلون مهارة أو كفاءة عن الهاكرز ولكنهم على العكس النقيض فإنهم يستخدمون هذه المهارة في التخريب والسرقة والحصول على الأموال بطريقة غير مشروعة[3].

كما يعرف الكراكر بأنه شخص خبيث متطفل فضولي يسعى إلى إكتشاف الحقائق والأخبار من خلال التطفل بوسائل غير قانونية وهم فضلا عن ذلك هم أشخاص عاديون يشغلون مناصب محل ثقة ولديهم الكفاءة الخاصة والمعرفة والمهارة المطلوبة في مجال الكمبيوتر[4]؛ المشترك بينهن وبين الهاكرز هو إيمانهم بضرورة مجانية المعلومات وعدم احتكار

1-3-3. الجريمة المعلوماتية[5]

لم يكن هناك قلق مع بدايات شبكة الإنترنت تجاه "جرائم" يمكن أن تنتهك على الشبكة، وذلك نظراً لمحدودية مستخدميها علاوة على كونها مقصورة على فئة معينة من المستخدمين وهم الباحثين ومنسوبي

---

[2] – **طرق الحماية من الهاكرز** [على الخط المباشر]. زيارة يوم :2006/02/12. متوفر على الموقع: http://www.absba.org/vb/forumdisplay

[3] – **من هم الهاكر ومن هم الكراكر**.[على الخط المباشر]. زيارة يوم:2005/12/20. متوفر على الموقع: < http://www.jehadokmatloob jeeran.com /al-hackerz/m.n.al hacker htm_l >

[4] – محمود، عبد الله حسين. **سرقة المعلومات المخزنة بالحاسب**. المرجع السابق. ص.54

[5] – الهاجري، إياس. **جرائم الإنترنت**. [على الخط المباشر].زيارة يوم :2006/02/12.متوفر على الموقع: http://www.egovs.com/egovs_webo2/news.

الجامعات. لهذا فالشبكة ليست آمنة في تصميمها وبناءها. لكن مع توسع إستخدام الشبكة ودخول جميع فئات المجتمع إلى قائمة المستخدمين بدأت تظهر جرائم على الشبكة إزدادت مع الوقت وتعددت صورها وأشكالها. وفيما يلي إستعراض لعدد من جرائم الإنترنت:

أولا: صناعة ونشر الفيروسات: وهي أكثر جرائم الإنترنت إنتشارا وتأثيرا. إن الفيروسات كما هو معلوم ليست وليدة الإنترنت فقد أشار إلى مفهوم فيروس الحاسب العالم الرياضي المعروف "فون نيومن"في منتصف الأربعينات الميلادية. لم تكن الإنترنت الوسيلة الأكثر استخداما في نشر وتوزيع الفيروسات إلا في السنوات الخمس الأخيرة، حيث أصبحت الإنترنت وسيلة فعالة وسريعة في نشر الفيروسات. ولا يخفى على الكثير سرعة توغل ما يسمى بـ "الدودة الحمراء" حيث استطاعت خلال أقل من تسع ساعات اقتحام ما يقرب من ربع مليون جهاز في 19 نوفمبر2001 م. إن الهدف المباشر للفيروسات هي المعلومات المخزنة على الأجهزة المقتحمة حيث تقوم بتغييرها أو حذفها أو سرقتها و نقلها إلى أجهزة أخرى.

ثانيا: الإختراقات : تتمثل في الدخول غير المصرح به إلى أجهزة أو شبكات حاسب آلي ؛ وجل عمليات الإختراقات (أو محاولات الإختراقات) تتم من خلال برامج متوفرة على الإنترنت يمكن لمن له خبرات تقنية متواضعة أن يستخدمها لشن هجماته على أجهزة الغير، وهنا تكمن الخطورة؛ تختلف الأهداف المباشرة للإختراقات، فقد تكون المعلومات هي الهدف المباشر حيث يسعى المخترق لتغيير أو سرقة أو إزالة معلومات معينة؛ وقد يكون الجهاز هو الهدف المباشر بغض النظر عن المعلومات المخزنة عليه، كأن يقوم المخترق بعمليته بقصد إبراز قدراته "الإختراقيه" أو لإثبات وجود ثغرات في الجهاز المخترق ؛ من أكثر الأجهزة المستهدفة في هذا النوع من الجرائم هي تلك التي تستضيف المواقع على الإنترنت، حيث يتم تحريف المعلومات الموجودة على الموقع أو ما يسمى بتغيير وجه الموقع(Defacing) ؛ إن استهداف هذا النوع من الأجهزة يعود إلى عدة أسباب من أهمها كثرة وجود هذه الأجهزة على الشبكة، وسرعة إنتشار الخبر حول اختراق ذلك الجهاز خاصة إذا كان يضم مواقع معروفة.

ثالثا: تعطيل الأجهزة: كثر مؤخراً إرتكاب مثل هذه العمليات، حيث يقوم مرتكبوها بتعطيل أجهزة أو شبكات عن تأدية عملها بدون أن تتم عملية إختراق فعلية لتلك الأجهزة , تتم عملية التعطيل بإرسال عدد هائل من الرسائل بطرق فنية معينة إلى الأجهزة أو الشبكات المراد تعطيلها الأمر الذي يعيقها عن تأدية عملها, من أشهر الأمثلة على هذا النوع من الجرائم تلك التي تقوم بتعطيل الأجهزة المستضيفة للمواقع على الشبكة ؛ إن الأسباب وراء إستهداف هذا النوع من الأجهزة تماثل أسباب استهدافها في جرائم الاختراقات والتي سبق ذكرها جميع الجرائم التي ذكرناها تستهدف بشكل مباشر معلومات أو أجهزة وشبكات حاسبات.

أما جرائم الإنترنت التي تستهدف جهات سواء كانوا أفراداً أو مؤسسات، ففيما يلي عرض لبعضها :

رابعاً: انتحال الشخصية: هي جريمة الألفية الجديدة كما سماها بعض المختصين في أمن المعلومات وذلك نظراً لسرعة إنتشار إرتكابها خاصة في الأوساط التجارية. تتمثل هذه الجريمة في استخدام هوية شخصية أخرى بطريقة غير شرعية، وتهدف إما لغرض الاستفادة من مكانة تلك الهوية (أي هوية الضحية) أو لإخفاء هوية

شخصية المجرم لتسهيل ارتكابه جرائم أخرى, إن إرتكاب هذه الجريمة على شبكة الإنترنت أمر سهل وهذه من أكبر سلبيات الإنترنت الأمنية، وللتغلب على هذه المشكلة، فقد بدأت كثير من المعاملات الحساسة على شبكة الإنترنت كالتجارية في الاعتماد على وسائل متينة لتوثيق الهوية كالتوقيع الرقمي والتي تجعل من الصعب إرتكاب هذه الجريمة.

خامساً: المضايقة والملاحقة: تتم جرائم الملاحقة على شبكة الإنترنت غالباً باستخدام البريد الإلكتروني أو وسائل الحوارات الآنية المختلفة على الشبكة , تشمل الملاحقة رسائل تهديد وتخويف ومضايق ؛ تتفق جرائم الملاحقة على شبكة الإنترنت مع مثيلاتها خارج الشبكة في الأهداف والتي تتمثل في الرغبة في التحكم في الضحية، تتميز جرائم المضايقة والملاحقة على الإنترنت بسهولة إمكانية المجرم في إخفاء هويته علاوة على تعدد وسهولة وسائل الاتصال عبر الشبكة، الأمر الذي ساعد في تفشي هذه الجريمة ؛ من المهم الإشارة إلى أن كون طبيعة جريمة الملاحقة على شبكة الإنترنت لا تتطلب اتصال مادي بين المجرم والضحية لا يعني بأي حال من الأحوال قلة خطورتها فقدرة المجرم على إخفاء هويته تساعده على التمادي في جريمته والتي قد تفضي به إلى تصرفات عنف مادية علاوة على الآثار السلبية النفسية على الضحية.

سادساً: التغرير والاستدراج: غالب ضحايا هذا النوع من الجرائم هم صغار السن من مستخدمي الشبكة ؛ حيث يوهم المجرمون ضحاياهم برغبتهم في تكوين علاقة صداقة على الإنترنت والتي قد تتطور إلى التقاء مادي بين الطرفين, إن مجرمي التغرير والاستدراج على شبكة الإنترنت يمكن لهم أن يتجاوزوا الحدود السياسية فقد يكون المجرم في بلد والضحية في بلد آخر وكون معظم الضحايا هم من صغار السن، فإن كثير من الحوادث لا يتم الإبلاغ عنها حيث لا يدرك كثير من الضحايا أنهم قد ُغرر بهم.

سابعاً: التشهير وتشويه السمعة: يقوم المجرم بنشر معلومات قد تكون سرية أو مضللة أو مغلوطة عن ضحيته، والذي قد يكون فرداً أو مجتمع أو دين أو مؤسسة تجارية أو سياسية. تتعدد الوسائل المستخدمة في هذا النوع من الجرائم، لكن في مقدمة قائمة هذه الوسائل إنشاء موقع على الشبكة يحوي المعلومات المطلوب نشرها أو إرسال هذه المعلومات عبر القوائم البريدية إلى أعداد كبيرة من المستخدمين.

ثامناً: صناعة ونشر الإباحية: لقد وفرت شبكة الإنترنت أكثر الوسائل فعالية وجاذبية لصناعة ونشر الإباحية؛ إن الإنترنت جعلت الإباحية بشتى وسائل عرضها من صور وفيديو وحوارات في متناول الجميع، ولعل هذا يعد أكبر الجوانب السلبية للإنترنت خاصة في مجتمع محافظ على دينه وتقاليده ؛ إن صناعة ونشر الإباحية تعد جريمة في كثير من دول العالم خاصة تلك التي تستهدف أو تستخدم الأطفال ؛ لقد تمت إدانة مجرمين في أكثر من مائتي جريمة في الولايات المتحدة الأمريكية خلال فترة أربع سنوات والتي انتهت في ديسمبر 1998م، تتعلق هذه الجرائم بتغرير الأطفال في أعمال إباحية أو نشر مواقع تعرض مشاهد إباحية لأطفال.

تاسعاً: النصب والاحتيال :أصبحت الإنترنت مجالاً رحباً لمن له سلع أو خدمات تجارية يريد أن يقدمها، وبوسائل غير مسبوقة كاستخدام البريد الإلكتروني أو عرضها على موقع على الشبكة أو عن طريق ساحات الحوار؛ ومن الطبيعي أن ُيساء استخدام هذه الوسائل في عمليات نصب واحتيال ؛ ولعل الذي يستخدم البريد

الإلكتروني بشكل مستمر تصله رسائل بريدية من هذا النوع. إن كثيراً من صور النصب والاحتيال التي يتعرض لها الناس في حياتهم اليومية لها مثيل على شبكة الإنترنت مثل بيع سلع أو خدمات وهمية، أو المساهمة في مشاريع استثمارية وهمية أو سرقة معلومات البطاقات الائتمانية واستخدامها ؛ وتتصدر المزادات العامة على البضائع عمليات النصب والاحتيال على الإنترنت ؛ إن ما يميز عمليات النصب والاحتيال على الإنترنت عن مثيلاتها في الحياة اليومية هي سرعة قدرة مرتكبها على الاختفاء والتلاشي. بعد هذا العرض لعدد من أنواع جرائم الإنترنت.

1-3-4. الفيروســــــــــــــــــــــات[6]:

أصبح الحديث عن الفيروسات من الأمور الطبيعية بل أن الكثير ممن لديهم حاسبات شخصية ربما يكونون قد تعرضوا لأذى تلك الفيروسات إذا ما علمنا أن هناك أكثر من20 ألف فيروس معروف في الوقت الحاضر. ونحاول من خلال هذا العنصر تسليط الضوء على الفيروسات بأنواعها المختلفة وكيفية الوقاية منها عن طريق أشهر برامج الحماية"Antivirus Programs " المجاني منها والتجاري علما بأن الدراسات تقول: أن 40% فقط ممن يستخدمون الحاسبات الشخصية في المكاتب أو المنازل لديهم برامج حماية من الفيروسات، ويأتي حديثنا هذا متصلا لكون الكثير من المستخدمين بدؤوا يلحظون انتشار الفيروسات في الوقت الحاضر خاصة أثناء عملية جلب البرامج DownLoad مثل الألعاب والبرامج المجانية، كما أن الفيروسات يمكن أن تصيب جهازك أثناء قراءتك أو من خلال مرفقات بريدك الالكتروني .

و الفيروس الحاسوبي Computer Virus عبارة عن برنامج Software مخفي لا يمكن رؤيته من خلال برامج الاستعراض كتب بعناية ليكون قادرا على الدخول إلى نظامك الحاسوبي بشكل سري Surreptitiously وقد يُصيبُ بعض ملفاتكَ بالأذى والتخريب أو قد يكتفي بعرض رسالة ما تلبث أن تذهب؛ عموما يمكن القول أن أي برنامج يهدف إلى إلحاق الأذى بأنظمة وملفات الغير يسمى فيروسا، عادة ما يقوم الفيروس بإعادة نفسه (تكرار نفسه Replicate Itself) وإصابة اكبر قدر من الملفات وهنا تكمن الخطورة، وكثيراً ما توصف الفيروسات على أنها سريعة الانتشار أي أنها تنتقل من نظام أو وسط تخزيني لآخر بسرعة كبيرة. على سبيل المثال لنفترض أن حاسبا شخصيا مصاباً بفيروس من الفيروسات ثم قمت بحفظ بعض الملفات من ذلك الجهاز إلى قرص مرن أو قرص CD أو أرسلت منه ملفاً عبر البريد الالكتروني أو عبر برامج الاتصال مثل ICQ فإن الجهاز المستقبل سيصاب بذلك الفيروس وهكذا تتسع دائرة الإصابة إلا إذا تم القضاء على ذلك الفيروس بواسطة أحد برامج الحماية القوية.

أنواع الفيروسات

تظل حرب الفيروسات مستعرة ودائما ما توصف بأنها الحرب التي لا يمكن أن تقف بل أن إتهامات

---

[6]- **فيروسات الحاسب أنماطها وأعراضها وطرق الوقاية منها**. [على الخط المباشر].زيارة يوم 2006/02/12:.متوفر على الموقع:**http://www.al-jazirah.com.sa/services**

تقول أن الشركات المنتجة للبرامج وحفاظا على حقوقها تقوم بصنع فيروسات تظهر فور استخدام نسخ غير أصلية من تلك البرامج، وهذا الكلام لا يستطيع أحد أن يثبت صحته من عدمها لكن الفيروسات موجودة ويجب علينا كمستخدمين للحاسبات أن نقي أنفسنا من شرورها وأضرارها وحتى نفعل ذلك يجب أن نعرف أنواعها حيث إشتهرت منها أربعة أنواع هي على النحو التالي :

- فيروسات قطاع إعادة التحميل Boot sector viruses
- فيروسات البرامج أو الملفات Program Or File Viruses
- فيروسات الماكرو Macro Viruses
- فيروسات متعددة الأطراف Multipartite Viruses

وتسبب الفيروسات في عدة أعراض تتراوح من كونها مجرد رسالة أو عدة رسائل تظهر فجأة ثم سرعان ما تختفي أو أن تقوم بحذف بعض البرامج أو حذف قطاع التحميل أو تدمير كامل القرص الصلب وبالتالي تخسر كل المعلومات والبرامج التي به.

- ظهور رسائل غريبة على شاشة حاسوب، آو أصوات غريبة أو موسيقى صاخبة تنبعث من الجهاز في أوقات متفرقة .
- كثرة ظهور رسائل انتهاء الذاكرة Run Out of Memory أو المساحة التخزينة.
- تغيير إسم الجهاز .
- عدم وجود تطبيقات كانت في السابق تعمل بالجهاز.
- بطء الحاسب الآلي عن السرعة المعتادة .
- بطء الحاسب في أداء بعض المهمات البسيطة كان يأخذ وقتا طويلا في عملية حفظ وثيقة عبارة عن سطرين أو ثلاثة.

1-3-4. أمن المعلومـــــــــات:

إن شبكة الإنترنت كشبكة معلوماتية ينطبق عليها النموذج المعروف لأمن المعلومات ذو الأبعاد الثلاثة وهي:

1. سرية المعلومات: وذلك يعني ضمان حفظ المعلومات المخزنة في أجهزة الحاسبات أو المنقولة عبر الشبكة وعدم الإطلاع عليها إلا من قبل الأشخاص المخولين بذلك.

2. سلامة المعلومات: يتمثل ذلك في ضمان عدم تغيير المعلومات المخزنة على أجهزة الحاسب أو المنقولة عبر الشبكة إلا من قبل الأشخاص المخولين بذلك.

3 .وجود المعلومات: وذلك يتمثل في عدم حذف المعلومات المخزنة على أجهزة الحاسب إلا من قبل الأشخاص المخولين بذلك.

إن جرائم الإنترنت ليست محصورة في هذا النموذج، بل ظهرت جرائم لها صور أخرى متعددة تختلف باختلاف الهدف المباشر في الجريمة. إن أهم الأهداف المقصودة في تلك الجرائم هي كالتالي:

1. المعلومات: يشمل ذلك سرقة أو تغيير أو حذف المعلومات، ويرتبط هذا الهدف بشكل مباشر بالنموذج الذي سبق ذكره.

2 .الأجهزة: ويشمل ذلك تعطيلها أو تخريبها.

3. الأشخاص أو الجهات: تهدف فئة كبيرة من الجرائم على شبكة الإنترنت أشخاص أو جهات بشكل مباشر كالتهديد أو الابتزاز؛ علماً بأن الجرائم التي تكون أهدافها المباشرة هي المعلومات أو الأجهزة تهدف بشكل غير مباشر إلى الأشخاص المعنيين أو الجهات المعنية بتلك المعلومات أو الأجهزة. بقي أن نذكر أن هناك جرائم متعلقة بالإنترنت تشترك في طبيعتها مع جرائم التخريب أو السرقة التقليدية، كأن يقوم المجرمون بسرقة أجهزة الحاسب المرتبطة بالإنترنت أو تدميرها مباشرة أو تدمير وسائل الاتصال كالأسلاك والأطباق الفضائية وغيرها. حيث يستخدم المجرمون أسلحة تقليدية إبتداء من المشارط والسكاكين وحتى عبوات متفجرة، وكمثال لهذا الصنف من الجرائم قام مشغل أجهزة في إحدى الشركات الأمريكية بصب بترين على أجهزة شركة منافسة وذلك لإحراقها حيث دمر مركز الحاسب الآلي الخاص بتلك الشركة المنافسة برمتها[7].

أصبحت قضية الأمن، التي تؤرق العالم؛ شرقه وغربه، الهم الأكبر والشغل الشاغل للمتعاملين مع الشبكة العنكبوتية العالمية " الإنترنت "، سواء أكانوا أفرادا أم مؤسسات أم مجموعات ــ groups. وبات المتعاملون مع الشبكة العنكبوتية يخشون عمليات القرصنة على معلوماتهم وتعاملاتهم وحساباتهم المصرفية، وكل ما يرسلونه أو يستقبلونه على هذه الشبكة العنكبوتية. حتى أن عمليات القرصنة هذه، التي تقوم بها مجموعات "الهاكرز"، جزءا من الأمن القومي في معظم دول العالم، وخصوصاً تلك الدول الكبرى التي تستضيف خوادم الإنترنت ــ servers ــ حتى إن رئيس الوزراء البريطاني "توني بلير" اعتبرها من أكثر الجرائم التي تهدد الأمن القومي البريطاني؛ نظراً لصعوبة تعقّب مرتكبيها.

وأصبحت الحقيقة المؤكدة التي لاشك فيها في هذا المجال، هي: أن القراصنة أو " الهاكرز "، قد لجأوا إلى اختراع برامج وطرق جديدة معقدة جداً، من شأنها تمكينهم من اختراق الشبكات والأجهزة مهما تكون حمايتها، ومهما تكون تعقيدات الاحتياطات الأمنية التي تقوم بها الشركات الكبرى؛ لحماية معلوماتها وقواعد البيانات الخاصة بها. وتختلف برامج التجسس في المميزات وطرق الاستخدام، ولكن الطرق التقليدية التي يستعملها "الهاكرز" المبتدئون جميعاً، تعتمد على فكرة واحدة، وهي ما سُمي بـــ"الملف اللاصق" " file patch"، الذي يرسله المتجسس إلى جهاز الضحية، عن طريق البريد الإلكتروني، أو برامج المحادثة، فيقوم

---

[7] – الهاجري, إياس. **جرائم الإنترنت**. [على الخط المباشر].زيارة يوم :2006/02/12.متوفر على الموقع: http://www.egovs.com/egovs_webo2/news

الضحية المستخدم بفتحه بحسن نية، دون دراية منه أنه قام في الوقت نفسه بفتح الباب على مصراعيه للمتجسس؛ ليفعل ما يريد بجهازه [8].

[8] –عبد الله، إسلام. **الحماية من فيروسات الإنترنت ضرب من الخيال**. [على الخط المباشر]. زيارة يوم 2006/02/12:. متوفر على الموقع: http://www.aljesr.nl/map.htm

الفصل الثاني

أساسيات شبكات المعلومات

عندما تحدثت تقارير 1989 عن أول فيروس كمبيوتر خيل للكثيرين من بينهم خبراء في مجال الإعلام الآلي أن ذلك مجرد خرافة ابتدعها أحد كتاب قصص الخيال العلمي, وأن وسائل الإعلام تحاول ترسيخها في أذهان الناس كحقيقة رغم أنها لا تمت إلى الواقع بصلة ، ولقد امتدت تلك الظاهرة واتسعت حتى باتت تشكل خطرا حقيقيا يهدد ثورة المعلوماتية التي فجرتها التقنيات الحديثة؛ فمن بضع فيروسات تعد على الأصابع في السنة الأولى إلى عدد يقدر بالملايين في يومنا هذا، وفي كل يوم تكتشف أنواع جديدة من الفيروسات المختلفة التأثير والشراسة ، ومن الفيروسات البسيطة إلى الفيروسات المكارة والذكية التي تتفنن في التغير والتخفي والتحول؛ ترى ما حقيقة هذا الوباء وإلى أي حد يشكل خطرا على بنية المعلومات الكونية ؟ هذا ما س أجيب عليه في هذا الفصل.

4-1. الفيروسات: الماهية

تعد الفيروسات الوباء الأول الذي يهدد البيئة الإلكترونية وفي ما يلي أهم أبجديات هذا العالم:

4-1-1. ماذا نعني بالفيروس:

4-1-1-1. ندة تاريخية عن الفيروسات:

إستسقى مصطلح فيروس من العلوم البيولوجية وهو يعني باللاتينية «سم" وكان أول ظهور معروف لفيروس الكمبيوتر عام 1981 حيث كان بغرض علمي كما يقول المؤرخون و يعتبر البذرة الأولى التي أثمرة لتشكل شجرة الفيروسات الحالية؛ وكان الفيروس ينشر عن طريق الأقراص المرنة و يعمل على نظام (أبل **APPLE 2**) يكتفي هذا الفيروس بإظهار مقطع شعري على شاشة الحاسب دون أن يقوم بأية عملية تخريبية أو تدميرية على النظام.

أما عام 1983 في شهر نوفمبر بالتحديد كانت أول تجربة علمية مسجلة لفيروس وتم تقديمها في مؤتمر أمني خاص بالحاسب الآلي وكان الفيروس يعمل على نظام اليونكس في ذلك الوقت.

أما أول ظهور لفيروس ينتقل عن طريق الأقراص المرنة في نظام الدوس فكان الأصل فيه كما يقال يعود لأخوين في باكستان استطاعا تحليل الجزء المشغل في القرص ، ومن تم قاما بتطوير طريقة عبقرية لإصابته بالفيروس وأطلقا عليه المخ (**BRAIN**)؛ وفي نفس العام شهد العالم الحاسوبي أول ملف تجسس انتقل عن طريق برنامج مجاني يدعى **PC.WRITE** ؛ كما شهد هذا العام ظهور فيروس **VIRDEM** المدمر لكن هذا الأمر ليس تابت بشكل قطعي.

1987 أول ظهور لفيروسات تستهدف ملفات التشغيل **EXE.COM** التي كان نظام الدوس يعتمد عليها بشكل كلي وهو نفس العام الذي شهد انطلاق فيروس "القدس " الذي امتد حول العالم ليشكل أول تهديد فعلي للحاسبات ؛ ثم ظهور أول دودة الأنترنيت **IBM** مسماة دودة الكريسماس والتي كانت تعيد نسخ نفسها 500ألف مرة بالساعة.

1988 ظهور فيروس يدعى الماك ماج **MAC MAG** ومن ثم إنشاء منظمة السيرت **www.cirt.org** لمواجهة أخطار الفيروسات والديدان بعد أن تسببت دودة موريس في إغلاق الكثير من الأجهزة على الأنترنت[9].

الأعوام التالية شهدت ظهور العديد من الفيروسات إلا أن عام 1990 شهد ظهور تنافس تطوير الفيروسات بين المبرمجين ونشرها على الأنترنت.

في عام 1995 ظهر فيروس الماكرو والذي يستهدف برنامج الورد

1996 بروز فيروسات خصيصا لمهاجمة أنظمة تشغيل الوندوز 95

1998 ظهور أو فيروس جافا في العالم، وفي 1999 انفتحت نافذة الجحيم على الأنترنت وبدأ عصر جديد من التهديدات ابتدأها فيروس ملسا الذي جمع بين فيروس الماكرو ودودة الأنترنت والذي تسبب في تعطيل الكثير من الخوادم لكبريات الشركات.

وفي الأعوام التالية ظهرت العديد من الفيروسات التي تسببت بخسائر تقدر بملايير الدولارات و لم تكن بالضرورة بنفس الطبيعة إلا أنها اتفقت جميعا على كونها الخطر الأكبر الذي يهدد الحاسبات.

2000 اكتشاف فيروس وينوكس والذي استهدف منصات تشغيل الويندوز ولسنكس معا ليكون الأول من نوعه في هذا المجال[10].

4-1-1-2. تعريف الفيروس:

وهنا يمكن إيراد عدة تعاريف نذكر منها:

1- برنامج صغير ولكن خبيث طور خصيصا لتنفيذ أعمال تخريبية علي الحاسب الآلي يحتوي هذا النوع من البرامج في معظم الأحيان علي أوامر تخريبية معينة في نص الشفرة وتختلف التي تكتب بها وتنفذ عند تحقيق شروط معينة وتختلف طرق الإصابة بالفيروسات فمنها ما ينسخ نفسه داخل ملفات ذات هيئة معينة ومتوافقة مع ما هو مصمم له وكلما تم استدعاء هذه الملفات أو تشغيلها ويتحقق بالبيئة المحيطة

---

2 – الجنبيهي ,منير محمد ؛ الجنبيهي , ممدوح محمد. **أمن المعلومات الإلكترونية**.الإسكندرية:دار الفكر الجامعي , 2005.صص48-49.

[9]

[10]– الجنبيهي ,منير محمد ؛ الجنبيهي , ممدوح محمد. لأمن المعلومات الإلكترونية.المرجع السابق. ض.50.

ومن هذه البرامج الخبيثة ما ينسخ نفسه في الذاكرة مما يؤدي إلى بطئ شديد في عمل الجهاز ومنها ما يقوم بتخريب نظام الإدخال والإخراج الأساسي في الوقت الذي تزداد فيه خبرة وذكاء مؤلفي (مصممي) الفيروسات وبالتالي زيادة عدد الفيروسات وأنواعها يتم تطويرها في تقنيات مكافحة تلك الفيروسات للتصدي لها وإزالتها قبل حدوث أي الضرر [11].

2- كما يعرف أيضا بأنه برنامج حاسب مثل أي برنامج تطبيقي آخر ولكن يتم تصميمه بواسطة أحد المخربين لهدف محدد هو إحداث أكبر ضرر ممكن بنظام الحاسب ولتنفيذ ذلك يتم إعطائه القدرة على ربط نفسه ببرامج آخرى وكذلك إعادة إنشاء نفسه حتى يبدو أنه يتكاثر ويتوالد ذاتيا وهذا يتيح له قدرة كبيرة على الإنشار بين البرامج المختلفة وكذلك بين المواقع المختلفة في الذاكرة حتى يحقق أهدافه التدميرية كما أن إنتشار الفيروس لا يقتصر على النظام الذي يتواجد به ولكنه ينتقل أيضا إلى نظم أخرى قد تكون أبعد مسافة ممكنة على هذا النظام ويعود هذا الإنتشار إلى عاملين أساسيين هما:

أ- التوافق: وهو يعني قدرة البرامج الواحد على التشغيل على أنواع مختلفة من الحواسب وإصدارات مختلفة من نظم التشغيل وهذا العامل رغم تأثيره الإيجابي والهام بالنسبة لتطوير النظم أن أثره على إنتشار الفيروس كان كبير.

ب – وسائل الإتصال:

وهي الوسائل التي أدت إلى ربط عدد من أجهزة الحاسب بشبكة الأن ترنيت و اتصالهم من خلالها وهذه الأجهزة قد تكون في نفس الوقع وقد تكون في مواقع مختلفة [12]

4-1-1-3. لماذا سمي بالفيروس[13]:

تطلق كلمة الفيروس أساسا على الفيروسات التي تنقل الأمراض عن طريق انتقالها من إنسان مريض إلى إنسان آخر وبمجرد انتقالها إلى الإنسان تتكاثر حتى تصيب الأجهزة العضوية.

والفيروس الخاص بالحاسب يقوم بعمل مشابه لذلك ، حيث أنه عبارة عن برنامج يصممه بعض المتخصصين لأهداف تخريبية مع إعطائه القدرة على ربط نفسه ببرامج أخرى ثم يتكاثر وينتشر داخل النظام حتى يتسبب في تدمير هاما؛ وهناك أوجه تشابه متعددة بين الفيروس العضوي وفيروس الحاسب يمكن تلخيصها في ما يلي:

---

1 – الربيعي ,محمد,شعبان أحمد أحمد ,وآخرون. المعجم الشامل لمصطلحات الحاسب الآلي ة الأنترنت.مكتبة السيكان الرياض 2001ص 446

1- طلية.محمد فهمي المرجع السابق ص.34.

[13]– – طلية. محمد فهمي.؛ عبد الوهاب، مصطفى رضا....وآخرون .فيروسات الحاسب وأمن البيانات، 1996.موسوعة دلتا كمبيوتر 8

- يقوم الفيروس العضوي بتغيير الخصائص العضوية لخلايا الجسم ويقوم فيروس الحاسب بتغيير وظائف برامج لأخرى.

- يتكاثر الفيروس العضوي ويتسبب في أنتاج فيروسات جديدة ويقوم فيروس الحاسب بإعادة إنشاء نفسه.

- الخلية التي تصاب بالفيروس العضوي لا تصاب بنسف الفيروس مرة ثانية وتحدث نفس الشيء مع الفيروس حيث يقوم باختيار البرنامج المطلوب نقل العدوى فإن وجد أنه سبق إصابته به لا يصيبه مرة ثانية وينتقل إلى برامج أخرى

- الجسم الذي تنتقل إليه العدوى قد يظل مدة طويلة دون ظهور أعراض المرض عليه ويقوم برنامج الحاسب بأداء وظائفها لمدة طويلة دون ظهور أخطاء نتيجة وجود الفيروس

- من ذلك ينضح سبب إطلاق تسمية الفيروس رغم أنه في الحقيقة ليس إلا برنامج مثل البرامج الحاسب ولكنه يختلف عنه في الوظائف التدميرية.

4-1-2. خصائص الفيروس:

كما سبق ذكره فإن الفيروس هو برنامج له صفات التكاثر والمضاعفة والاختفاء أو التخفي والإننفجار وعلى هذا الأساس يمكن ذكر أهم الخصائص التي يميز بها الفيروس في ما يلي:

4-1-2-1- القدرة على الاختفاء:

فالفيروس ما هو إلا برنامج أو القدرة على الاختفاء عن المستخدم والتمويه غليه وهو يستخدم وسائل متعددة في الاختفاء ومنها الارتباط بالبرامج الشائعة الاستعمال حيث أن مستخدم للحاسب الشخصي يهتم بتوفير البرامج التي تمكنه من الاستفادة من خصائص الحاسب؛ وبعض المستخدمين يقوم بنسخ هذه البرامج دون السؤال عن مصدرها وعند تشغيلها ينتقل الفيروس إلى القرص ويقوم بأعماله التدميرية ؛ وهناك فيروسات تدخل إلى الحاسب كملفات متخفية بحيث لا يستطيع المستخدم ملاحظة تواجدها عن طريق فهرس الملفات وهناك بعضا منها يستقر في أماكن معينة حيث يصعب العثور عليها ثم تبرمج على تاريخ معين ثم تقوم بتنفيذ وتشغيل نفسها في هذا التاريخ , وهناك أنماط أخرى من الفيروسات تقوم بإخفاء أي أثر على تواجدها حيث تظل البرامج المصابة تعمل بكفاءة دون أخطاء مدة طويلة بينما يقوم هو بالإنتقال من برنامج إلى آخر بخفة [14].

1 – الرومي , محمد أمين. جرائم الكمبيوتر والأنترنت. الإسكندرية: دار المطبوعات الجامعية ,2003.ص.28

4-1-2-2. الانتشار:

يتميز فيروس الحاسب بقدرة كبيرة على الإنتشار ومن أهم الوسائل التي تساعد على ذلك إنتشار وسائل الإتصال الحديثة التي تجعل الفيروس ينتقل بسرعة من حاسب إلى آخر شبكة الأنترنت إلى ملايين المستعملين وكذلك توافق الأجهزة الذي يساعد الفيروس على العمل وإذا قارنا بين إنتشار الفيروس العضوي وفيروس الحاسب نجد أن هذا الأخير أسرع إنتشار بدرجة كبيرة حيث يمكنه في ثوان محدودة الإنتقال من قارة إلى أخرى كما يمكنه الإنتقال إلى عدد ضخم من المستخدمين في نفس الوقت بينما لا يستطيع الفيروس العضوي فعل ذلك وعند انتقال الفيروس إلى الحاسب فإنه ينتشر بسرعة كبيرة داخل الذاكرة حيث أنه يربط نفسه بالبرامج المخزنة داخل الذاكرة كما يقوم بعمل نسخ كبيرة لنفسه [15].

3- القدرة على الإختراق:

يتميز فيروس الحاسب بقدر ة كبيرة على الدخول والتسلل واختراق الحصون والمواقع التي يقيمها المستخدم بتحميل هذه البرامج حيث يكون الفيروس عادة موجودا في احد البرامج المفيدة التي يحتاجها المستخدم لتشغيل الحاسب ثم يقوم المستخدم بتحميل هذه البرامج وإدخال الفيروس دون أن يشعر وبعض الفيروسات يتم إدخالها بإستخدام حصان طروادة حيث يرتبط بأحد البرامج المثيرة التي تجدب المستخدم وتثير لديه حب الإطلاع وعند تحميل هذه البرامج يبدأ الفيروس في الإنتشار وتنفيذ عملياته التدميرية [16]

4- القدرة على التدمير:

عندما يدخل الفيروس إلى الكمبيوتر يظل ساكنا حتى تبدأ لحظة الصفر التي يبدأ عندها في الإنتشار والحركة وساعة الصفر هذه إما أن تكون كلمة معينة كتبها المستخدم أو إشارة معينة أو عند تاريخ معين ويعمل الفيروس غالبا على محور البيانات المخزنة في الذاكرة[17]

4-1-3. دورة حياة الفيروسات وانتشارها:

4-1-3-1. . دورة حياة الفيروس[18]:

وهناك سقمراحل لدورة حياة فيروس الكمبيوتر تتمثل في:

1- مرحلة التصميم

2- طلية.محمد فهمي المرجع السابق ص 64

1- طلية.محمد فهمي المرجع السابق ص 64

17

[18]- دورة حياة الفيروس (على الخط المباشر).(14-12-2006) متوفر على الخط المباشر
http// www.jparisnajd.com /

عملية تصميم فيروس جديد تحتاج إلى شخص على درجة عالية من الكفاءة في التعامل مع لغات البرمجة على الحاسب الشخصي مثل لغة البيسك والجافا والفيجوال **c++**

وقد لا تبح هذه الخبرات والكفاءات ضرورية في المستقبل حيث يتم تقديم مساعدات كبيرة على مستوى شبكة الأنترنيت للمبرمجين المبتدئين الذين يردون القيام بتصميمات

2-مرحلة الإنتشار:

عادة ما يقوم مطورو الفيروسات بنشر فيروساتهم على أكبر عدد من الحواسب الشخصية قبل أن يبدأ الفيروس بإحداث الآثار التدميرية المكلف بها والسبب في ذلك وهو نشر أكبر عدد من النسخ قبل أن تنتبه شركات مقاومة الفيروسات لوجوده فتبدأ بوضع البرامج المضادة لها وفي هذه المرحلة تصل الفيروسات إلى الحاسبات وتظل بها دون أن تظهر أية أعراض على الحاسبات المصابة.

3- مرحلة النشاط:

تبدأ الفيروسات في النشاط ولإحداث الآثار التدميرية التي تمت برمجتها للقيام بها عند وقوع حدث معين وقد تتم برمجته لكي ينشط في توقيت معين أو عند تشغيل برنامج ما أو عند الإتصال بشبكة الأن ترنيت أو عند وصول جزء ثان من الفيروس إلى الحاسب وتنوع الأعمال التخريبية من تدمير الملفات المخزنة على الحاسب أو استهلاك المساحات ووحدة التخزين

4- مرحلة اكتشاف الفيروس:

قد لا تتبع هذه الخطوة دائما عملية نشاط الفيروس فقد تكون الشركات المنتجة لبرامج مقاومة الفيروسات أكثر ذكاء بحيث تكتشف وجود الفيروس قبل أن ينشط ومن تم العمل على مقاومته.

5 – مرحلة المواجهة:

في هذه المرحلة تقوم شركات إنتاج برامج مقاومة الفيروسات تعديل برامجها وملفاتها لكي تتعامل مع الفيروس الجديد ولكل فيروس بصمة خاصة به وهي (الكود الذي تكتب به أوامر الفيروس بأحد لغات الحاسب) ويتم إضافة هذه البصمة إلى ملفات البرامج بعد ذلك يقوم المستخدمون بتويل الملفات على موقع الشركة على شبكة ويقومون بتحدث البرامج بعد التعديل. هذه المرحلة قد تصل إلى ستة أشهر حسب نوع الفيروس

6- مرحلة الإستئصال:

بعد فترة من القيام بعدد كبير من حديث برامجهم ,تنحصر آثار الفيروس بالتعديلات التي تكتشف وتقضي على الفيروس بحيث تنخفض درجة تهديده لمجتمع المعلومات

4-1-3-2. عوامل إنتشار الفيروسات[19]:

هناك العديد من العوامل التي تقف وراء الإنتشار الكبير للفيروسات في هذه الأيام وهذه العوامل لخصها التقرير الذي قدم إلى مجلس بحوث أمن المعلومات في الولايات المتحدة فيما يلي:

1 إنتشار الشبكات:

بازدياد ارتباط الحاسبات ببعضها من خلال شبكة الأنترنت ازدادت سهولة شن الهجمات كما ازداد عدد هذه الهجمات تبعا لذلك وأصبح من النادر اليوم أن نرى جهاز حاسب غير مرتبط بشبكة الأنترنت ويدعم ذلك الاتجاه ما نشهده من الاعتماد المتزايد لدى الأفراد والشركات على البريد الإلكتروني كوسيلة اتصال وتواصل وباختصار شديد فإن مهاجم اليوم لا يحتاج إلى الوصول المباشر إلى جهاز الحاسب لزرع فيروسه كما ساعد انتشار الشبكات على شن أنواع آلية من الهجوم لا يتدخل فيها البشر وقد حدث في فيبراير 2000 هجوم تسبب في عرقلة الخدمة في العديد من مواقع التجارة الإلكترونية

2 زيادة تعقيد النظم

بازدياد حجم نظم المعلومات ودرجة تعقيدها زاد إعتمادها على نظم التشغيل في توفير الحماية الأمنية لها ونظم التشغيل نفسها تضم آلاف من البرامج التي تحتوي على عشرات الملايين من الأوامر وفي نظم بهذا الحجم لا يمكن تفادي الثغرات ,وزاد تفاقم المشكلة استخدام لغات لا تتمتع بالحماية الأمنية مثل لغة **c++** التي لا تقاوم أبسط أنواع الهجوم

ومن جهة أخرى فإن التطبيقات الضخمة المعقدة تشكل بيئة صالحة لنمو الفيروسات فلا يلحظ وجودها أحد , فقد نستطيع فحص برنامج صغير وتأكيد نظافته وخلوته من الفيروسات ولكن من المستحيل عمل ذلك في تطبيقات اليوم التي تملأ حياتنا الشخصية ناهيك عن التطبيقات الضخمة التي تعمل في الشركات والدوائر الحكومية

3- سهولة الإضافة إلى النظم:

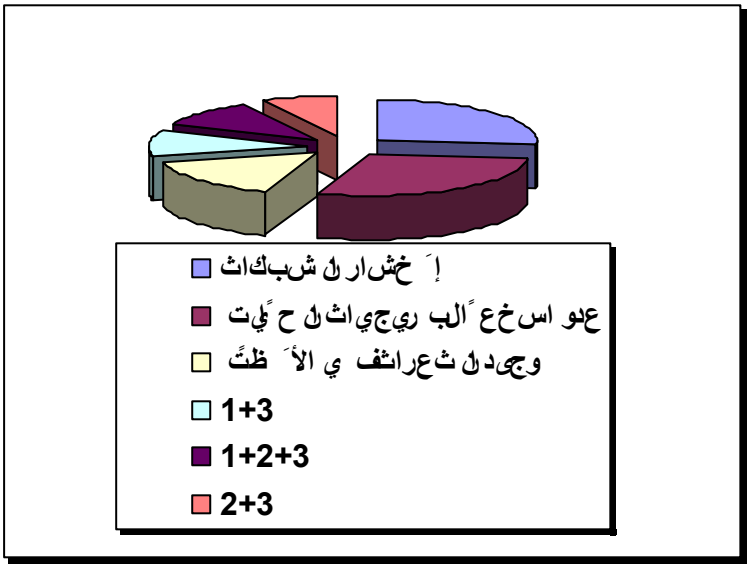
تفخر الكثير من نظم المعلومات اليوم بأنها نظم قابلة للتوسع بمعنى أنها تقبل التحديث والإضافة سواء من جانب المحدد أو المستخدم وتأتي هذه الإضافات بشكل برامج منقولة ولذلك فُن مع ظم البرمجيات ونظم التشغيل الحالية تجدها قابلة للتوسع مما سهل اقتحام الفيروسات وأوضح مثال على ذلك الكيفية التي انتشر بها فيروس (ميلسا) حيث استغل قابلية البرنامج الإلكتروني (أوت لوك) **oritlook** لتوسع فقد تم كتابة الفيروس في صورة رسالة إنخد بها معظم المستخدمين.

---

[19]- أمن شبكات المعلومات ص 167

إذن وكما سبق الإشارة إليه فإن البيئة الإلكترونية أدت إلى قلب العديد من الأمور؛ حيث ظهرت العديد من الإفرازات منها ما هو سلبي ومنها ما هو إيجابي، وتعد الفيروسات واحدة من أبرز الإفرازات السلبية وقد ساهم في انتشاره هذه الأوبئة عدة أمور موضحة في الجدول رقم **15** الصفحة 144

وفقد أعرب الطلبة على أنه ومهما اختلفت الأسباب التي تؤدي إلى إنتشار الفيروسات بشكل رهيب فإن أهمها على الإطلاق هو عدم استعمال برمجيات الحماية بنسبة (28,9 %) وذلك على الرغم كمن الأهمية التي تكتسيها هذه البرمجيات، ثم يليها إنتشار الشبكات بنسبة (26,3 %)، حيث أن الشبكات اكتسحت العالم المعاصر مما جعلها تشكل مناخا ملائما لنمو وتطور الفيروسات، كما أدى ظهور الشبكة العنكبوتية إلى استعمالها كناقل ممتاز لنشر هذه الفيروسات؛ ومن أهم أسباب انتشارها كذلك وجود ثغرات كثيرة في الحاسب وأنظمة التشغيل وهذا ما عبر عنه (17,7 %) من العينة، كما تشكل هذه الأسباب إذا توفرت جميعها لأكبر وأحسن بيئة لالتهاب الشبكة بهذه الفيروسات وهذا ما يوضحه الشكل البياني التالي:



الشكل رقم :11 أسباب إنتشار الشبكات

4-1-3-3. وسائل إنتقال الفيروس[20]:

يمكن لفيروس الحاسب الإنتقال داخل شبكة الإنترنيت أو أي شبكة محلية عن طريق وسائل أربعة:

1- البريد الإلكتروني:

ينتقل الفيروس عبر برنامج أوت لوك وأوت لوك اكيبريس وذلك عن طريق ملف يلصق بالرسالة التي ترد عبر البريد الإلكتروني ويحمل ملف إسم **REACLM EXE** وتظهر له أيقونة بقوته **ATML** وذلك في

[20]- حجارى , عبد الفتاح بيومي. النظام القانوني لحماية الحكومة الإلكتورنية. الكتاب الثاني و الجنائية المعلوماتية لنظام الحكومة الإلكترونية. الإسكندرية:دار الفكر الجامعي 2003 ص ص 74 - 78

محاولة لخداع المستخدم ويكفي قيام المستخدم بالنقر على الملف حتى ينسخ الفيروس نفسه و يمد رسالة تلقائية ترسل إلى جميع العناوين الخاصة بالبريد الإلكتروني التي توجد في دفتر عناوين المستخدم.

2- مزود ويب ISS

يضع الفيروس عناوين عديدة بشكل ؟؟؟؟؟ لما يفعله فيروس **CODERED** بحثا عن مزودات **ISS**والتي تتضمن ثغرات أمنية يستفيد منها في عملية الإنشار ويحاول الفيروس كذلك الاستفادة من دودة فيروس**CODERED2** التي تنتشر عبر مزود **ISS** حيث كانت الدودة تترك برنامج باب خلفي في هذه المزودات كي تسمح للمخترق بالدخول إليها والسيطرة عليها فيما بعد

3- متصفح الأنترنت:

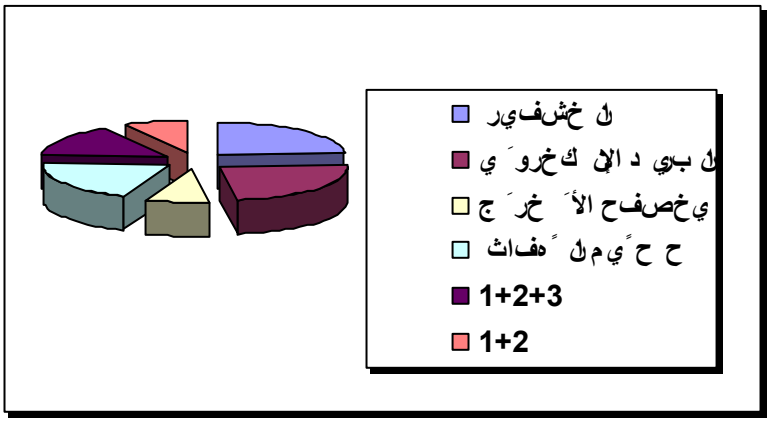
بعد أن يصيب الفيروس أحد المزودات – شبكة الأنترنيت – بالطريقتين السابقتين بنسخ شفرة معينة إلى كل صفحات (**asp- htmail- htm**) التي توجد في المواقع التي يستضيفها مزود -الأنترنيت – وعند زيارة الموقع المصاب من طرف أحد المستخدمين ويبد أفي تتزيل ملف منه يشتعل الفيروس تلقائيا ويصيب جهاز المستخدم

4- المشاركة على الملفات:

تسمح هذه الطريقة للفيروس أن ينتشر عبر الشبكات المحلية التيوجدت ملفات أو مجلدات مشتركة عبر شبكة ميكروسوفت .

وكما سبق الإشارة إليه فإن الفيروسات تنتشر بعدة طرق أهمها البريد الإلكتروني وكذا تحميل الملفات من الأنترنت والجدول 16 الصفحة 144 بوضح ذلك

ترى عينة الدراسة أن أهم طرق انتشار الفيروسات هي البريد الإلكتروني (31,5 %)،فمع إنتشار شبكة الانترنت أصبح البريد الإلكتروني الخدمة الأكثر شعبية والتي أدت إلى زيادة استخدام الشبكة وقد استغل صناع الفيروسات هذه الخدمة من أجل نشر سمومهم على الشبكة، كما يمكن أن يؤدي تحميل الملفات من الأنترنت خصوصا من المواقع المشبوهة إلى المساهمة في إنتشار هذه الأوبئة وهذا ما عبرت عنه (26,5 %) من عينة الدراسة إضافة على العديد من الطرق الأخرى كمتصفح الأنترنت ونوضح ما سبق ذكره بشكل أفضل بالرسم البياني التالي:



الشكل رقم: 12 طرق نشر الفيروسات

4-2. أنواع الفيروسات وأشكالها:

4-2-1. أنواع الفيروسات

إن الفيروسات مهما أختلف شكلها أو نوعها خاصة واحدة هي إلحاق الأدى والضرر بالبرامج إلي برمجت لإلحاق الأذى بها ويمكن أن نميز العديد من أنواع الفيروسات:

4-2-1-1. قطاع التشغيل bootseetor :

وتعتبر من أقدم الفيروسات وأكثرها إنتشار إذ تستطيع أن تصيب المقطع التشغيلي في الأقراص المرنة أو مقطع نظام تشغيل الدوس **dos** حيث أن كل الأقراص سواء كانت صلبة أو مرنة تملك قطاع تشغيل ويتكون من المعلومات الخاصة بشكل القرص (نوع البنية , نوع المعطيات) وتكمن خطورة هذه الفيروسات في قدرتها على إتلاف هذا الجزء ثم يقوم بأحد مكان قطاع تشغيل القرص المصاب بنسخة منه ثم ينقل المقطع الأصلي إلى مكان آخر في القرص [21] .

4-2-1-2. فيروسات الملفات:

وهي الفيروسات التي تلصق نفسها مع ملفات البرامج التنفيدية ذات الإمتداد **com exe** وقد يمتد أثرها ليصيب الملفات ذات الإمتداد **ouc , dry ,sys**.....ومع هذا النوع من الفيروسات فإن البرامج تصاب بمجرد بدأ تشغيل هذه الرمج[22] ويمكن تقسيم هذه الفيروسات إلى أربغة أنواع[23]:

---

[21] -**types des virus informatique.(**en ligne) (23/02/2006)
fr escpotting.com/ seardr/ riduchon.html www.affiliate

[2] - المرجع السابق

3 – شوقي , حسام المرجع السابق ص10

أ- الفيروسات المتطفلة:

التي تلصق نفسها بالملفات لكي تتكاثر وتبقي الملف الأصلي بحالة سليمة

ب- الفيروسات المرافقة:

التي تعتمد على قاعدة الأسبقية في التنفيد للملفات ذات الإمتداد **com** وتتمكن من نقل العدوى عن طريق إنشاء ملف جديد بدون ؟؟؟؟؟ الملف

ج- الفيروسات الرابطة:

وهي التي تصيب البرامج بتغيير المعلومات في جدول مواقع الملفات

د- الفيروسات المستبدلة:

التي تقوم بالكتابة فوق جزء من برنامج دون تغيير حجم الملف مما يؤدي إلى فشل الملف عند تنفيذه.

4-2-1-2. الفيروسات متعددة القدرة التحويلية:

وهذه الفيروسات لها القدرة الديناميكية على وتنفيذ الشفرات عند الإنتقال من ملف إلى آخر لكي يصعب اكتشافها [24].

4-2-1-4. فيروس الماكرو:

هذا النوع أيضا سريع الإنتشار بين المستخدمين خاصة أنه قادر على كل الطرق كالأقراص الصلبة والبريد الإلكتروني والبرامج المجانية ويعتبر من أحد أنواع الفيروسات والجدير بالذكر وهذا الفيروس لا يصيب إلا البرنامج التطبيقي الذي صمم لإتلافه فمثلا لو إن فيروس صمم ليصيب برنامج تحرير الكلمات والنصوص فإنهلا يستطيع إلحاق الأذى بأي برنامج آخر[25].

4-2-1-5. الفيروسات قطاع الإقلاع:

تستقر هذه النوعية من الفيروسات في الأماكن التي يقرأها الكمبيوتر بالقرص الصلب وينفد التعليمات المخزنة ضمنها عند الإقلاع ثم تصيب قطاع الإقلاع الخاصة بنظام الدوس بينما تصيب فيروسات الفئة الفرعية المسماة **MBR virus** قطاع الإقلاع الرئيسي للكومبيوتر كما يمكن أن يصيب الفيروس قطاع الإقلاع ةالملفات في وقت واحد ويطلق عليه - الفيروس المتعدد الأجزاء - [26].

---

[24]- شوقي ,حسام.المرجع السابق.ص. 10

2- **أروع كتاب في الهاكينغ**: الفيروسات.JOUAHARA2.CD.ROM

[26]- شوقي ,حسام.المرجع السابق.ص. 10

4-2-2. أشكال الفيروسات:

بعد تطرقنا بشيء من الإنجاز إلى أهم أنواع الفيروسات والتي من الممكن أن تصيب جهاز الحاسب وإلحاق الخراب والدمار به يجدر بنا الإشارة إلى أنه هناك عدة أشكال للفيروسات حيث أنها لا تتخذ نمطا واحدا ويمكن أن نلخص أهم أشكالها كما يلي[27]:

4-2-2-1.المتخفي: وهو الذي يختبئ في الذاكرة الرئيسية ويسيطر على القطاعات.

4-2-2-2. البطيء: كلما كان إنتشار الفيروس بطيئا كلما صعب إكتشافه والتخلص منه سريعا وأسلوب عما هذا الفيروس هو إصابة الملفات التي كان المستخدم ينوي تعديلها.

4-2-2-3. السريع: يصيب هذا الفيروس كل الملفات الحالية بمجرد دخوله إلى الحاسب وهو ليس خطيرا بشكل كبير.

4-2-2-4. المتعدد الأشكال: هي الفيروسات التي لو تتم مقارنة نسختين من الفيروس نفسه لا يتطابقان مما يصعب مهمة برنامج الحماية ويتطلب منها القيام بأمور كثيرة ومعقدة لاكتشاف هذا النوع.

4-2-2. أشهر الفيروسات:

4-2-2-1. أشهر فيروسات الحاسب

الفيروس الباكستاني: صمم هذا النوع من الفيروس من طرف باكستاني متخصص في المعلوماتية كان يبيع البرامج المعلوماتية بنصف دولار بينما سعرها في الولايات المتحدة الأمريكية 450 دولار.

الفيروس 13 أكتوبر: تعد نسبة الإصابة بهذا الفيروس قليلة أما سبب تسميته بهذا الإسم هو الشائعة التي ظهرت من أنه سوف يصيب أجهزة الحاسب جميعا في 13 أكتوبر 1989.

الفيروس العقل: وهو من فيروسات نظام التشغيل الدوس وتتمثل خطورته في أنه يكتب على قطاع التحميل للقرص مما يسبب تحميل الفيروس بمجرد تشغيل الجهاز وقبل تحميل أية برامج مضادة وهو ينقل العدوى إلى أي قرص بمجرد عرض الفهرس الخاص بهذا القرص ,ويتميز بقدرته على الإختفاء حيث يقوم بتخزين نفسه بالقطاعات التالفة من القرص[28].

فيروس الحب: ظهر هذا الفيروس في جميع أحاء العالم وبصفة خاصة بالولايات المتحدة الأمريكية وتقدر خسائر أمريكا منه نحو 10مليار دولار وقد اقتحم أنظمة الكمبيوتر العسكرية في وكالة الأمن القومي وقد انتشر هذا الفيروس عن طريق فتح البريد الإلكتروني للمستخدم تحت عنوان **LOVE** ثم لا يلبث أن ينتشر في كافة أنحاء الحاسب بمجرد فتحه.

---

[27]- - شوقي ,حسام.المرجع السابق.ص.14.

-1

فيروس مايكل أنجلو: أنطلق هذا الفيروس في 06 مارس 1992 بمناسبة الإحتفال بذكرى ميلاد الرسام الإيطالي مايكل أنجلو والذي توفي عام 1564 ولقد أصاب العديد من أنواع الحاسب [29].

4-2-2-2. أشباه الفيروسات:

1- الدودة:

برامج الدودة هي عبارة عن برامج مخصصة لاستغلال أية فجوات لكي تنتقل إلى الحاسبات الآلية عبر الوصلات التي تربط بينها وتجدر الإشارة إلى أن هده البرامج تتكاثر وتنتشر أثناء عملية انتقالها وتهدف إلى التقليل أو خفض كفاءة النظام ألمعلوماتي أو إتلاف نظم التشغيل والبيانات والملفات والبرامج [30].

ولقد ضربت نماذج كثيرة من هده الدودة شبكات الحاسب حول العالم نورد بعضا منها غي ما يلي [31]:

1-1 –الدودة مصاصة الدماء:

يعتبر بعض الدود خبيثا وبعضه حميدا وقد استخدمت شركة ّ زيدوكسّ

غي بداية الثمانينات دودة حميدة أسمتها الدودة مصاصة الدماء وكانت هده الدودة تظل خامدة طول النهار عندما يكون استخدام النظام الفي ساعات الذروة وفي الليل تستيقظ وتنشط وتستخدم المعالج بعد أن يكون قد تخفف عبء العمل لأداء بعض المهام المعقدة التي تحتاج إلى قدرات المعالج باستمرار.

1-2. دودة الأنترنت الهائلة:

لم يكن الاهتمام الموجه لهدا النوع من الفيروسات كبيرا حتى 3نوفمبر 1988 عندما أطلقت دودة الأنترنت الهائلة لتغزو الشبكة ففي أقل من ستة ساعات استطاع هدا البرنامج الذي لابتعد حجمه 99 سطرا أن يشل كل الأجهزة المرتبطة بالانترنت من نوع صن فاكس وعددها 6.000 جهاز ؛ وكانت هده الدودة عندما تصيب الجهاز تقوم بتشغيل برنامج صغير في خلفية الجهاز المصاب و لم يشعر أحد يهدا الأمر في البداية ؛ لولا خطأ بسيط من المبرمج وهو أن الدودة لا تقوم باختبار الجهاز إدا ما كان مصابا أم لا وكان من اثر دلك أن حدثت حالات كثيرة من تعدد الإصابة التي وصلت في بعض الحالات إلى المئات مما عرقل عمل الأجهزة ؛وتفاقم المشكل لاعتمادها على البريد الإلكتروني مما أدى ببعض المواقع إلى فصل نظمها عن الأنترنت.

2- القنابل:

2- العريان , على محمد. المرجع السابق.ص.90.

30- – العريان , محمد علي.المرجع السابق.ص.97.

31- داود , حسن الطاهر. **أمن الشبكات والمعلومات**. المرحع السابق. ص.

تعد القنابل إحدى الطرق التي تتلف بها المعلومات وهي على غرار باقي الفيروسات صممت لإحداث الضرر بالأنظمة والمعلومات وأهم انواع القنابل:

1 القنبلة المنطقية:

القنبلة المنطقية هي عبارة عن برنامج أو جزء من برنامج ينغد في لحظة معينة أو كل فترة زمنية منظمة ويتم وضعه في شبكة الأنترنت بهدف تحديد ظروف أو حالة النظام لغرض تسهيل تنفيذ عمل غير مشروع ؛ومن دلك مثلا إدخال التعليمات في برنامج تشغيل وهو البرنامج الذي يقوم بتحميل ذاكرة الحاسب بالبرنامج المراد تنفيده ؛وهو الذي ينفد في مرة عمل جديد وينصب البحث على عمل معين يمكن أن يكون محل للاعتداء كأن تسعي القنبلة المنطقية مثلا بالبحث عن حرف معين وليكن الألف في السجلات وعند الأمر بالحذف تتحرك متتالية وتقوم بإزالة هدا الحرف أينما وجدته ومن الأمثلة الواقعية التي استخدمت فيها 2- **القنبلة المنطقية:**

- تمكن خبير في نظم المعلومات غي الدنمارك من صنع قنبلة منطقية في نظام الحاسبات أدى إلى محو أكثر من مئة برنامج وقد تم أيضا محو النسخ الاحتياطية عند تشغيلها نظرا لانتقال آثار القنبلة إليها ثم ضبط الفاعل وحكم عليه بالسجن لستة أشهر[32].

2- القنبلة الزمنية:

أما عن القنبلة الزمنية فهي تثيرا حدثا في لحظة زمنية معينة بالساعة واليوم والسنة ويتم إدخالها في البرنامج وتنفد في جزء من الميلي ثانية أو دقائق بتاريخ المحدد سلغا ؛ وبمعنى آخر لأي خبير في صناعة البرامج أن يقوم بصناعة الفيروس إذا كان يضمر شرا للمستهدف ومن اهم الأمثلة التي إستجدمت فيها الهذا الأسلوب[33]:

في فرنسا قام خبير في نظم المعلومات بدافع الإنتقام على اثر فصله من المنشأ الذي يعمل فيه بوةضع قنبلة في شبكة المعلومات الخاصة بالمنشأ بحيث تنفجر بعد مضي ستة أشهر من رحيله وترتب عن ذلك إتلاف كل البيانات المتعلقة بها[34].

4-2-2-3.أحصنة طروادة* trojan horse[35]:

---

[32]- الرومي ,محمد أمبن.المرجع السابق.ص.57.

[33]- العريان , محمد علي.المرجع السابق.ص.57.

[34]- الرومي ,محمد أمبن.المرجع السابق.ص.57.

*- حصان طروادة: تقول الأسطورة أن طروادة كانت مدينة عظيمة منيعة الأسوار والحصون ولم يتمكن مقاتلي إسبارطة من دخولها رغم صبرهم في حصار المدينة الذي دام عشر سنوات وفي الأخير لجأوا إلى حيلة إدعاء الإنسحاب مخلفين وراءهم حصانا خشبيا هدية للطروادبين وكان الحصان يحوي في داخله ثلث الجيش الإسبرطي ,ثم فتح الباب لباقي الجيش بعد إدخال الحصان إلى المدينة.

* **تعريف:** حصان طروادة هو أح د الأساليب الهجوم الخطيرة التي تشبه الفيروسات, والتي تخفي مفاجأة شريرة تظهر في وقت معين ؛يطلق عليه اسم التروجان للاختصار وهو يختلف عن الفيروس في كونه لا يتكاثرولا يلتصق بالملفات وإنما هو برنامج مستقل بذاته ويحمل بين طياته نوقيته وأسلوب إستقاضه وبدئه النشاط وهناك العديد من هذه الأنواع تهاجم نظام اليونكس فتحل محل بعض تطبيقات الشبكة فقد تحتل تطبيق خدمة الإتصال عن بعد **Telenet** بحيث يقوم التروجان عند التعامل مع هذه الخدمة بتسجيل كل الأسماء التي تصل وكلمات السر الخاصة بها[36] .

*** كيف يصل التروجان إلى حاسوبك:**

- يرسل التروجان إلى حاسوب الضحية عن طريق البريد الإلكتروني كملف ملحق فعند استقباله وتشغيله وقد لا يرسل لوحده بل مع مجموعة كبيرة من الملفات.

- إذا كان الشخص من مستعملي أي سي كيو (**ICQ**) أو برامج المحادثة فقد يرسل له ملف مصاب.

- عندما نقوم بإنزال برنامج من أحد المواقع الغير موثوقة بها وهي كثيرة جدا.

- كتابة التروجان مباشرة على الحاسب حيث لا تستغرق العملية سوى دقائق معدودة.

في البداية كان تصميم التروجان لأغراض نبيلة مثل معرفة ما يقوم به الأبناء أو المظفون على جهاز الحاسب عند غياب المسؤول آو الأب من خلال ما يكتبه على لوحة المفاتيح ثم أصبح يستخدم لأغراض شريرة.

4-3. آثار الفيروسات:

تخلف الفيروسات آثارا وتصاحبها عدت اعراض نوجزها في ما يلي:

4-3-1 . أعراض الإصابة بالفيروس:

كما أن لكل مرض الأعراض الخاصة به والتي تساعد الطبيب على التشخيص فإن الإصابة بالفيروسات كذلك تصاحبها أعراض معينة تدل على وجوده ومن أهم هذه الأعراض:

4-3-1-1. نفص شديد في الذاكرة:

- و يلاحظ أن للذاكرة ثلاث حالات, فقبل دخول الفيروس تكون الذاكرة في حالة طبيعية ثم بعد أن يبدأ الفيروس في العمل فإنه يلاحظ نقص شديد في الذاكرة وذلك لأن الفيروس في هذه الحالة يبدأ في

---

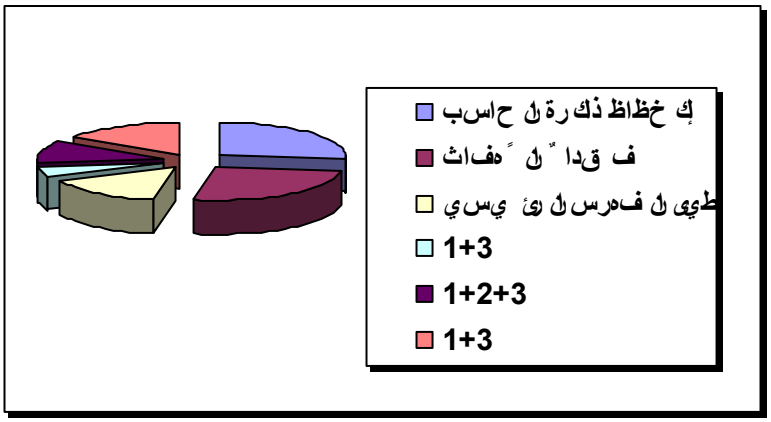
[35]- الفئر ,غبير الرضا.الأنترنت:النشأة والأخطار. مؤخودة من مجلة عجمال للعلوم والتكنولوجيا.مج6.ع.3 ,2001.ص.100.

[36]- داود ,حسن الطاهر.أمن شبكات المعلومات.المرجع السابق.ص.178.

تدمير الذاكرة وكذلك ملفات التبادل عن طريق إزالة البيانات المخزنة مما ينتج عنه توقف البرنامج العامل في الوقت ذاته لعدم وجود أي بيانات في الذاكرة ,وإنما يستبدلها بمجموعة أصفار في تعليمات التشغيل.

- **عرض رسائل الخطأ بدون أسباب حقيقية .**
- **تغيير في عدد ومكان الملفات وكذلك حجمها بدون أي أسبا ب منطقية**
- **الخطأ في استعمال لوحة المفاتيح عن طريق إظهار أحرف غريبة أو خاطئة** عند النقر على حرف معين .
- استخدام القرص الصلب بطريقة عشوائية ..وتستطيع أن تلاحظ ذلك من إضائة لمبة القرص الصلب حتى وإن كان لا يعمل .
- اختلاط أدلة القرص أو رفض النظام العمل منذ البداية .

اكتظاظ ذاكرة الحاسب، فقدان الملفات، تحطيم الفهرس الرئيسي كل هذه الأعراض تنبأ عن دخول فيروس على جهاز الحاسب والجدول رقم:17 في الصفحة 145 يوضح أهم هذه الأعراض
أعربت (26,3 %) من عينة الدراسة أن اكتظاظ الذاكرة،فقدان الملفات من الذاكرة تعد أهم الأغراض المصاحبة للإصابة بالفيروس، وهذا راجع إلى أن الفيروسات لها قابلية التضاعف حيث يعمل الفيروس عند التو ضع في الذاكرة على إعادة نسخ نفسه مما يؤدي إلى اكتظاظ الذاكرة وهذا ما يسبب ثقل الجهاز وبطئ في تنفيذ العمليات، كما يتميز الفيروس بالقدرة على التدمير فيعمل على تدمير الملفات ومنه تفقد من ذاكرة الحاسب،وهناك بعض الفيروسات التي تصل درجة خطورتها إلى حد تحطيم الفهرس الرئيسي للملفات كما يمكن أن تجتمع كل هذه الأعراض معا،الشكل البياني التالي يوضح نسب هذه الأعراض حسب عينة الدراسة :



الشكل رقم:12 أعراض الإصابة بالفيروسات

4-3-2. الأضرار التي تترتب على الإصابة بالفيروس:[37]

إن الأضرار التي يمكن أن تصيب الحاسب الآلي من جراء الفيروسات كثيرة جدا وتجدر الإشارة إلى أن الفيروس بمجرد أن يتنشط فإنه يؤدي إلى حدوث واحد أو أكثر من الأضرار التالية:

4-3-2-1. ملء ذاكرة الحاسب بالنفايات:

بما أن الفيروسات تنتشر بسرعة كبيرة ويحتل أماكن عديدة في ذاكرة الحاسب إذن فإنه يترتب على ذلك ملأ الذاكرة بالنفايات وبمعنى آخر عندما يحتل الفيروس لهذه الأماكن فإنه يجعلها غير صالحة للاستعمال مما يصيب المستخدم بخسارة مادية فادحة.

4-3-2-2. فقد ملفات من الذاكرة:

يترتب على تكاثر الفيروس في ذاكرة الحاسب خلقه لحياة ذاتية لنفسه وعندئذ يمارس الفيروس تدميره للذاكرة من خلال مسح أجزاء من الملفات المخزنة مما يجعل الملف غير قابل للاسترجاع ومن ثم لا يستطيع المستخدم أن يصل إلى إلى الملف المفقود وبالتالي لا يستطيع أن يستخدم البرنامج.

4-3-2-3. تحطيم الفهرس الرئيسي:

بعض الفيروسات تقوم أحيانا بالهجوم على الفهرس الرئيسي لنظام الحاسب فيستخدم في ذلك عدة وسائل منها تغيير حرف واحد في هذا الفهرس والذي يؤدي بدوره إلى عدم التمكن من الوصول إلى أي ملف على القرص رغم وجود الملفات فعليا.

4-3-2-4. فقد قطاع التشغيل بالقرص:

وهذا القطاع هو الذي يتم بواسطته بدأ تشغيل الجهاز وعدم تغيير النتائج الموجودة به لا يمكن تشغيل الحاسب من دلك القرص.

4-3-2-5. كتابة رسالة مطبوعة على الطابعة:

عند الكتابة في الحاسب وطباعة ما تم كتابته تظهر رسالة أخرى نتيجة لتغيير مكان الحروف على الطابعة ملم تستهلك المزيد من الوقت والجهد للإعادة.

4-3-3. أنواع دمار الفيروسات:

يختلف أنواع الدمار الذي تسببه الفيروسات حسب نوعية الفيروس المتسبب فيه ومدى خطورة ومنه نجد:

---

[37]- العريان ,محمد علي.المرجع السابق.ص..93

4-3-3-1. دمار تافـــــه:

وهو ما تسببه الفيروسات غير المضرة وكل ما يجب فعله هو التخلص من هذا الفيروس حيث لا يستغرق وقتا لإزالته.

4-3-3-2. الدمار الثانوي:

وتسببه الفيروسات الثانوية **minore virus** وتسببه الفيروسات الثانوية حيث تتسبب في تغيير أو مسح لواحد أو أكثر من الملفات القابلة للتفنيد

4-3-3-3. الدمار المعتدل:

ويتسبب فيه الفيروس المعتدل والذي يمكن جمع الملفات الموجودة على القرص الصلب عت طريق لإعادة تهيئة أو إستبدال المعلومات بكنابة معلومات أخرى تافهة فوقها.

4ـــ3ـــ3ـــ4.الدمار الرئيسي :

يؤدي الفيروس إلى تخريب المعلومات كلية.

الفصل الثالث

أمن شبكات المعلومات

تمهيـــــــد :

أمن شبكات المعلومات

عندما تحدثت تقارير 1989 عن أول فيروس كمبيوتر خيل للكثيرين من بينهم خبراء في مجال الإعلام الآلي أن ذلك مجرد خرافة ابتدعها أحد كتاب قصص الخيال العلمي, وأن وسائل الإعلام تحاول ترسيخها في أذهان الناس كحقيقة رغم أنها لا تمت إلى الواقع بصلة ، ولقد امتدت تلك الظاهرة واتسعت حتى باتت تشكل خطرا حقيقيا يهدد ثورة المعلوماتية التي فجرتها التقنيات الحديثة؛ فمن بضع فيروسات تعد على الأصابع في السنة الأولى إلى عدد يقدر بالملايين في يومنا هذا، وفي كل يوم تكتشف أنواع جديدة من الفيروسات المختلفة التأثير والشراسة ، ومن الفيروسات البسيطة إلى الفيروسات المكارة والذكية التي تتفنن في التغير والتخفي والتحول؛ ترى ما حقيقة هذا الوباء وإلى أي حد يشكل خطرا على بنية المعلومات الكونية ؟ هذا ما س أجيب عليه في هذا الفصل.

4-1. الفيروسات: الماهية

تعد الفيروسات الوباء الأول الذي يهدد البيئة الإلكترونية وفي ما يلي أهم أبجديات هذا العالم:

4-1-1. ماذا نعني بالفيروس:

4-1-1-1. ندة تاريخية عن الفيروسات:

إستسقى مصطلح فيروس من العلوم البيولوجية وهو يعني باللاتينية «سم" وكان أول ظهور معروف لفيروس الكمبيوتر عام 1981 حيث كان بغرض علمي كما يقول المؤرخون و يعتبر البذرة الأولى التي أثمرة لتشكل شجرة الفيروسات الحالية؛ وكان الفيروس ينشر عن طريق الأقراص المرنة و يعمل على نظام (أبل **APPLE 2**) يكتفي هذا الفيروس بإظهار مقطع شعري على شاشة الحاسب دون أن يقوم بأية عملية تخريبية أو تدميرية على النظام.

أما عام 1983 في شهر نوفمبر بالتحديد كانت أول تجربة علمية مسجلة لفيروس وتم تقديمها في مؤتمر أمني خاص بالحاسب الآلي وكان الفيروس يعمل على نظام اليونكس في ذلك الوقت.

أما أول ظهور لفيروس ينتقل عن طريق الأقراص المرنة في نظام الدوس فكان الأصل فيه كما يقال يعود لأخوين في باكستان استطاعا تحليل الجزء المشغل في القرص ، ومن تم قاما بتطوير طريقة عبقرية لإصابته بالفيروس وأطلقا عليه المخ (**BRAIN**)؛ وفي نفس العام شهد العالم الحاسوبي أول ملف تجسس انتقل عن طريق برنامج مجاني يدعى **PC.WRITE** ؛ كما شهد هذا العام ظهور فيروس **VIRDEM** المدمر لكن هذا الأمر ليس تابت بشكل قطعي.

1987 أول ظهور لفيروسات تستهدف ملفات التشغيل **EXE.COM**التي كان نظام الدوس يعتمد عليها بشكل كلي وهو نفس العام الذي شهد انطلاق فيروس "القدس " الذي امتد حول العالم ليشكل

أول تهديد فعلي للحاسبات ؛ ثم ظهور أول دودة الأنترنيت **IBM** مسماة دودة الكريسماس والتي كانت تعيد نسخ نفسها 500ألف مرة بالساعة.

1988 ظهور فيروس يدعى الماك ماج **MAC MAG**ومن ثم إنشاء منظمة السيرت **www.cirt.org**لمواجهة أخطار الفيروسات والديدان بعد أن تسببت دودة موريس في إغلاق الكثير من الأجهزة على الأنترنت[38].

الأعوام التالية شهدت ظهور العديد من الفيروسات إلا أن عام 1990 شهد ظهور تنافس تطوير الفيروسات بين المبرمجين ونشرها على الأنترنت.

في عام 1995 ظهر فيروس الماكرو والذي يستهدف برنامج الورد

1996 بروز فيروسات خصيصا لمهاجمة أنظمة تشغيل الوندوز 95

1998 ظهور أو فيروس جافا في العالم، وفي 1999 انفتحت نافذة الجحيم على الأنترنت وبدأ عصر جديد من التهديدات ابتدأها فيروس ملسا الذي جمع بين فيروس الماكرو ودودة الأنترنت والذي تسبب في تعطيل الكثير من الخوادم لكبريات الشركات.

وفي الأعوام التالية ظهرت العديد من الفيروسات التي تسببت بخسائر تقدر بملايير الدولارات و لم تكن بالضرورة بنفس الطبيعة إلا أنها اتفقت جميعا على كونها الخطر الأكبر الذي يهدد الحاسبات.

2000 اكتشاف فيروس وينوكس والذي استهدف منصات تشغيل الويندوز ولسنكس معا ليكون الأول من نوعه في هذا المجال[39].

4-1-1-2. تعريف الفيروس:

وهنا يمكن إيراد عدة تعاريف نذكر منها:

1- برنامج صغير ولكن خبيث طور خصيصا لتنفيذ أعمال تخريبية علي الحاسب الآلي يحتوي هذا النوع من البرامج في معظم الأحيان علي أوامر تخريبية معينة في نص الشفرة وتختلف التي تكتب بها وتنفذ عند تحقيق شروط معينة وتختلف طرق الإصابة بالفيروسات فمنها ما ينسخ نفسه داخل ملفات ذات هيئة معينة ومتوافقة مع ما هو مصمم له وكلما تم استدعاء هذه الملفات أو تشغيلها ويتحقق بالبيئة المحيطة

ومن هذه البرامج الخبيثة ما ينسخ نفسه في الذاكرة مما يؤدي إلى بطئ شديد في عمل الجهاز ومنها ما يقوم بتخريب نظام الإدخال والإخراج الأساسي في الوقت الذي تزداد فيه خبرة وذكاء مؤلفي (مصممي)

---

2 – الجنبيهي ,منير محمد ؛ الجنبيهي , ممدوح محمد. **أمن المعلومات الإلكترونية**.الإسكندرية:دار الفكر الجامعي , 2005.صص48-49.[38]

[39]– الجنبيهي ,منير محمد ؛ الجنبيهي , ممدوح محمد. لأمن المعلومات الإلكترونية.المرجع السابق. ض.50.

الفيروسات وبالتالي زيادة عدد الفيروسات وأنواعها يتم تطويرها في تقنيات مكافحة تلك الفيروسات للتصدي لها وإزالتها قبل حدوث أي الضرر [40].

2- كما يعرف أيضا بأنه برنامج حاسب مثل أي برنامج تطبيقي آخر ولكن يتم تصميمه بواسطة أحد المخربين لهدف محدد هو إحداث أكبر ضرر ممكن بنظام الحاسب ولتنفيذ ذلك يتم إعطائه القدرة على ربط نفسه ببرامج آخرى وكذلك إعادة إنشاء نفسه حتى يبدو أنه يتكاثر ويتوالد ذاتيا وهذا يتيح له قدرة كبيرة على الإنشار بين البرامج المختلفة وكذلك بين المواقع المختلفة في الذاكرة حتى يحقق أهدافه التدميرية كما أن إنتشار الفيروس لا يقتصر على النظام الذي يتواجد به ولكنه ينتقل أيضا إلى نظم أخرى قد تكون أبعد مسافة ممكنة على هذا النظام ويعود هذا الإنتشار إلى عاملين أساسيين هما:

أ- التوافق: وهو يعني قدرة البرامج الواحد على التشغيل على أنواع مختلفة من الحواسب وإصدارات مختلفة من نظم التشغيل وهذا العامل رغم تأثيره الإيجابي والهام بالنسبة لتطوير النظم أن أثره على إنتشار الفيروس كان كبير.

ب – وسائل الإتصال:

وهي الوسائل التي أدت إلى ريط عدد من أجهزة الحاسب بشبكة الأن ترنيت و اتصالهم من خلالها وهذه الأجهزة قد تكون في نفس الوقع وقد تكون في مواقع مختلفة [41]

4-1-1-3. لماذا سمي بالفيروس[42]:

تطلق كلمة الفيروس أساسا على الفيروسات التي تنقل الأمراض عن طريق انتقالها من إنسان مريض إلى إنسان آخر وبمجرد انتقالها إلى الإنسان تتكاثر حتى تصيب الأجهزة العضوية.

والفيروس الخاص بالحاسب يقوم بعمل مشابه لذلك ، حيث أنه عبارة عن برنامج يصممه بعض المتخصصين لأهداف تخريبية مع إعطائه القدرة على ربط نفسه ببرامج أخرى ثم يتكاثر وينتشر داخل النظام حتى يتسبب في تدمير هاما؛ وهناك أوجه تشابه متعددة بين الفيروس العضوي وفيروس الحاسب يمكن تلخيصها في ما يلي:

- يقوم الفيروس العضوي بتغيير الخصائص العضوية لخلايا الجسم ويقوم فيروس الحاسب بتغيير وظائف برامج لأخرى.

---

1 – الربيعي ,محمد,شعبان أحمد أحمد ,وآخرون. المعجم الشامل لمصطلحات الحاسب الآلي ة الأنترنت.مكتبة السيكان الرياض 2001ص 446

1- طلية.محمد فهمي المرجع السابق ص.34.

[42]– – طلية. محمد فهمي.؛ عبد الوهاب، مصطفى رضا....وآخرون .فيروسات الحاسب وأمن البيانات، 1996.موسوعة دلتا كمبيوتر 8

- يتكاثر الفيروس العضوي ويتسبب في أنتاج فيروسات جديدة ويقوم فيروس الحاسب بإعادة إنشاء نفسه.

- الخلية التي تصاب بالفيروس العضوي لا تصاب بنسف الفيروس مرة ثانية وتحدث نفس الشيء مع الفيروس حيث يقوم باختيار البرنامج المطلوب نقل العدوى فإن وجد أنه سبق إصابته به لا يصيبه مرة ثانية وينتقل إلى برامج أخرى

- الجسم الذي تنتقل إليه العدوى قد يظل مدة طويلة دون ظهور أعراض المرض عليه ويقوم برنامج الحاسب بأداء وظائفها لمدة طويلة دون ظهور أخطاء نتيجة وجود الفيروس

- من ذلك ينضح سبب إطلاق تسمية الفيروس رغم أنه في الحقيقة ليس إلا برنامج مثل البرامج الحاسب ولكنه يختلف عنه في الوظائف التدميرية.

4-1-2. خصائص الفيروس:

كما سبق ذكره فإن الفيروس هو برنامج له صفات التكاثر والمضاعفة والاختفاء أو التخفي والإننفجار وعلى هذا الأساس يمكن ذكر أهم الخصائص التي يميز بها الفيروس في ما يلي:

4-1-2-1- القدرة على الاختفاء:

فالفيروس ما هو إلا برنامج أو القدرة على الاختفاء عن المستخدم والتمويه غليه وهو يستخدم وسائل متعددة في الاختفاء ومنها الارتباط بالبرامج الشائعة الاستعمال حيث أن مستخدم للحاسب الشخصي يهتم بتوفير البرامج التي تمكنه من الاستفادة من خصائص الحاسب؛ وبعض المستخدمين يقوم بنسخ هذه البرامج دون السؤال عن مصدرها وعند تشغيلها ينتقل الفيروس إلى القرص ويقوم بأعماله التدميرية ؛ وهناك فيروسات تدخل إلى الحاسب كملفات متخفية بحيث لا يستطيع المستخدم ملاحظة تواجدها عن طريق فهرس الملفات وهناك بعضا منها يستقر في أماكن معينة حيث يصعب العثور عليها ثم تبرمج على تاريخ معين ثم تقوم بتنفيذ وتشغيل نفسها في هذا التاريخ , وهناك أنماط أخرى من الفيروسات تقوم بإخفاء أي أثر على تواجدها حيث تظل البرامج المصابة تعمل بكفاءة دون أخطاء مدة طويلة بينما يقوم هو بالإنتقال من برنامج إلى آخر بخفة [43].

1 - الرومي , محمد أمين. جرائم الكمبيوتر والأنترنت. الإسكندرية: دار المطبوعات الجامعية ,2003.ص.28

4-1-2-2. الانتشار:

يتميز فيروس الحاسب بقدرة كبيرة على الإنتشار ومن أهم الوسائل التي تساعد على ذلك إنتشار وسائل الإتصال الحديثة التي تجعل الفيروس ينتقل بسرعة من حاسب إلى آخر شبكة الأنترنت إلى ملايين المستعملين وكذلك توافق الأجهزة الذي يساعد الفيروس على العمل وإذا قارنا بين إنتشار الفيروس العضوي وفيروس الحاسب نجد أن هذا الأخير أسرع إنتشار بدرجة كبيرة حيث يمكنه في ثوان محدودة الإنتقال من قارة إلى أخرى كما يمكنه الإنتقال إلى عدد ضخم من المستخدمين في نفس الوقت بينما لا يستطيع الفيروس العضوي فعل ذلك وعند انتقال الفيروس إلى الحاسب فإنه ينتشر بسرعة كبيرة داخل الذاكرة حيث أنه يربط نفسه بالبرامج المخزنة داخل الذاكرة كما يقوم بعمل نسخ كبيرة لنفسه [44].

3- القدرة على الإختراق:

يتميز فيروس الحاسب بقدر ة كبيرة على الدخول والتسلل واختراق الحصون والمواقع التي يقيمها المستخدم بتحميل هذه البرامج حيث يكون الفيروس عادة موجودا في احد البرامج المفيدة التي يحتاجها المستخدم لتشغيل الحاسب ثم يقوم المستخدم بتحميل هذه البرامج وإدخال الفيروس دون أن يشعر وبعض الفيروسات يتم إدخالها بإستخدام حصان طروادة حيث يرتبط بأحد البرامج المثيرة التي تجدب المستخدم وتثير لديه حب الإطلاع وعند تحميل هذه البرامج يبدأ الفيروس في الإنتشار وتنفيذ عملياته التدميرية [45]

4- القدرة على التدمير:

عندما يدخل الفيروس إلى الكمبيوتر يظل ساكنا حتى تبدأ لحظة الصفر التي يبدأ عندها في الإنتشار والحركة وساعة الصفر هذه إما أن تكون كلمة معينة كتبها المستخدم أو إشارة معينة أو عند تاريخ معين ويعمل الفيروس غالبا على محور البيانات المخزنة في الذاكرة[46]

4-1-3. دورة حياة الفيروسات وانتشارها:

4-1-3-1. . دورة حياة الفيروس[47]:

وهناك سقمراحل لدورة حياة فيروس الكمبيوتر تتمثل في:

1- مرحلة التصميم

2- طلية.محمد فهمي المرجع السابق ص 64

1- طلية.محمد فهمي المرجع السابق ص 64

46

[47]- دورة حياة الفيروس (على الخط المباشر).(14-12-2006) متوفر على الخط المباشر
http// www.jparisnajd.com /

عملية تصميم فيروس جديد تحتاج إلى شخص على درجة عالية من الكفاءة في التعامل مع لغات البرمجة على الحاسب الشخصي مثل لغة البيسك والجافا والفيجوال **c++**

وقد لا تبح هذه الخبرات والكفاءات ضرورية في المستقبل حيث يتم تقديم مساعدات كبيرة على مستوى شبكة الأنترنيت للمبرمجين المبتدئين الذين يردون القيام بتصميمات

2-مرحلة الإنتشار:

عادة ما يقوم مطورو الفيروسات بنشر فيروساتهم على أكبر عدد من الحواسب الشخصية قبل أن يبدأ الفيروس بإحداث الآثار التدميرية المكلف بها والسبب في ذلك وهو نشر أكبر عدد من النسخ قبل أن تنتبه شركات مقاومة الفيروسات لوجوده فتبدأ بوضع البرامج المضادة لها وفي هذه المرحلة تصل الفيروسات إلى الحاسبات وتظل بها دون أن تظهر أية أعراض على الحاسبات المصابة.

3- مرحلة النشاط:

تبدأ الفيروسات في النشاط ولإحداث الآثار التدميرية التي تمت برمجتها للقيام بها عند وقوع حدث معين وقد تتم برمجته لكي ينشط في توقيت معين أو عند تشغيل برنامج ما أو عند الإتصال بشبكة الأن ترنيت أو عند وصول جزء ثان من الفيروس إلى الحاسب وتنوع الأعمال التخريبية من تدمير الملفات المخزنة على الحاسب أو استهلاك المساحات ووحدة التخزين

4- مرحلة اكتشاف الفيروس:

قد لا تتبع هذه الخطوة دائما عملية نشاط الفيروس فقد تكون الشركات المنتجة لبرامج مقاومة الفيروسات أكثر ذكاء بحيث تكتشف وجود الفيروس قبل أن ينشط ومن تم العمل على مقاومته.

5 – مرحلة المواجهة:

في هذه المرحلة تقوم شركات إنتاج برامج مقاومة الفيروسات تعديل برامجها وملفاتها لكي تتعامل مع الفيروس الجديد ولكل فيروس بصمة خاصة به وهي (الكود الذي تكتب به أوامر الفيروس بأحد لغات الحاسب) ويتم إضافة هذه البصمة إلى ملفات البرامج بعد ذلك يقوم المستخدمون بتويل الملفات على موقع الشركة على شبكة ويقومون بتحدث البرامج بعد التعديل. هذه المرحلة قد تصل إلى ستة أشهر حسب نوع الفيروس

6- مرحلة الإستئصال:

بعد فترة من القيام بعدد كبير من حديث برامجهم ,تنحصر آثار الفيروس بالتعديلات التي تكتشف وتقضي على الفيروس بحيث تنخفض درجة تهديده لمجتمع المعلومات

4-1-3-2. عوامل إنتشار الفيروسات[48]:

هناك العديد من العوامل التي تقف وراء الإنتشار الكبير للفيروسات في هذه الأيام وهذه العوامل لخصها التقرير الذي قدم إلى مجلس بحوث أمن المعلومات في الولايات المتحدة فيما يلي:

3 إنتشار الشبكات:

بازدياد ارتباط الحاسبات ببعضها من خلال شبكة الأنترنت ازدادت سهولة شن الهجمات كما ازداد عدد هذه الهجمات تبعا لذلك وأصبح من النادر اليوم أن نرى جهاز حاسب غير مرتبط بشبكة الأنترنت ويدعم ذلك الاتجاه ما نشهده من الاعتماد المتزايد لدى الأفراد والشركات على البريد الإلكتروني كوسيلة اتصال وتواصل وباختصار شديد فإن مهاجم اليوم لا يحتاج إلى الوصول المباشر إلى جهاز الحاسب لزرع فيروسه كما ساعد انتشار الشبكات على شن أنواع آلية من الهجوم لا يتدخل فيها البشر وقد حدث في فيبراير 2000 هجوم تسبب في عرقلة الخدمة في العديد من مواقع التجارة الإلكترونية

4 زيادة تعقيد النظم

بازدياد حجم نظم المعلومات ودرجة تعقيدها زاد إعتمادها على نظم التشغيل في توفير الحماية الأمنية لها ونظم التشغيل نفسها تضم آلاف من البرامج التي تحتوي على عشرات الملايين من الأوامر وفي نظم بهذا الحجم لا يمكن تفادي الثغرات ,وزاد تفاقم المشكلة استخدام لغات لا تتمتع بالحماية الأمنية مثل لغة **c++** التي لا تقاوم أبسط أنواع الهجوم

ومن جهة أخرى فإن التطبيقات الضخمة المعقدة تشكل بيئة صالحة لنمو الفيروسات فلا يلحظ وجودها أحد , فقد نستطيع فحص برنامج صغير وتأكيد نظافته وخلوته من الفيروسات ولكن من المستحيل عمل ذلك في تطبيقات اليوم التي تملأ حياتنا الشخصية ناهيك عن التطبيقات الضخمة التي تعمل في الشركات والدوائر الحكومية

3- سهولة الإضافة إلى النظم:

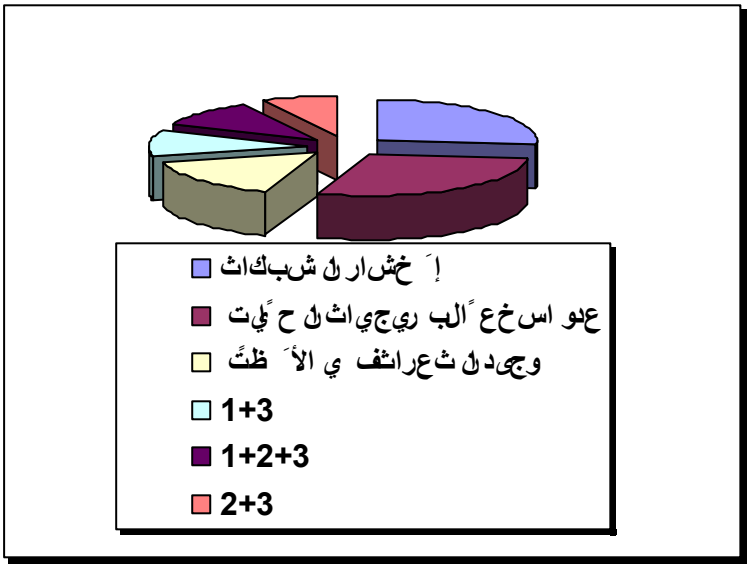
تفخر الكثير من نظم المعلومات اليوم بأنها نظم قابلة للتوسع بمعنى أنها تقبل التحديث والإضافة سواء من جانب المحدد أو المستخدم وتأتي هذه الإضافات بشكل برامج منقولة ولذلك فُن مع ظم البرمجيات ونظم التشغيل الحالية تجدها قابلة للتوسع مما سهل اقتحام الفيروسات وأوضح مثال على ذلك الكيفية التي انتشر بها فيروس (ميلسا) حيث استغل قابلية البرنامج الإلكتروني (أوت لوك) **oritlook** لتوسع فقد تم كتابة الفيروس في صورة رسالة إنخد بها معظم المستخدمين.

---

[48]- أمن شبكات المعلومات ص 167

إذن وكما سبق الإشارة إليه فإن البيئة الإلكترونية أدت إلى قلب العديد من الأمور؛ حيث ظهرت العديد من الإفرازات منها ما هو سلبي ومنها ما هو إيجابي، وتعد الفيروسات واحدة من أبرز الإفرازات السلبية وقد ساهم في انتشاره هذه الأوبئة عدة أمور موضحة في الجدول رقم **15** الصفحة 144

وفقد أعرب الطلبة على أنه ومهما اختلفت الأسباب التي تؤدي إلى إنتشار الفيروسات بشكل رهيب فإن أهمها على الإطلاق هو عدم استعمال برمجيات الحماية بنسبة (28,9 %) وذلك على الرغم كمن الأهمية التي تكتسيها هذه البرمجيات، ثم يليها إنتشار الشبكات بنسبة (26,3 %)، حيث أن الشبكات اكتسحت العالم المعاصر مما جعلها تشكل مناخا ملائما لنمو وتطور الفيروسات، كما أدى ظهور الشبكة العنكبوتية إلى استعمالها كناقل ممتاز لنشر هذه الفيروسات؛ ومن أهم أسباب انتشارها كذلك وجود ثغرات كثيرة في الحاسب وأنظمة التشغيل وهذا ما عبر عنه (17,7 %) من العينة، كما تشكل هذه الأسباب إذا توفرت جميعها لأكبر وأحسن بيئة لالتهاب الشبكة بهذه الفيروسات وهذا ما يوضحه الشكل البياني التالي:



الشكل رقم :11 أسباب إنتشار الشبكات

الفصل الرابع

الإدارة الإلكترونية للمعلومات من خلال الشبكات

الإدارة الالكترونية للمعلومات من خلال الشبكات

وسائل الإدارة:

يمكن لفيروس الحاسب الإنتقال داخل شبكة الإنترنيت أو أي شبكة محلية عن طريق وسائل أربعة:

1- البريد الإلكتروني:

ينتقل الفيروس عبر برنامج أوت لوك وأوت لوك اكيبريس وذلك عن طريق ملف يلصق بالرسالة التي ترد عبر البريد الإلكتروني ويحمل ملف إسم **REACLM EXE** وتظهر له أيقونة بقوته **ATML** وذلك في محاولة لخداع المستخدم ويكفي قيام المستخدم بالنقر على الملف حتى ينسخ الفيروس نفسه و بمد رسالة تلقائية ترسل إلى جميع العناوين الخاصة بالبريد الإلكتروني التي توجد في دفتر عناوين المستخدم.

2- مزود ويب ISS

يضع الفيروس عناوين عديدة بشكل ؟؟؟؟؟ لما يفعله فيروس **CODERED** بحثا عن مزودات **ISS**والتي تتضمن ثغرات أمنية يستفيد منها في عملية الإنشار ويحاول الفيروس كذلك الاستفادة من دودة فيروس**CODERED2** التي تنتشر عبر مزود **ISS** حيث كانت الدودة تترك برنامج باب خلفي في هذه المزودات كي تسمح للمخترق بالدخول إليها والسيطرة عليها فيما بعد

3- متصفح الأنترنت:

بعد أن يصيب الفيروس أحد المزودات – شبكة الأنترنيت – بالطريقتين السابقتين بنسخ شفرة معينة إلى كل صفحات (**asp- htmail- htm**) التي توجد في المواقع التي يستضيفها مزود -الأنترنيت – وعند زيارة الموقع المصاب من طرف أحد المستخدمين ويبد أفي تزيل ملف منه يشتعل الفيروس تلقائيا ويصيب جهاز المستخدم

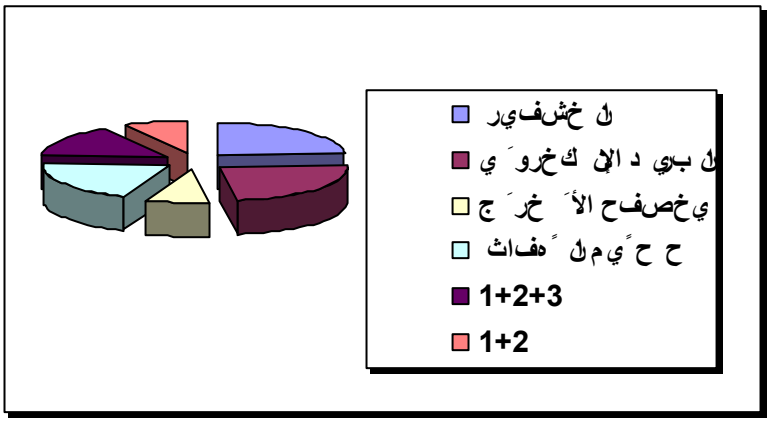
4- المشاركة على الملفات:

تسمح هذه الطريقة للفيروس أن ينتشر عبر الشبكات المحلية التيوجدت ملفات أو مجلدات مشتركة عبر شبكة ميكروسوفت .

وكما سبق الإشارة إليه فإن الفيروسات تنتشر بعدة طرق أهمها البريد الإلكتروني وكذا تحميل الملفات من الأنترنت والجدول 16 الصفحة 144 بوضح ذلك

ترى عينة الدراسة أن أهم طرق انتشار الفيروسات هي البريد الإلكتروني (31,5 %)،فمع إنتشار شبكة الانترنت أصبح البريد الإلكتروني الخدمة الأكثر شعبية والتي أدت إلى زيادة استخدام الشبكة وقد استغل صناع الفيروسات هذه الخدمة من أجل نشر سمومهم على الشبكة، كما يمكن أن يؤدي تحميل الملفات من الأنترنت

خصوصا من المواقع المشبوهة إلى المساهمة في إنتشار هذه الأوبئة وهذا ما عبرت عنه (26,5 %) من عينة الدراسة إضافة على العديد من الطرق الأخرى كمتصفح الأنترنت ونوضح ما سبق ذكره بشكل أفضل بالرسم البياني التالي:



الشكل رقم: 12 طرق نشر الفيروسات

4-2. أنواع الفيروسات وأشكالها:

4-2-1. أنواع الفيروسات

إن الفيروسات مهما أختلف شكلها أو نوعها خاصة واحدة هي إلحاق الأدى والضرر بالبرامج إلي برمجت لإلحاق الأذى بها ويمكن أن نميز العديد من أنواع الفيروسات:

4-2-1-1. قطاع التشغيل bootseetor :

وتعتبر من أقدم الفيروسات وأكثرها إنتشار إذ تستطيع أن تصيب المقطع التشغيلي في الأقراص المرنة أو مقطع نظام تشغيل الدوس **dos** حيث أن كل الأقراص سواء كانت صلبة أو مرنة تملك قطاع تشغيل ويتكون من المعلومات الخاصة بشكل القرص (نوع البنية , نوع المعطيات) وتكمن خطورة هذه الفيروسات في قدرتها على إتلاف هذا الجزء ثم يقوم بأحد مكان قطاع تشغيل القرص المصاب بنسخة منه ثم ينقل المقطع الأصلي إلى مكان آخر في القرص [49] .

4-2-1-2. فيروسات الملفات:

[49] -**types des virus informatique.(**en ligne) (23/02/2006)

وهي الفيروسات التي تلصق نفسها مع ملفات البرامج التنفيدية ذات الإمتداد **com exe** وقد يمتد أثرها ليصيب الملفات ذات الإمتداد **ouc , dry ,sys**.....ومع هذا النوع من الفيروسات فإن البرامج تصاب بمجرد بدأ تشغيل هذه الرمج[50] ويمكن تقسيم هذه الفيروسات إلى أربغة أنواع[51]:

أ- الفيروسات المتطفلة:

التي تلصق نفسها بالملفات لكي تتكاثر وتبقي الملف الأصلي بحالة سليمة

ب- الفيروسات المرافقة:

التي تعتمد على قاعدة الأسبقية في التنفيد للملفات ذات الإمتداد **com** وتتمكن من نقل العدوى عن طريق إنشاء ملف جديد بدون ؟؟؟؟؟ الملف

ج- الفيروسات الرابطة:

وهي التي تصيب البرامج بتغيير المعلومات في جدول مواقع الملفات

د- الفيروسات المستبدلة:

التي تقوم بالكتابة فوق جزء من برنامج دون تغيير حجم الملف مما يؤدي إلى فشل الملف عند تنفيذه.

4-2-1-2. الفيروسات متعددة القدرة التحويلية:

وهذه الفيروسات لها القدرة الديناميكية على وتنفيذ الشفرات عند الإنتقال من ملف إلى آخر لكي يصعب اكتشافها [52].

4-2-1-4. فيروس الماكرو:

هذا النوع أيضا سريع الإنتشار بين المستخدمين خاصة أنه قادر على كل الطرق كالأقراص الصلبة والبريد الإلكتروني والبرامج المجانية ويعتبر من أحد أنواع الفيروسات والجدير بالذكر وهذا الفيروس لا يصيب إلا

---

fr escpotting.com/ seardr/ riduchon.html www.affiliate

[2] - المرجع السابق

3 – شوقي , حسام المرجع السابق ص10

[52]- شوقي ,حسام.المرجع السابق.ص. 10

البرنامج التطبيقي الذي صمم لإتلافه فمثلا لو إن فيروس صمم ليصيب برنامج تحرير الكلمات والنصوص فإنهلا يستطيع إلحاق الأذى بأي برنامج آخر[53].

4-2-1-5. الفيروسات قطاع الإقلاع:

تستقر هذه النوعية من الفيروسات في الأماكن التي يقرأها الكمبيوتر بالقرص الصلب وينفد التعليمات المخزنة ضمنها عند الإقلاع ثم تصيب قطاع الإقلاع الخاصة بنظام الدوس بينما تصيب فيروسات الفئة الفرعية المسماة **MBR virus** قطاع الإقلاع الرئيسي للكومبيوتر كما يمكن أن يصيب الفيروس قطاع الإقلاع ةالملفات في وقت واحد ويطلق عليه - الفيروس المتعدد الأجزاء -[54].

4-2-2. أشكال الفيروسات:

بعد تطرفنا بشيء من الإنجاز إلى أهم أنواع الفيروسات والتي من الممكن أن تصيب جهاز الحاسب وإلحاق الخراب والدمار به يجدر بنا الإشارة إلى أنه هناك عدة أشكال للفيروسات حيث أنها لا تتخذ نمطا واحدا ويمكن أن نلخص أهم أشكالها كما يلي[55]:

4-2-2-1.المتخفي: وهو الذي يختبئ في الذاكرة الرئيسية ويسيطر على القطاعات.

4-2-2-2. البطيء: كلما كان إنتشار الفيروس بطيئا كلما صعب إكتشافه والتخلص منه سريعا وأسلوب عما هذا الفيروس هو إصابة الملفات التي كان المستخدم ينوي تعديلها.

4-2-2-3. السريع: يصيب هذا الفيروس كل الملفات الحالية بمجرد دخوله إلى الحاسب وهو ليس خطيرا بشكل كبير.

4-2-2-4. المتعدد الأشكال: هي الفيروسات التي لو تتم مقارنة نسختين من الفيروس نفسه لا يتطابقان مما يصعب مهمة برنامج الحماية ويتطلب منها القيام بأمور كثيرة ومعقدة لاكتشاف هذا النوع.

4-2-2. أشهر الفيروسات:

4-2-2-1. أشهر فيروسات الحاسب

الفيروس الباكستاني: صمم هذا النوع من الفيروس من طرف باكستاني متخصص في المعلوماتية كان يبيع البرامج المعلوماتية بنصف دولار بينما سعرها في الولايات المتحدة الأمريكية 450 دولار.

2- **أروع كتاب في الهاكينغ:** الفيروسات.JOUAHARA2.CD.ROM

[54]- شوقي ,حسام.المرجع السابق.ص. 10

[55]- - شوقي ,حسام.المرجع السابق.ص.14.

الفيروس 13 أكتوبر: تعد نسبة الإصابة بهذا الفيروس قليلة أما سبب تسميته بهذا الإسم هو الشائعة التي ظهرت من أنه سوف يصيب أجهزة الحاسب جميعا في 13 أكتوبر 1989.

الفيروس العقل: وهو من فيروسات نظام التشغيل الدوس وتتمثل خطورته في أنه يكتب على قطاع التحميل للقرص مما يسبب تحميل الفيروس بمجرد تشغيل الجهاز وقبل تحميل أية برامج مضادة وهو ينقل العدوى إلى أي قرص بمجرد عرض الفهرس الخاص بهذا القرص ,ويتميز بقدرته على الإختفاء حيث يقوم بتخزين نفسه بالقطاعات التالفة من القرص[56].

فيروس الحب: ظهر هذا الفيروس في جميع أحاء العالم وبصفة خاصة بالولايات المتحدة الأمريكية وتقدر خسائر أمريكا منه نحو 10مليار دولار وقد اقتحم أنظمة الكمبيوتر العسكرية في وكالة الأمن القومي وقد انتشر هذا الفيروس عن طريق فتح البريد الإلكتروني للمستخدم تحت عنوان **LOVE** ثم لا يلبث أن ينتشر في كافة أنحاء الحاسب بمجرد فتحه.

فيروس مايكل أنجلو: أنطلق هذا الفيروس في 06 مارس 1992 بمناسبة الإحتفال بذكرى ميلاد الرسام الإيطالي مايكل أنجلو والذي توفي عام 1564 ولقد أصاب العديد من أنواع الحاسب [57].

4-2-2-2. أشباه الفيروسات:

1- الدودة:

برامج الدودة هي عبارة عن برامج مخصصة لاستغلال أية فجوات لكي تنتقل إلى الحاسبات الآلية عبر الوصلات التي تربط بينها وتجدر الإشارة إلى أن هده البرامج تتكاثر وتنتشر أثناء عملية انتقالها وتهدف إلى التقليل أو خفض كفاءة النظام ألمعلوماتي أو إتلاف نظم التشغيل والبيانات والملفات والبرامج [58].

ولقد ضربت نماذج كثيرة من هده الدودة شبكات الحاسب حول العالم نورد بعضا منها غي ما يلي [59]:

1-1 –الدودة مصاصة الدماء:

يعتبر بعض الدود خبيثا وبعضه حميدا وقد استخدمت شركة ّ زيدوكسّ

غي بداية الثمانينات دودة حميدة أسمتها الدودة مصاصة الدماء وكانت هده الدودة تظل خامدة طول النهار عندما يكون استخدام النظام الفي ساعات الذروة وفي الليل تستيقظ وتنشط وتستخدم المعالج بعد أن يكون قد تخفف عبء العمل لأداء بعض المهام المعقدة التي تحتاج إلى قدرات المعالج باستمرار.

-1

2- العريان , على محمد. المرجع السابق.ص.90.

58- – العريان , محمد علي.المرجع السابق.ص.97.

59- داود , حسن الطاهر. **أمن الشبكات والمعلومات**. المرجع السابق. ص.

1-2. دودة الأنترنت الهائلة:

لم يكن الاهتمام الموجه لهدا النوع من الفيروسات كبيرا حتى 3نوفمبر 1988 عندما أطلقت دودة الأنترنت الهائلة لتغزو الشبكة ففي أقل من ستة ساعات استطاع هدا البرنامج الذي لابتعد حجمه 99 سطرا أن يشل كل الأجهزة المرتبطة بالانترنت من نوع صن فاكس وعددها 6.000 جهاز ؛ وكانت هده الدودة عندما تصيب الجهاز تقوم بتشغيل برنامج صغير في خلفية الجهاز المصاب و لم يشعر أحد يهدا الأمر في البداية ؛ لولا خطأ بسيط من المبرمج وهو أن الدودة لا تقوم باختبار الجهاز إدا ما كان مصابا أم لا وكان من اثر دلك أن حدثت حالات كثيرة من تعدد الإصابة التي وصلت في بعض الحالات إلى المئات مما عرقل عمل الأجهزة ؛وتفاقم المشكل لاعتمادها على البريد الإلكتروني مما أدى ببعض المواقع إلى فصل نظمها عن الأنترنت.

2- القنابل:

تعد القنابل إحدى الطرق التي تتلف بها المعلومات وهي على غرار باقي الفيروسات صممت لإحداث الضرر بالأنظمة والمعلومات وأهم انواع القنابل:

2 القنبلة المنطقية:

القنبلة المنطقية هي عبارة عن برنامج أو جزء من برنامج ينغد في لحظة معينة أو كل فترة زمنية منظمة ويتم وضعه في شبكة الأنترنت بهدف تحديد ظروف أو حالة النظام لغرض تسهيل تنفيذ عمل غير مشروع ؛ومن دلك مثلا إدخال التعليمات في برنامج تشغيل وهو البرنامج الذي يقوم بتحميل ذاكرة الحاسب بالبرنامج المراد تنفيده ؛وهو الذي ينفد في مرة عمل جديد وينصب البحث على عمل معين يمكن أن يكون محل للاعتداء كأن تسعي القنبلة المنطقية مثلا بالبحث عن حرف معين وليكن الألف في السجلات وعند الأمر بالحذف تتحرك متتالية وتقوم بإزالة هدا الحرف أينما وجدته ومن الأمثلة الواقعية التي استخدمت فيها 2- **القنبلة المنطقية:**

- تمكن خبير في نظم المعلومات غي الدنمارك من صنع قنبلة منطقية في نظام الحاسبات أدى إلى محو أكثر من مئة برنامج وقد تم أيضا محو النسخ الاحتياطية عند تشغيلها نظرا لانتقال آثار القنبلة إليها ثم ضبط الفاعل وحكم عليه بالسجن لستة أشهر[60].

2- القنبلة الزمنية:

أما عن القنبلة الزمنية فهي تثيرا حدثا في لحظة زمنية معينة بالساعة واليوم والسنة ويتم إدخالها في البرنامج وتنفد في جزء من الميلي ثانية أو دقائق بتاريخ المحدد سلغا ؛ وبمعنى آخر لأي خبير في صناعة البرامج أن

---

[60]- الرومي ,محمد أمبن.المرجع السابق.ص.57.

يقوم بصناعة الفيروس إذا كان يضمر شرا للمستهدف ومن اهم الأمثلة التي إستجدمت فيها الهذا الأسلوب :[61]

في فرنسا قام خبير في نظم المعلومات بدافع الإنتقام على اثر فصله من المنشأ الذي يعمل فيه بوةضع قنبلة في شبكة المعلومات الخاصة بالمنشأ بحيث تنفجر بعد مضي ستة أشهر من رحيله وترتب عن ذلك إتلاف كل البيانات المتعلقة بها[62].

4-2-2-3.أحصنة طروادة* trojan horse [63]:

* **تعريف:** حصان طروادة هو أح د الأساليب الهجوم الخطيرة التي تشبه الفيروسات, والتي تخفي مفاجأة شريرة تظهر في وقت معين ؛يطلق عليه اسم التروجان للاختصار وهو يختلف عن الفيروس في كونه لا يتكاثرولا يلتصق بالملفات وإنما هو برنامج مستقل بذاته ويحمل بين طياته نوقيته وأسلوب إستقاضه وبدئه النشاط وهناك العديد من هذه الأنواع تهاجم نظام اليونكس فتحل محل بعض تطبيقات الشبكة فقد تحتل تطبيق خدمة الإتصال عن بعد **Telenet** بحيث يقوم التروجان عند التعامل مع هذه الخدمة بتسجيل كل الأسماء التي تصل وكلمات السر الخاصة بها[64] .

* **كيف يصل التروجان إلى حاسوبك:**

- يرسل التروجان إلى حاسوب الضحية عن طريق البريد الإلكتروني كملف ملحق فعند استقباله وتشغيله وقد لا يرسل لوحده بل مع مجموعة كبيرة من الملفات.

- إذا كان الشخص من مستعملي أي سي كيو (**ICQ**) أو برامج المحادثة فقد يرسل له ملف مصاب.

- عندما نقوم بإنزال برنامج من أحد المواقع الغير موثوقة بها وهي كثيرة جدا.

- كتابة التروجان مباشرة على الحاسب حيث لا تستغرق العملية سوى دقائق معدودة.

---

[61]- العريان , محمد علي.المرجع السابق.ص.57.

[62]- الرومي ,محمد أمبن.المرجع السابق.ص.57.

*- حصان طروادة: تقول الأسطورة أن طروادة كانت مدينة عظيمة منيعة الأسوار والحصون ولم يتمكن مقاتلي إسبارطة من دخولها رغم صبرهم في حصار المدينة الذي دام عشر سنوات وفي الأخير لجأوا إلى حيلة إدعاء الإنسحاب مخلفين وراءهم حصانا خشبيا هدية للطرواديين وكان الحصان يحوي في داخله ثلث الجيش الإسبرطي ,ثم فتح الباب لباقي الجيش بعد إدخال الحصان إلى المدينة.

[63]- الفئر ,غبير الرضا.الأنترنت:النشأة والأخطار. مؤخودة من مجلة عجمال للعلوم والتكنولوجيا.مج6.ع.3 ,2001.ص.100.

[64]- داود ,حسن الطاهر.أمن شبكات المعلومات.المرجع السابق.ص.178.

في البداية كان تصميم التروجان لأغراض نبيلة مثل معرفة ما يقوم به الأبناء أو المظفون على جهاز الحاسب عند غياب المسؤول آو الأب من خلال ما يكتبه على لوحة المفاتيح ثم أصبح يستخدم لأغراض شريرة.

4-3. آثار الفيروسات:

تخلف الفيروسات آثارا وتصاحبها عدت اعراض نوجزها في ما يلي:

4-3-1 . أعراض الإصابة بالفيروس:

كما أن لكل مرض الأعراض الخاصة به والتي تساعد الطبيب على التشخيص فإن الإصابة بالفيروسات كذلك تصاحبها أعراض معينة تدل على وجوده ومن أهم هذه الأعراض:

4-3-1-1. نفص شديد في الذاكرة:

- و يلاحظ أن للذاكرة ثلاث حالات, فقبل دخول الفيروس تكون الذاكرة في حالة طبيعية ثم بعد أن يبدأ الفيروس في العمل فإنه يلاحظ نقص شديد في الذاكرة وذلك لأن الفيروس في هذه الحالة يبدأ في تدمير الذاكرة وكذلك ملفات التبادل عن طريق إزالة البيانات المخزنة مما ينتج عنه توقف البرنامج العامل في الوقت ذاته لعدم وجود أي بيانات في الذاكرة ,وإنما يستبدلها بمجموعة أصفار في تعليمات التشغيل.

- **عرض رسائل الخطأ بدون أسباب حقيقية .**

- **تغيير في عدد ومكان الملفات وكذلك حجمها بدون أي أسبا ب منطقية**

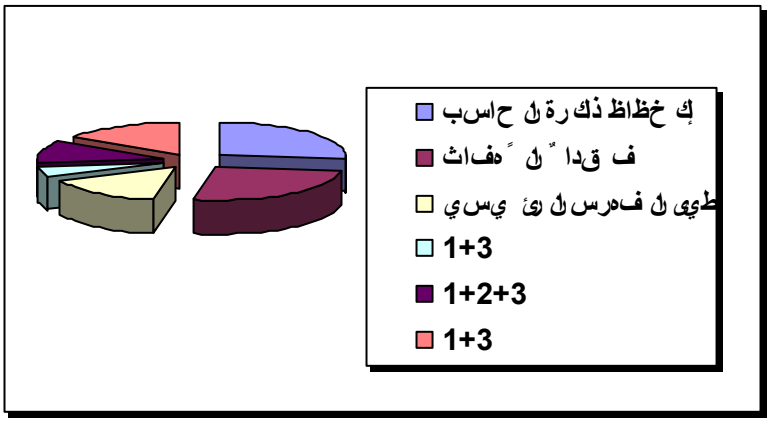
- **الخطأ في استعمال لوحة المفاتيح عن طريق إظهار أحرف غريبة أو خاطئة** عند النقر على حرف معين .

- استخدام القرص الصلب بطريقة عشوائية ..وتستطيع أن تلاحظ ذلك من إضائة لمبة القرص الصلب حتى وإن كان لا يعمل .

- اختلاط أدلة القرص أو رفض النظام العمل منذ البداية .

اكتظاظ ذاكرة الحاسب، فقدان الملفات، تحطيم الفهرس الرئيسي كل هذه الأعراض تنبأ عن دخول فيروس على جهاز الحاسب والجدول رقم:17 في الصفحة 145 يوضح أهم هذه الأعراض
أعربت (26,3 %) من عينة الدراسة أن اكتظاظ الذاكرة،فقدان الملفات من الذاكرة تعد أهم الأغراض المصاحبة للإصابة بالفيروس، وهذا راجع إلى أن الفيروسات لها قابلية التضاعف حيث يعمل الفيروس عند التو ضع في الذاكرة على إعادة نسخ نفسه مما يؤدي إلى اكتظاظ الذاكرة وهذا ما يسبب ثقل الجهاز وبطئ في

تنفيذ العمليات، كما يتميز الفيروس بالقدرة على التدمير فيعمل على تدمير الملفات ومنه تفقد من ذاكرة الحاسب،وهناك بعض الفيروسات التي تصل درجة خطورتها إلى حد تحطيم الفهرس الرئيسي للملفات كما يمكن أن تجتمع كل هذه الأعراض معا،الشكل البياني التالي يوضح نسب هذه الأعراض حسب عينة الدراسة :



الشكل رقم:12 أعراض الإصابة بالفيروسات

4-3-2. الأضرار التي تترتب على الإصابة بالفيروس:[65]

إن الأضرار التي يمكن أن تصيب الحاسب الآلي من جراء الفيروسات كثيرة جدا وتجدر الإشارة إلى أن الفيروس بمجرد أن يتنشط فإنه يؤدي إلى حدوث واحد أو أكثر من الأضرار التالية:

4-3-2-1. ملء ذاكرة الحاسب بالنفايات:

بما أن الفيروسات تنتشر بسرعة كبيرة ويحتل أماكن عديدة في ذاكرة الحاسب إذن فإنه يترتب على ذلك ملأ الذاكرة بالنفايات وبمعنى آخر عندما يحتل الفيروس لهذه الأماكن فإنه يجعلها غير صالحة للاستعمال مما يصيب المستخدم بخسارة مادية فادحة.

4-3-2-2. فقد ملفات من الذاكرة:

يترتب على تكاثر الفيروس في ذاكرة الحاسب خلقه لحياة ذاتية لنفسه وعندئذ يمارس الفيروس تدميره للذاكرة من خلال مسح أجزاء من الملفات المخزنة مما يجعل الملف غير قابل للاسترجاع ومن ثم لا يستطيع المستخدم أن يصل إلى إلى الملف المفقود وبالتالي لا يستطيع أن يستخدم البرنامج.

4-3-2-3. تحطيم الفهرس الرئيسي:

---

[65]- العريان ,محمد علي.المرجع السابق.ص..93

بعض الفيروسات تقوم أحيانا بالهجوم على الفهرس الرئيسي لنظام الحاسب فيستخدم في ذلك عدة وسائل منها تغيير حرف واحد في هذا الفهرس والذي يؤدي بدوره إلى عدم التمكن من الوصول إلى أي ملف على القرص رغم وجود الملفات فعليا.

4-3-2-4. فقد قطاع التشغيل بالقرص:

وهذا القطاع هو الذي يتم بواسطته بدأ تشغيل الجهاز وعند تغيير النتائج الموجودة به لا يمكن تشغيل الحاسب من دلك القرص.

4-3-2-5. كتابة رسالة مطبوعة على الطابعة:

عند الكتابة في الحاسب وطباعة ما تم كتابته تظهر رسالة أخرى نتيجة لتغيير مكان الحروف على الطابعة ملم تستهلك المزيد من الوقت والجهد للإعادة.

4-3-3. أنواع دمار الفيروسات:

يختلف أنواع الدمار الذي تسببه الفيروسات حسب نوعية الفيروس المتسبب فيه ومدى خطورة ومنه نجد:

4-3-3-1. دمار تافـــــه:

وهو ما تسببه الفيروسات غير المضرة وكل ما يجب فعله هو التخلص من هذا الفيروس حيث لا يستغرق وقتا لإزالته.

4-3-3-2. الدمار الثانوي:

وتسببه الفيروسات الثانوية **minore virus** وتسببه الفيروسات الثانوية حيث تتسبب في تغيير أو مسح لواحد أو أكثر من الملفات القابلة للتفنيد

4-3-3-3. الدمار المعتدل:

ويتسبب فيه الفيروس المعتدل والذي يمكن جمع الملفات الموجودة على القرص الصلب عت طريق لإعادة تهيئة أو إستبدال المعلومات بكنابة معلومات أخرى تافهة فوقها.

4ـ3ـ3ـ4.الدمار الرئيسي :

يؤدي الفيروس إلى تخريب المعلومات كلية.

الفصل الخامس

الفصل الميداني

الفصل الميداني

في مجال الإعلام الآلي أن ذلك مجرد خرافة ابتدعها أحد كتاب قصص الخيال العلمي, وأن وسائل الإعلام تحاول ترسيخها في أذهان الناس كحقيقة رغم أنها لا تمت إلى الواقع بصلة ، ولقد امتدت تلك الظاهرة واتسعت حتى باتت تشكل خطرا حقيقيا يهدد ثورة المعلوماتية التي فجرتها التقنيات الحديثة؛ فمن بضع فيروسات تعد على الأصابع في السنة الأولى إلى عدد يقدر بالملايين في يومنا هذا، وفي كل يوم تكتشف أنواع جديدة من الفيروسات المختلفة التأثير والشراسة، ومن الفيروسات البسيطة إلى الفيروسات المكارة والذكية التي تتفنن في التغير والتخفي والتحول؛ ترى ما حقيقة هذا الوباء وإلى أي حد يشكل خطرا على بنية المعلومات الكونية ؟ هذا ما سأجيب عليه في هذا الفصل.

تعد الفيروسات الوباء الأول الذي يهدد البيئة الإلكترونية وفي ما يلي أهم أبجديات هذا العالم:

4-1-1. ماذا نعني بالفيروس:

4-1-1-1. ندة تاريخية عن الفيروسات:

إستسقى مصطلح فيروس من العلوم البيولوجية وهو يعني باللاتينية «سم" وكان أول ظهور معروف لفيروس الكمبيوتر عام 1981 حيث كان بغرض علمي كما يقول المؤرخون و يعتبر البذرة الأولى التي أثمرة لتشكل شجرة الفيروسات الحالية؛ وكان الفيروس ينشر عن طريق الأقراص المرنة و يعمل على نظام (أبل **APPLE 2**) يكتفي هذا الفيروس بإظهار مقطع شعري على شاشة الحاسب دون أن يقوم بأية عملية تخريبية أو تدميرية على النظام.

أما عام 1983 في شهر نوفمبر بالتحديد كانت أول تجربة علمية مسجلة لفيروس وتم تقديمها في مؤتمر أمني خاص بالحاسب الآلي وكان الفيروس يعمل على نظام اليونكس في ذلك الوقت.

أما أول ظهور لفيروس ينتقل عن طريق الأقراص المرنة في نظام الدوس فكان الأصل فيه كما يقال يعود لأخوين في باكستان استطاعا تحليل الجزء المشغل في القرص ، ومن تم قاما بتطوير طريقة عبقرية لإصابته بالفيروس وأطلقا عليه المخ (**BRAIN**)؛ وفي نفس العام شهد العالم الحاسوبي أول ملف تجسس انتقل عن طريق برنامج مجاني يدعى **PC.WRITE** ؛ كما شهد هذا العام ظهور فيروس **VIRDEM** المدمر لكن هذا الأمر ليس تابت بشكل قطعي.

1987 أول ظهور لفيروسات تستهدف ملفات التشغيل **EXE.COM**التي كان نظام الدوس يعتمد عليها بشكل كلي وهو نفس العام الذي شهد انطلاق فيروس "القدس " الذي امتد حول العالم ليشكل

أول تهديد فعلي للحاسبات ؛ ثم ظهور أول دودة الأنترنيت **IBM** مسماة دودة الكريسماس والتي كانت تعيد نسخ نفسها 500ألف مرة بالساعة.

1988 ظهور فيروس يدعى الماك ماج **MAC MAG**ومن ثم إنشاء منظمة السيرت **www.cirt.org**لمواجهة أخطار الفيروسات والديدان بعد أن تسببت دودة موريس في إغلاق الكثير من الأجهزة على الأنترنت[66].

الأعوام التالية شهدت ظهور العديد من الفيروسات إلا أن عام 1990 شهد ظهور تنافس تطوير الفيروسات بين المبرمجين ونشرها على الأنترنت.

في عام 1995 ظهر فيروس الماكرو والذي يستهدف برنامج الورد

1996 بروز فيروسات خصيصا لمهاجمة أنظمة تشغيل الوندوز 95

1998 ظهور أو فيروس جافا في العالم، وفي 1999 انفتحت نافذة الجحيم على الأنترنت وبدأ عصر جديد من التهديدات ابتدأها فيروس ملسا الذي جمع بين فيروس الماكرو ودودة الأنترنت والذي تسبب في تعطيل الكثير من الخوادم لكبريات الشركات.

وفي الأعوام التالية ظهرت العديد من الفيروسات التي تسببت بخسائر تقدر بملايير الدولارات و لم تكن بالضرورة بنفس الطبيعة إلا أنها اتفقت جميعا على كونها الخطر الأكبر الذي يهدد الحاسبات.

2000 اكتشاف فيروس وينوكس والذي استهدف منصات تشغيل الويندوز ولسنكس معا ليكون الأول من نوعه في هذا المجال[67].

4-1-1-2. تعريف الفيروس:

وهنا يمكن إيراد عدة تعاريف نذكر منها:

1- برنامج صغير ولكن خبيث طور خصيصا لتنفيذ أعمال تخريبية علي الحاسب الآلي يحتوي هذا النوع من البرامج في معظم الأحيان علي أوامر تخريبية معينة في نص الشفرة وتختلف التي تكتب بها وتنفذ عند تحقيق شروط معينة وتختلف طرق الإصابة بالفيروسات فمنها ما ينسخ نفسه داخل ملفات ذات هيئة معينة ومتوافقة مع ما هو مصمم له وكلما تم استدعاء هذه الملفات أو تشغيلها ويتحقق بالبيئة المحيطة

ومن هذه البرامج الخبيثة ما ينسخ نفسه في الذاكرة مما يؤدي إلى بطئ شديد في عمل الجهاز ومنها ما يقوم بتخريب نظام الإدخال والإخراج الأساسي في الوقت الذي تزداد فيه خبرة وذكاء مؤلفي (مصممي)

---

2 – الجنبيهي ,منير محمد ؛ الجنبيهي , ممدوح محمد. **أمن المعلومات الإلكترونية**.الإسكندرية:دار الفكر الجامعي , 2005.صص48-49.[66]

[67]– الجنبيهي ,منير محمد ؛ الجنبيهي , ممدوح محمد. لأمن المعلومات الإلكترونية.المرجع السابق. ض.50.

الفيروسات وبالتالي زيادة عدد الفيروسات وأنواعها يتم تطويرها في تقنيات مكافحة تلك الفيروسات للتصدي لها وإزالتها قبل حدوث أي الضرر [68].

2- كما يعرف أيضا بأنه برنامج حاسب مثل أي برنامج تطبيقي آخر ولكن يتم تصميمه بواسطة أحد المخربين لهدف محدد هو إحداث أكبر ضرر ممكن بنظام الحاسب ولتنفيذ ذلك يتم إعطائه القدرة على ربط نفسه ببرامج آخرى وكذلك إعادة إنشاء نفسه حتى يبدو أنه يتكاثر ويتوالد ذاتيا وهذا يتيح له قدرة كبيرة على الإنشار بين البرامج المختلفة وكذلك بين المواقع المختلفة في الذاكرة حتى يحقق أهدافه التدميرية كما أن إنتشار الفيروس لا يقتصر على النظام الذي يتواجد به ولكنه ينتقل أيضا إلى نظم أخرى قد تكون أبعد مسافة ممكنة على هذا النظام ويعود هذا الإنتشار إلى عاملين أساسيين هما:

أ- التوافق: وهو يعني قدرة البرامج الواحد على التشغيل على أنواع مختلفة من الحواسب وإصدارات مختلفة من نظم التشغيل وهذا العامل رغم تأثيره الإيجابي والهام بالنسبة لتطوير النظم أن أثره على إنتشار الفيروس كان كبير.

ب – وسائل الإتصال:

وهي الوسائل التي أدت إلى ريط عدد من أجهزة الحاسب بشبكة الأن ترنيت و اتصالهم من خلالها وهذه الأجهزة قد تكون في نفس الوقع وقد تكون في مواقع مختلفة [69]

4-1-1-3. لماذا سمي بالفيروس[70]:

تطلق كلمة الفيروس أساسا على الفيروسات التي تنقل الأمراض عن طريق انتقالها من إنسان مريض إلى إنسان آخر وبمجرد انتقالها إلى الإنسان تتكاثر حتى تصيب الأجهزة العضوية.

والفيروس الخاص بالحاسب يقوم بعمل مشابه لذلك ، حيث أنه عبارة عن برنامج يصممه بعض المتخصصين لأهداف تخريبية مع إعطائه القدرة على ربط نفسه ببرامج أخرى ثم يتكاثر وينتشر داخل النظام حتى يتسبب في تدمير هاما؛ وهناك أوجه تشابه متعددة بين الفيروس العضوي وفيروس الحاسب يمكن تلخيصها في ما يلي:

- يقوم الفيروس العضوي بتغيير الخصائص العضوية لخلايا الجسم ويقوم فيروس الحاسب بتغيير وظائف برامج لأخرى.

---

1 – الربيعي ,محمد,شعبان أحمد أحمد ,وآخرون. المعجم الشامل لمصطلحات الحاسب الآلي ة الأنترنت.مكتبة السيكان الرياض 2001ص 446

1- طلية.محمد فهمي المرجع السابق ص.34.

[70]– – طلية. محمد فهمي.؛ عبد الوهاب، مصطفى رضا....وآخرون .فيروسات الحاسب وأمن البيانات، 1996.موسوعة دلتا كمبيوتر 8

- يتكاثر الفيروس العضوي ويتسبب في أنتاج فيروسات جديدة ويقوم فيروس الحاسب بإعادة إنشاء نفسه.

- الخلية التي تصاب بالفيروس العضوي لا تصاب بنسف الفيروس مرة ثانية وتحدث نفس الشيء مع الفيروس حيث يقوم باختيار البرنامج المطلوب نقل العدوى فإن وجد أنه سبق إصابته به لا يصيبه مرة ثانية وينتقل إلى برامج أخرى

- الجسم الذي تنتقل إليه العدوى قد يظل مدة طويلة دون ظهور أعراض المرض عليه ويقوم برنامج الحاسب بأداء وظائفها لمدة طويلة دون ظهور أخطاء نتيجة وجود الفيروس

- من ذلك ينضح سبب إطلاق تسمية الفيروس رغم أنه في الحقيقة ليس إلا برنامج مثل البرامج الحاسب ولكنه يختلف عنه في الوظائف التدميرية.

4-1-2. خصائص الفيروس:

كما سبق ذكره فإن الفيروس هو برنامج له صفات التكاثر والمضاعفة والاختفاء أو التخفي والإننفجار وعلى هذا الأساس يمكن ذكر أهم الخصائص التي يميز بها الفيروس في ما يلي:

4-1-2-1- القدرة على الاختفاء:

فالفيروس ما هو إلا برنامج أو القدرة على الاختفاء عن المستخدم والتمويه غليه وهو يستخدم وسائل متعددة في الاختفاء ومنها الارتباط بالبرامج الشائعة الاستعمال حيث أن مستخدم للحاسب الشخصي يهتم بتوفير البرامج التي تمكنه من الاستفادة من خصائص الحاسب؛ وبعض المستخدمين يقوم بنسخ هذه البرامج دون السؤال عن مصدرها وعند تشغيلها ينتقل الفيروس إلى القرص ويقوم بأعماله التدميرية ؛ وهناك فيروسات تدخل إلى الحاسب كملفات متخفية بحيث لا يستطيع المستخدم ملاحظة تواجدها عن طريق فهرس الملفات وهناك بعضا منها يستقر في أماكن معينة حيث يصعب العثور عليها ثم تبرمج على تاريخ معين ثم تقوم بتنفيذ وتشغيل نفسها في هذا التاريخ , وهناك أنماط أخرى من الفيروسات تقوم بإخفاء أي أثر على تواجدها حيث تظل البرامج المصابة تعمل بكفاءة دون أخطاء مدة طويلة بينما يقوم هو بالإنتقال من برنامج إلى آخر بخفة [71].

1 - الرومي , محمد أمين. جرائم الكمبيوتر والأنترنت. الإسكندرية: دار المطبوعات الجامعية ,2003.ص.28

4-1-2-2. الانتشار:

يتميز فيروس الحاسب بقدرة كبيرة على الإنتشار ومن أهم الوسائل التي تساعد على ذلك إنتشار وسائل الإتصال الحديثة التي تجعل الفيروس ينتقل بسرعة من حاسب إلى آخر شبكة الأنترنت إلى ملايين المستعملين وكذلك توافق الأجهزة الذي يساعد الفيروس على العمل وإذا قارنا بين إنتشار الفيروس العضوي وفيروس الحاسب نجد أن هذا الأخير أسرع إنتشار بدرجة كبيرة حيث يمكنه في ثوان محدودة الإنتقال من قارة إلى أخرى كما يمكنه الإنتقال إلى عدد ضخم من المستخدمين في نفس الوقت بينما لا يستطيع الفيروس العضوي فعل ذلك وعند انتقال الفيروس إلى الحاسب فإنه ينتشر بسرعة كبيرة داخل الذاكرة حيث أنه يربط نفسه بالبرامج المخزنة داخل الذاكرة كما يقوم بعمل نسخ كبيرة لنفسه [72].

3- القدرة على الإختراق:

يتميز فيروس الحاسب بقدر ة كبيرة على الدخول والتسلل واختراق الحصون والمواقع التي يقيمها المستخدم بتحميل هذه البرامج حيث يكون الفيروس عادة موجودا في احد البرامج المفيدة التي يحتاجها المستخدم لتشغيل الحاسب ثم يقوم المستخدم بتحميل هذه البرامج وإدخال الفيروس دون أن يشعر وبعض الفيروسات يتم إدخالها بإستخدام حصان طروادة حيث يرتبط بأحد البرامج المثيرة التي تجدب المستخدم وتثير لديه حب الإطلاع وعند تحميل هذه البرامج يبدأ الفيروس في الإنتشار وتنفيذ عملياته التدميرية [73]

4- القدرة على التدمير:

عندما يدخل الفيروس إلى الكمبيوتر يظل ساكنا حتى تبدأ لحظة الصفر التي يبدأ عندها في الإنتشار والحركة وساعة الصفر هذه إما أن تكون كلمة معينة كتبها المستخدم أو إشارة معينة أو عند تاريخ معين ويعمل الفيروس غالبا على محور البيانات المخزنة في الذاكرة[74]

4-1-3. دورة حياة الفيروسات وانتشارها:

4-1-3-1. . دورة حياة الفيروس[75]:

وهناك سقمراحل لدورة حياة فيروس الكمبيوتر تتمثل في:

1- مرحلة التصميم

2- طلية.محمد فهمي المرجع السابق ص 64

1- طلية.محمد فهمي المرجع السابق ص 64

74

[75]- دورة حياة الفيروس (على الخط المباشر).(14-12-2006) متوفر على الخط المباشر
http// www.jparisnajd.com /

عملية تصميم فيروس جديد تحتاج إلى شخص على درجة عالية من الكفاءة في التعامل مع لغات البرمجة على الحاسب الشخصي مثل لغة البيسك والجافا والفيجوال **c++**

وقد لا تبح هذه الخبرات والكفاءات ضرورية في المستقبل حيث يتم تقديم مساعدات كبيرة على مستوى شبكة الأنترنيت للمبرمجين المبتدئين الذين يردون القيام بتصميمات

2-مرحلة الإنتشار:

عادة ما يقوم مطورو الفيروسات بنشر فيروساتهم على أكبر عدد من الحواسب الشخصية قبل أن يبدأ الفيروس بإحداث الآثار التدميرية المكلف بها والسبب في ذلك وهو نشر أكبر عدد من النسخ قبل أن تنتبه شركات مقاومة الفيروسات لوجوده فتبدأ بوضع البرامج المضادة لها وفي هذه المرحلة تصل الفيروسات إلى الحاسبات وتظل بها دون أن تظهر أية أعراض على الحاسبات المصابة.

3- مرحلة النشاط:

تبدأ الفيروسات في النشاط ولإحداث الآثار التدميرية التي تمت برمجتها للقيام بها عند وقوع حدث معين وقد تتم برمجته لكي ينشط في توقيت معين أو عند تشغيل برنامج ما أو عند الإتصال بشبكة الأن ترنيت أو عند وصول جزء ثان من الفيروس إلى الحاسب وتنوع الأعمال التخريبية من تدمير الملفات المخزنة على الحاسب أو استهلاك المساحات ووحدة التخزين

4- مرحلة اكتشاف الفيروس:

قد لا تتبع هذه الخطوة دائما عملية نشاط الفيروس فقد تكون الشركات المنتجة لبرامج مقاومة الفيروسات أكثر ذكاء بحيث تكتشف وجود الفيروس قبل أن ينشط ومن تم العمل على مقاومته.

5 – مرحلة المواجهة:

في هذه المرحلة تقوم شركات إنتاج برامج مقاومة الفيروسات تعديل برامجها وملفاتها لكي تتعامل مع الفيروس الجديد ولكل فيروس بصمة خاصة به وهي (الكود الذي تكتب به أوامر الفيروس بأحد لغات الحاسب) ويتم إضافة هذه البصمة إلى ملفات البرامج بعد ذلك يقوم المستخدمون بتويل الملفات على موقع الشركة على شبكة ويقومون بتحدث البرامج بعد التعديل. هذه المرحلة قد تصل إلى ستة أشهر حسب نوع الفيروس

6- مرحلة الإستئصال:

بعد فترة من القيام بعدد كبير من حديث برامجهم ,تنحصر آثار الفيروس بالتعديلات التي تكتشف وتقضي على الفيروس بحيث تنخفض درجة تهديده لمجتمع المعلومات

4-1-3-2. عوامل إنتشار الفيروسات[76]:

هناك العديد من العوامل التي تقف وراء الإنتشار الكبير للفيروسات في هذه الأيام وهذه العوامل لخصها التقرير الذي قدم إلى مجلس بحوث أمن المعلومات في الولايات المتحدة فيما يلي:

5 إنتشار الشبكات:

بازدياد ارتباط الحاسبات ببعضها من خلال شبكة الأنترنت ازدادت سهولة شن الهجمات كما ازداد عدد هذه الهجمات تبعا لذلك وأصبح من النادر اليوم أن نرى جهاز حاسب غير مرتبط بشبكة الأنترنت ويدعم ذلك الاتجاه ما نشهده من الاعتماد المتزايد لدى الأفراد والشركات على البريد الإلكتروني كوسيلة اتصال وتواصل وباختصار شديد فإن مهاجم اليوم لا يحتاج إلى الوصول المباشر إلى جهاز الحاسب لزرع فيروسه كما ساعد انتشار الشبكات على شن أنواع آلية من الهجوم لا يتدخل فيها البشر وقد حدث في فيبراير 2000 هجوم تسبب في عرقلة الخدمة في العديد من مواقع التجارة الإلكترونية

6 زيادة تعقيد النظم

بازدياد حجم نظم المعلومات ودرجة تعقيدها زاد إعتمادها على نظم التشغيل في توفير الحماية الأمنية لها ونظم التشغيل نفسها تضم آلاف من البرامج التي تحتوي على عشرات الملايين من الأوامر وفي نظم بهذا الحجم لا يمكن تفادي الثغرات ,وزاد تفاقم المشكلة استخدام لغات لا تتمتع بالحماية الأمنية مثل لغة **c++** التي لا تقاوم أبسط أنواع الهجوم

ومن جهة أخرى فإن التطبيقات الضخمة المعقدة تشكل بيئة صالحة لنمو الفيروسات فلا يلحظ وجودها أحد , فقد نستطيع فحص برنامج صغير وتأكيد نظافته وخلوته من الفيروسات ولكن من المستحيل عمل ذلك في تطبيقات اليوم التي تملأ حياتنا الشخصية ناهيك عن التطبيقات الضخمة التي تعمل في الشركات والدوائر الحكومية

3- سهولة الإضافة إلى النظم:

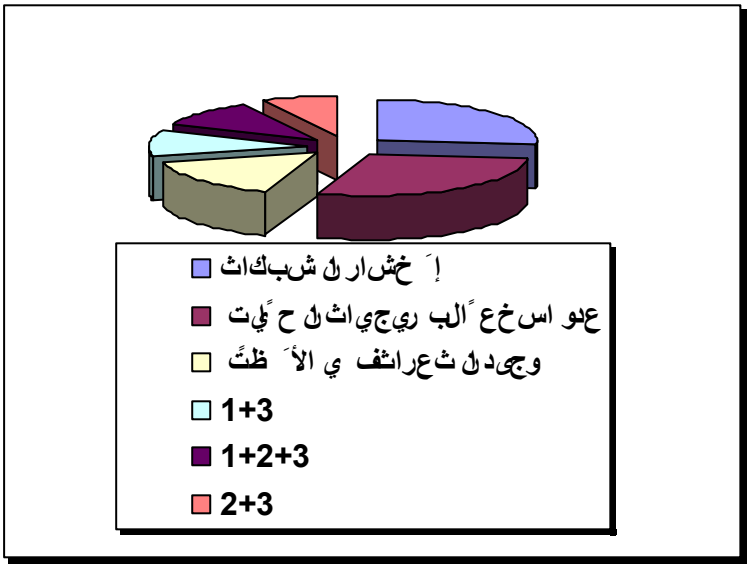
تفخر الكثير من نظم المعلومات اليوم بأنها نظم قابلة للتوسع بمعنى أنها تقبل التحديث والإضافة سواء من جانب المحدد أو المستخدم وتأتي هذه الإضافات بشكل برامج منقولة ولذلك فُن مع ظم البرمجيات ونظم التشغيل الحالية تجدها قابلة للتوسع مما سهل اقتحام الفيروسات وأوضح مثال على ذلك الكيفية التي انتشر بها فيروس (ميلسا) حيث استغل قابلية البرنامج الإلكتروني (أوت لوك) **oritlook** لتوسع فقد تم كتابة الفيروس في صورة رسالة إنخد بها معظم المستخدمين.

---

[76]- أمن شبكات المعلومات ص 167

إذن وكما سبق الإشارة إليه فإن البيئة الإلكترونية أدت إلى قلب العديد من الأمور؛ حيث ظهرت العديد من الإفرازات منها ما هو سلبي ومنها ما هو إيجابي، وتعد الفيروسات واحدة من أبرز الإفرازات السلبية وقد ساهم في انتشاره هذه الأوبئة عدة أمور موضحة في الجدول رقم **15** الصفحة 144

وفقد أعرب الطلبة على أنه ومهما اختلفت الأسباب التي تؤدي إلى إنتشار الفيروسات بشكل رهيب فإن أهمها على الإطلاق هو عدم استعمال برمجيات الحماية بنسبة (28,9 %) وذلك على الرغم كمن الأهمية التي تكتسيها هذه البرمجيات، ثم يليها إنتشار الشبكات بنسبة (26,3 %)، حيث أن الشبكات اكتسحت العالم المعاصر مما جعلها تشكل مناخا ملائما لنمو وتطور الفيروسات، كما أدى ظهور الشبكة العنكبوتية إلى استعمالها كناقل ممتاز لنشر هذه الفيروسات؛ ومن أهم أسباب انتشارها كذلك وجود ثغرات كثيرة في الحاسب وأنظمة التشغيل وهذا ما عبر عنه (17,7 %) من العينة، كما تشكل هذه الأسباب إذا توفرت جميعها لأكبر وأحسن بيئة لالتهاب الشبكة بهذه الفيروسات وهذا ما يوضحه الشكل البياني التالي:



الشكل رقم :11 أسباب إنتشار الشبكات

4-1-3-3. وسائل إنتقال الفيروس[77]:

يمكن لفيروس الحاسب الإنتقال داخل شبكة الإنترنيت أو أي شبكة محلية عن طريق وسائل أربعة:

1- البريد الإلكتروني:

ينتقل الفيروس عبر برنامج أوت لوك وأوت لوك اكيبريس وذلك عن طريق ملف يلصق بالرسالة التي ترد عبر البريد الإلكتروني ويحمل ملف إسم **REACLM EXE** وتظهر له أيقونة بقوته **ATML** وذلك في

[77]- حجارى , عبد الفتاح بيومي. النظام القانوني لحماية الحكومة الإلكتورنية. الكتاب الثاني و الجنائية المعلوماتية لنظام الحكومة الإلكترونية. الإسكندرية:دار الفكر الجامعي 2003 ص ص 74 - 78

محاولة لخداع المستخدم ويكفي قيام المستخدم بالنقر على الملف حتى ينسخ الفيروس نفسه و يمد رسالة تلقائية ترسل إلى جميع العناوين الخاصة بالبريد الإلكتروني التي توجد في دفتر عناوين المستخدم.

2- مزود ويب ISS

يضع الفيروس عناوين عديدة بشكل ؟؟؟؟؟ لما يفعله فيروس **CODERED** بحثا عن مزودات **ISS**والتي تتضمن ثغرات أمنية يستفيد منها في عملية الإنشار ويحاول الفيروس كذلك الاستفادة من دودة فيروس**CODERED2** التي تنتشر عبر مزود **ISS** حيث كانت الدودة تترك برنامج باب خلفي في هذه المزودات كي تسمح للمخترق بالدخول إليها والسيطرة عليها فيما بعد

3- متصفح الأنترنت:

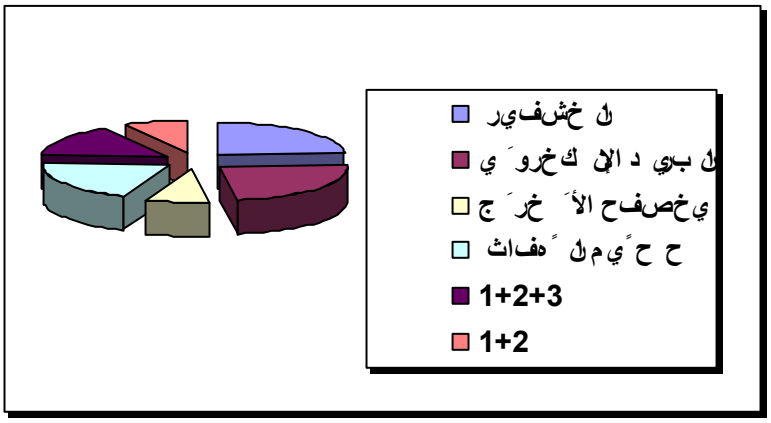
بعد أن يصيب الفيروس أحد المزودات – شبكة الأنترنيت – بالطريقتين السابقتين بنسخ شفرة معينة إلى كل صفحات (**asp- htmail- htm**) التي توجد في المواقع التي يستضيفها مزود -الأنترنيت – وعند زيارة الموقع المصاب من طرف أحد المستخدمين ويبد أفي تتزيل ملف منه يشتعل الفيروس تلقائيا ويصيب جهاز المستخدم

4- المشاركة على الملفات:

تسمح هذه الطريقة للفيروس أن ينتشر عبر الشبكات المحلية التيوجدت ملفات أو مجلدات مشتركة عبر شبكة ميكروسوفت .

وكما سبق الإشارة إليه فإن الفيروسات تنتشر بعدة طرق أهمها البريد الإلكتروني وكذا تحميل الملفات من الأنترنت والجدول 16 الصفحة 144 بوضح ذلك

ترى عينة الدراسة أن أهم طرق انتشار الفيروسات هي البريد الإلكتروني (31,5 %)،فمع إنتشار شبكة الانترنت أصبح البريد الإلكتروني الخدمة الأكثر شعبية والتي أدت إلى زيادة استخدام الشبكة وقد استغل صناع الفيروسات هذه الخدمة من أجل نشر سمومهم على الشبكة، كما يمكن أن يؤدي تحميل الملفات من الأنترنت خصوصا من المواقع المشبوهة إلى المساهمة في إنتشار هذه الأوبئة وهذا ما عبرت عنه (26,5 %) من عينة الدراسة إضافة على العديد من الطرق الأخرى كمتصفح الأنترنت ونوضح ما سبق ذكره بشكل أفضل بالرسم البياني التالي:



الشكل رقم: 12 طرق نشر الفيروسات

4-2. أنواع الفيروسات وأشكالها:

4-2-1. أنواع الفيروسات

إن الفيروسات مهما أختلف شكلها أو نوعها خاصة واحدة هي إلحاق الأدى والضرر بالبرامج إلي برمجت لإلحاق الأذى بها ويمكن أن نميز العديد من أنواع الفيروسات:

4-2-1-1. قطاع التشغيل bootseetor :

وتعتبر من أقدم الفيروسات وأكثرها إنتشار إذ تستطيع أن تصيب المقطع التشغيلي في الأقراص المرنة أو مقطع نظام تشغيل الدوس **dos** حيث أن كل الأقراص سواء كانت صلبة أو مرنة تملك قطاع تشغيل ويتكون من المعلومات الخاصة بشكل القرص (نوع البنية , نوع المعطيات) وتكمن خطورة هذه الفيروسات في قدرتها على إتلاف هذا الجزء ثم يقوم بأحد مكان قطاع تشغيل القرص المصاب بنسخة منه ثم ينقل المقطع الأصلي إلى مكان آخر في القرص [78] .

4-2-1-2. فيروسات الملفات:

وهي الفيروسات التي تلصق نفسها مع ملفات البرامج التنفيدية ذات الإمتداد **com exe** وقد يمتد أثرها ليصيب الملفات ذات الإمتداد **ouc , dry ,sys**.....ومع هذا النوع من الفيروسات فإن البرامج تصاب بمجرد بدأ تشغيل هذه الرمج[79] ويمكن تقسيم هذه الفيروسات إلى أربغة أنواع[80]:

---

78 -**types des virus informatique.(**en ligne) (23/02/2006)
fr escpotting.com/ seardr/ riduchon.html www.affiliate

2 - المرجع السابق

3 - شوقي , حسام المرجع السابق ص10

أ- الفيروسات المتطفلة:

التي تلصق نفسها بالملفات لكي تتكاثر وتبقي الملف الأصلي بحالة سليمة

ب- الفيروسات المرافقة:

التي تعتمد على قاعدة الأسبقية في التنفيد للملفات ذات الإمتداد **com** وتتمكن من نقل العدوى عن طريق إنشاء ملف جديد بدون ؟؟؟؟؟ الملف

ج- الفيروسات الرابطة:

وهي التي تصيب البرامج بتغيير المعلومات في جدول مواقع الملفات

د- الفيروسات المستبدلة:

التي تقوم بالكتابة فوق جزء من برنامج دون تغيير حجم الملف مما يؤدي إلى فشل الملف عند تنفيذه.

4-2-1-2. الفيروسات متعددة القدرة التحويلية:

وهذه الفيروسات لها القدرة الديناميكية على وتنفيذ الشفرات عند الإنتقال من ملف إلى آخر لكي يصعب اكتشافها [81].

4-2-1-4. فيروس الماكرو:

هذا النوع أيضا سريع الإنتشار بين المستخدمين خاصة أنه قادر على كل الطرق كالأقراص الصلبة والبريد الإلكتروني والبرامج المجانية ويعتبر من أحد أنواع الفيروسات والجدير بالذكر وهذا الفيروس لا يصيب إلا البرنامج التطبيقي الذي صمم لإتلافه فمثلا لو إن فيروس صمم ليصيب برنامج تحرير الكلمات والنصوص فإنهلا يستطيع إلحاق الأذى بأي برنامج آخر[82].

4-2-1-5. الفيروسات قطاع الإقلاع:

تستقر هذه النوعية من الفيروسات في الأماكن التي يقرأها الكمبيوتر بالقرص الصلب وينفد التعليمات المخزنة ضمنها عند الإقلاع ثم تصيب قطاع الإقلاع الخاصة بنظام الدوس بينما تصيب فيروسات الفئة الفرعية المسماة **MBR virus** قطاع الإقلاع الرئيسي للكومبيوتر كما يمكن أن يصيب الفيروس قطاع الإقلاع ةالملفات في وقت واحد ويطلق عليه - الفيروس المتعدد الأجزاء - [83].

---

[81]- شوقي ,حسام.المرجع السابق.ص. 10

2- **أروع كتاب في الهاكينغ**: الفيروسات.JOUAHARA2.CD.ROM

[83]- شوقي ,حسام.المرجع السابق.ص. 10

4-2-2. أشكال الفيروسات:

بعد تطرقنا بشيء من الإنجاز إلى أهم أنواع الفيروسات والتي من الممكن أن تصيب جهاز الحاسب وإلحاق الخراب والدمار به يجدر بنا الإشارة إلى أنه هناك عدة أشكال للفيروسات حيث أنها لا تتخذ نمطا واحدا ويمكن أن نلخص أهم أشكالها كما يلي[84]:

4-2-2-1.المتخفي: وهو الذي يختبئ في الذاكرة الرئيسية ويسيطر على القطاعات.

4-2-2-2. البطيء: كلما كان إنتشار الفيروس بطيئا كلما صعب إكتشافه والتخلص منه سريعا وأسلوب عما هذا الفيروس هو إصابة الملفات التي كان المستخدم ينوي تعديلها.

4-2-2-3. السريع: يصيب هذا الفيروس كل الملفات الحالية بمجرد دخوله إلى الحاسب وهو ليس خطيرا بشكل كبير.

4-2-2-4. المتعدد الأشكال: هي الفيروسات التي لو تتم مقارنة نسختين من الفيروس نفسه لا يتطابقان مما يصعب مهمة برنامج الحماية ويتطلب منها القيام بأمور كثيرة ومعقدة لاكتشاف هذا النوع.

4-2-2. أشهر الفيروسات:

4-2-2-1. أشهر فيروسات الحاسب

الفيروس الباكستاني: صمم هذا النوع من الفيروس من طرف باكستاني متخصص في المعلوماتية كان يبيع البرامج المعلوماتية بنصف دولار بينما سعرها في الولايات المتحدة الأمريكية 450 دولار.

الفيروس 13 أكتوبر: تعد نسبة الإصابة بهذا الفيروس قليلة أما سبب تسميته بهذا الإسم هو الشائعة التي ظهرت من أنه سوف يصيب أجهزة الحاسب جميعا في 13 أكتوبر 1989.

الفيروس العقل: وهو من فيروسات نظام التشغيل الدوس وتتمثل خطورته في أنه يكتب على قطاع التحميل للقرص مما يسبب تحميل الفيروس بمجرد تشغيل الجهاز وقبل تحميل أية برامج مضادة وهو ينقل العدوى إلى أي قرص بمجرد عرض الفهرس الخاص بهذا القرص ,ويتميز بقدرته على الإختفاء حيث يقوم بتخزين نفسه بالقطاعات التالفة من القرص[85].

فيروس الحب: ظهر هذا الفيروس في جميع أحاء العالم وبصفة خاصة بالولايات المتحدة الأمريكية وتقدر خسائر أمريكا منه نحو 10مليار دولار وقد اقتحم أنظمة الكمبيوتر العسكرية في وكالة الأمن القومي وقد انتشر هذا الفيروس عن طريق فتح البريد الإلكتروني للمستخدم تحت عنوان **LOVE** ثم لا يلبث أن ينتشر في كافة أنحاء الحاسب بمجرد فتحه.

---

[84]- - شوقي ,حسام.المرجع السابق.ص.14.

-1

فيروس مايكل أنجلو: أنطلق هذا الفيروس في 06 مارس 1992 بمناسبة الإحتفال بذكرى ميلاد الرسام الإيطالي مايكل أنجلو والذي توفي عام 1564 ولقد أصاب العديد من أنواع الحاسب [86].

4-2-2-2. أشباه الفيروسات:

1- الدودة:

برامج الدودة هي عبارة عن برامج مخصصة لاستغلال أية فجوات لكي تنتقل إلى الحاسبات الآلية عبر الوصلات التي تربط بينها وتجدر الإشارة إلى أن هده البرامج تتكاثر وتنتشر أثناء عملية انتقالها وتهدف إلى التقليل أو خفض كفاءة النظام ألمعلوماتي أو إتلاف نظم التشغيل والبيانات والملفات والبرامج [87].

ولقد ضربت نماذج كثيرة من هده الدودة شبكات الحاسب حول العالم نورد بعضا منها غي ما يلي [88]:

1-1 –الدودة مصاصة الدماء:

يعتبر بعض الدود خبيثا وبعضه حميدا وقد استخدمت شركة ّ زيدوكسّ

غي بداية الثمانينات دودة حميدة أسمتها الدودة مصاصة الدماء وكانت هده الدودة تظل خامدة طول النهار عندما يكون استخدام النظام الفي ساعات الذروة وفي الليل تستيقظ وتنشط وتستخدم المعالج بعد أن يكون قد تخفف عبء العمل لأداء بعض المهام المعقدة التي تحتاج إلى قدرات المعالج باستمرار.

1-2. دودة الأنترنت الهائلة:

لم يكن الاهتمام الموجه لهدا النوع من الفيروسات كبيرا حتى 3نوفمبر 1988 عندما أطلقت دودة الأنترنت الهائلة لتغزو الشبكة ففي أقل من ستة ساعات استطاع هدا البرنامج الذي لايتعد حجمه 99 سطرا أن يشل كل الأجهزة المرتبطة بالانترنت من نوع صن فاكس وعددها 6.000 جهاز ؛ وكانت هده الدودة عندما تصيب الجهاز تقوم بتشغيل برنامج صغير في خلفية الجهاز المصاب و لم يشعر أحد يهدا الأمر في البداية ؛ لولا خطأ بسيط من المبرمج وهو أن الدودة لا تقوم باختبار الجهاز إدا ما كان مصابا أم لا وكان من اثر دلك أن حدثت حالات كثيرة من تعدد الإصابة التي وصلت في بعض الحالات إلى المئات مما عرقل عمل الأجهزة ؛وتفاقم المشكل لاعتمادها على البريد الإلكتروني مما أدى ببعض المواقع إلى فصل نظمها عن الأنترنت.

2- القنابل:

2- العريان , على محمد. المرجع السابق.ص.90.

87- – العريان , محمد علي.المرجع السابق.ص.97.

88- داود , حسن الطاهر. **أمن الشبكات والمعلومات**. المرحع السابق. ص.

تعد القنابل إحدى الطرق التي تتلف بها المعلومات وهي على غرار باقي الفيروسات صممت لإحداث الضرر بالأنظمة والمعلومات وأهم انواع القنابل:

3 القنبلة المنطقية:

القنبلة المنطقية هي عبارة عن برنامج أو جزء من برنامج ينغد في لحظة معينة أو كل فترة زمنية منظمة ويتم وضعه في شبكة الأنترنت بهدف تحديد ظروف أو حالة النظام لغرض تسهيل تنفيذ عمل غير مشروع ؛ومن دلك مثلا إدخال التعليمات في برنامج تشغيل وهو البرنامج الذي يقوم بتحميل ذاكرة الحاسب بالبرنامج المراد تنفيده ؛وهو الذي ينفد في مرة عمل جديد وينصب البحث على عمل معين يمكن أن يكون محل للاعتداء كأن تسعي القنبلة المنطقية مثلا بالبحث عن حرف معين وليكن الألف في السجلات وعند الأمر بالحذف تتحرك متتالية وتقوم بإزالة هدا الحرف أينما وجدته ومن الأمثلة الواقعية التي استخدمت فيها 2- **القنبلة المنطقية:**

- تمكن خبير في نظم المعلومات غي الدنمارك من صنع قنبلة منطقية في نظام الحاسبات أدى إلى محو أكثر من مئة برنامج وقد تم أيضا محو النسخ الاحتياطية عند تشغيلها نظرا لانتقال آثار القنبلة إليها ثم ضبط الفاعل وحكم عليه بالسجن لستة أشهر[89].

2- القنبلة الزمنية:

أما عن القنبلة الزمنية فهي تثيرا حدثا في لحظة زمنية معينة بالساعة واليوم والسنة ويتم إدخالها في البرنامج وتنفد في جزء من الميلي ثانية أو دقائق بتاريخ المحدد سلغا ؛ وبمعنى آخر لأي خبير في صناعة البرامج أن يقوم بصناعة الفيروس إذا كان يضمر شرا للمستهدف ومن اهم الأمثلة التي إستجدمت فيها الهذا الأسلوب[90]:

في فرنسا قام خبير في نظم المعلومات بدافع الإنتقام على اثر فصله من المنشأ الذي يعمل فيه بوةضع قنبلة في شبكة المعلومات الخاصة بالمنشأ بحيث تنفجر بعد مضي ستة أشهر من رحيله وترتب عن ذلك إتلاف كل البيانات المتعلقة بها[91].

4-2-2-3.أحصنة طروادة* trojan horse [92]:

---

[89]- الرومي ,محمد أمبن.المرجع السابق.ص.57.

[90]- العريان , محمد علي.المرجع السابق.ص.57.

[91]- الرومي ,محمد أمبن.المرجع السابق.ص.57.

*- حصان طروادة: تقول الأسطورة أن طروادة كانت مدينة عظيمة منيعة الأسوار والحصون ولم يتمكن مقاتلي إسبارطة من دخولها رغم صبرهم في حصار المدينة الذي دام عشر سنوات وفي الأخير لجأوا إلى حيلة إدعاء الإنسحاب مخلفين وراءهم حصانا خشبيا هدية للطرواديين وكان الحصان يحوي في داخله ثلث الجيش الإسبرطي ,ثم فتح الباب لباقي الجيش بعد إدخال الحصان إلى المدينة.

* **تعريف:** حصان طروادة هو أح د الأساليب الهجوم الخطيرة التي تشبه الفيروسات, والتي تخفي مفاجأة شريرة تظهر في وقت معين ؛يطلق عليه اسم التروجان للاختصار وهو يختلف عن الفيروس في كونه لا يتكاثرولا يلتصق بالملفات وإنما هو برنامج مستقل بذاته ويحمل بين طياته نوقيته وأسلوب إستقاضه وبدئه النشاط وهناك العديد من هذه الأنواع تهاجم نظام اليونكس فتحل محل بعض تطبيقات الشبكة فقد تحتل تطبيق خدمة الإتصال عن بعد **Telenet** بحيث يقوم التروجان عند التعامل مع هذه الخدمة بتسجيل كل الأسماء التي تصل وكلمات السر الخاصة بها[93] .

* **كيف يصل التروجان إلى حاسوبك:**

- يرسل التروجان إلى حاسوب الضحية عن طريق البريد الإلكتروني كملف ملحق فعند استقباله وتشغيله وقد لا يرسل لوحده بل مع مجموعة كبيرة من الملفات.

- إذا كان الشخص من مستعملي أي سي كيو (**ICQ**) أو برامج المحادثة فقد يرسل له ملف مصاب.

- عندما نقوم بإنزال برنامج من أحد المواقع الغير موثوقة بها وهي كثيرة جدا.

- كتابة التروجان مباشرة على الحاسب حيث لا تستغرق العملية سوى دقائق معدودة.

في البداية كان تصميم التروجان لأغراض نبيلة مثل معرفة ما يقوم به الأبناء أو المظفون على جهاز الحاسب عند غياب المسؤول آو الأب من خلال ما يكتبه على لوحة المفاتيح ثم أصبح يستخدم لأغراض شريرة.

4-3. آثار الفيروسات:

تخلف الفيروسات آثارا وتصاحبها عدت اعراض نوجزها في ما يلي:

4-3-1 . أعراض الإصابة بالفيروس:

كما أن لكل مرض الأعراض الخاصة به والتي تساعد الطبيب على التشخيص فإن الإصابة بالفيروسات كذلك تصاحبها أعراض معينة تدل على وجوده ومن أهم هذه الأعراض:

4-3-1-1. نفص شديد في الذاكرة:

- و يلاحظ أن للذاكرة ثلاث حالات, فقبل دخول الفيروس تكون الذاكرة في حالة طبيعية ثم بعد أن يبدأ الفيروس في العمل فإنه يلاحظ نقص شديد في الذاكرة وذلك لأن الفيروس في هذه الحالة يبدأ في

---

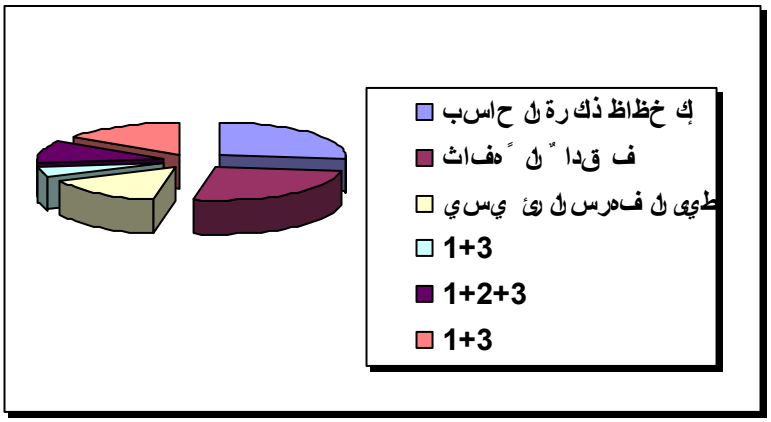
[92]- الفئر ,غبير الرضا.الأنترنت:النشأة والأخطار. مؤخودة من مجلة عجمال للعلوم والتكنولوجيا.مج6.ع.3 ,2001.ص.100.

[93]- داود ,حسن الطاهر.أمن شبكات المعلومات.المرجع السابق.ص.178.

تدمير الذاكرة وكذلك ملفات التبادل عن طريق إزالة البيانات المخزنة مما ينتج عنه توقف البرنامج العامل في الوقت ذاته لعدم وجود أي بيانات في الذاكرة ,وإنما يستبدلها بمجموعة أصفار في تعليمات التشغيل.

- **عرض رسائل الخطأ بدون أسباب حقيقية .**
- **تغيير في عدد ومكان الملفات وكذلك حجمها بدون أي أسبا ب منطقية**
- **الخطأ في استعمال لوحة المفاتيح عن طريق إظهار أحرف غريبة أو خاطئة** عند النقر على حرف معين .
- استخدام القرص الصلب بطريقة عشوائية ..وتستطيع أن تلاحظ ذلك من إضائة لمبة القرص الصلب حتى وإن كان لا يعمل .
- اختلاط أدلة القرص أو رفض النظام العمل منذ البداية .

اكتظاظ ذاكرة الحاسب، فقدان الملفات، تحطيم الفهرس الرئيسي كل هذه الأعراض تنبأ عن دخول فيروس على جهاز الحاسب والجدول رقم:17 في الصفحة 145 يوضح أهم هذه الأعراض
أعربت (26,3 %) من عينة الدراسة أن اكتظاظ الذاكرة،فقدان الملفات من الذاكرة تعد أهم الأغراض المصاحبة للإصابة بالفيروس، وهذا راجع إلى أن الفيروسات لها قابلية التضاعف حيث يعمل الفيروس عند التو ضع في الذاكرة على إعادة نسخ نفسه مما يؤدي إلى اكتظاظ الذاكرة وهذا ما يسبب ثقل الجهاز وبطئ في تنفيذ العمليات، كما يتميز الفيروس بالقدرة على التدمير فيعمل على تدمير الملفات ومنه تفقد من ذاكرة الحاسب،وهناك بعض الفيروسات التي تصل درجة خطورتها إلى حد تحطيم الفهرس الرئيسي للملفات كما يمكن أن تجتمع كل هذه الأعراض معا،الشكل البياني التالي يوضح نسب هذه الأعراض حسب عينة الدراسة :



الشكل رقم:12 أعراض الإصابة بالفيروسات

4-3-2. الأضرار التي تترتب على الإصابة بالفيروس:[94]

إن الأضرار التي يمكن أن تصيب الحاسب الآلي من جراء الفيروسات كثيرة جدا وتجدر الإشارة إلى أن الفيروس بمجرد أن يتنشط فإنه يؤدي إلى حدوث واحد أو أكثر من الأضرار التالية:

4-3-2-1. ملء ذاكرة الحاسب بالنفايات:

بما أن الفيروسات تنتشر بسرعة كبيرة ويحتل أماكن عديدة في ذاكرة الحاسب إذن فإنه يترتب على ذلك ملأ الذاكرة بالنفايات وبمعنى آخر عندما يحتل الفيروس لهذه الأماكن فإنه يجعلها غير صالحة للاستعمال مما يصيب المستخدم بخسارة مادية فادحة.

4-3-2-2. فقد ملفات من الذاكرة:

يترتب على تكاثر الفيروس في ذاكرة الحاسب خلقه لحياة ذاتية لنفسه وعندئذ يمارس الفيروس تدميره للذاكرة من خلال مسح أجزاء من الملفات المخزنة مما يجعل الملف غير قابل للاسترجاع ومن ثم لا يستطيع المستخدم أن يصل إلى إلى الملف المفقود وبالتالي لا يستطيع أن يستخدم البرنامج.

4-3-2-3. تحطيم الفهرس الرئيسي:

بعض الفيروسات تقوم أحيانا بالهجوم على الفهرس الرئيسي لنظام الحاسب فيستخدم في ذلك عدة وسائل منها تغيير حرف واحد في هذا الفهرس والذي يؤدي بدوره إلى عدم التمكن من الوصول إلى أي ملف على القرص رغم وجود الملفات فعليا.

4-3-2-4. فقد قطاع التشغيل بالقرص:

وهذا القطاع هو الذي يتم بواسطته بدأ تشغيل الجهاز وعدم تغيير النتائج الموجودة به لا يمكن تشغيل الحاسب من دلك القرص.

4-3-2-5. كتابة رسالة مطبوعة على الطابعة:

عند الكتابة في الحاسب وطباعة ما تم كتابته تظهر رسالة أخرى نتيجة لتغيير مكان الحروف على الطابعة ملم تستهلك المزيد من الوقت والجهد للإعادة.

4-3-3. أنواع دمار الفيروسات:

يختلف أنواع الدمار الذي تسببه الفيروسات حسب نوعية الفيروس المتسبب فيه ومدى خطورة ومنه نجد:

---

[94]- العريان ,محمد علي.المرجع السابق.ص.93.

4-3-3-1. دمار تافـــــه:

وهو ما تسببه الفيروسات غير المضرة وكل ما يجب فعله هو التخلص من هذا الفيروس حيث لا يستغرق وقتا لإزالته.

4-3-3-2. الدمار الثانوي:

وتسببه الفيروسات الثانوية **minore virus** وتسببه الفيروسات الثانوية حيث تتسبب في تغيير أو مسح لواحد أو أكثر من الملفات القابلة للتفنيد

4-3-3-3. الدمار المعتدل:

ويتسبب فيه الفيروس المعتدل والذي يمكن جمع الملفات الموجودة على القرص الصلب عت طريق لإعادة تهيئة أو إستبدال المعلومات بكنابة معلومات أخرى تافهة فوقها.

4ـــ3ـــ3ـــ4.الدمار الرئيسي :

يؤدي الفيروس إلى تخريب المعلومات كلية.

. أمن المعلومات: الماهية والأنواع:

ونتطرق في هذا العنصر إلى أهم جوانب أمن المعلومات

5-1-1. ماهية أمن المعلومات:

على ضوء التطورات المتسارعة في العالم والتي تؤثر في الإمكانيات والتقنيات المتقدمة المتاحة الرامية إلى حذف منظومات الحواسب بغية السرقة أو تخريب المعلومات أو تدمير الحواسب ومراكزها أدى إلى التفكير الجدي لتحديث الأساليب والإجراءات الدفاعية والوقائية وذلك تبعا للإمكانيات المتوفرة وهذا ما سأتطرق إليه بالتفصيل في هذا الفصل من تعريف لماهية أمن المعلومات وكذلك أساليب الحماية سو اء القانونية أو الفنية أو الأخلاقية.

5-1-1-1. تعريف أمن المعلومات.

أمن المعلومات من الزاوية الأكاديمي هو العلم الذي يبحث في نظريات وا ستراتجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها ؛ ومن زاوية تقنية هو الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات الداخلية والخارجية ؛ ومن زاوية قانونية فإن أمن المعلومات هو محل دراسات وتدابير حماية سرية وسلامة محتوى وتوفير أمن المعلومات ومكافحة أنشطة الاعتداء عليها واستغلال نظمها في ارتكاب الجريمة وهو هدف وغرض تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية[95].

كما يعرف المعجم الموسوعي لمصطلحات مكتبات ومعلومات أمن المعلومات على أنه إجراءات خاصة تحول دون فقدان أو فساد البيانات أو استعمالها دون تفويض [96] ؛ ومنه يمكن القول أن أمن المعلومات هي

---

[95]- **أمن المعلومات ماهيتها وعناصرها وإستراتيجياتها**. [على الخط المباشر]. زيارة يوم 2005/12/25 متوفر على الموقع http //www.arablow.com

[96] الشامي ,أحمد محمد. المرجع السابق.

مجموع الإجراءات والتدابير الوقائية التي تستخدم سواء في المجال الفني أو الوقائي لصيانة المعلومات وحمايتها من الدخلاء أو الاستعمال غير قانوني لها.

إن أغراض ووسائل أمن المعلومات كذلك هدف التدابير في هذا الحقل هو ضمان الحماية للعناصر التالية :[97]

1- السرية أو الموثوقية : confidentiality: وتعني التأكد من أن المعلومات لا تكشف ولا يطلع عليها من قبل أشخاص غير مخولين بذلك.

2- التكاملية وسلامة المحتوى integrity:

التأكد من ان محتوى المعلومات صحيح و لم يتم تعديله أو العبث به بشكل خاص لن يتم تدمير المحتوى أو تغييره أو العبث به في أية مرحلة من مراحل المعالجة أو التبادل سواء في مرحلة التبادل الداخلي مع المعلومات أو عن طريق تدخل غير مشروع

3- إستمرارية توفر الخدمات availality:

التأكد من إستمرارية عمل النظام المعلوماتي واستمرار القدرة على التعامل مع المعلومات وتقديم الخدمة لمواقع المعلومات وأن مستخدم المعلومات لن يتعرض إلى منع استخدامه لها أودخوله إليها

4- عدم إنكار التصرف المرتبط بالمعلومات ممن قام به no repadiahin:

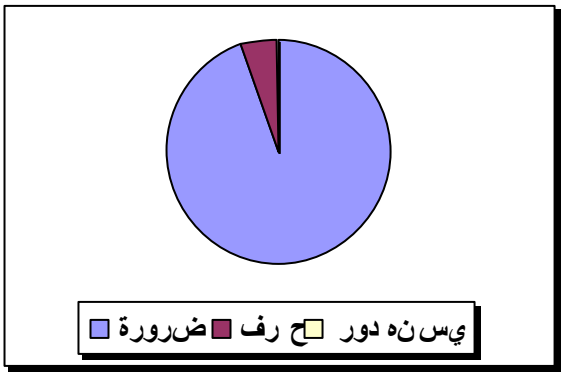
ويقصد به ضمان عدم إنكار الشخص الذي قام بتصرف ما متصل بالمعلومات أو مواقعها أنه الذي قام بهذا التصرف بحيث تتوفر قدرة.

إذن فقد أصبح امن المعلومات في العصر الحالي ضرورة حتمية للأفراد والمؤسسات وحتى الدول وذلك من أجل حماية المعلومات من الضياع والعبث بها؛ وقد أصبح الجميع على علم وقناعة تامة بالأهمية التي يكتسيها أمن المعلومات ووجوب توفير ميكانزمات للحفاظ عليها وقد أجاب أغلبية الطلبة بأهمية أمن المعلومات والنتائج موضحة في الجدول رقم 18 من الصفحة 145

قد أجمع الطلبة كما سبق ذكره على ضرورة توفير الحماية للمعلومات وعدم تركها في متناول العابثين بها وذلك بنسبة (94,8%) والشكل التالي يوضح ذلك :

---

[97] أمن المعلومات.ماهيتها وعناصرها ,المرجع السابق



الشكل رقم:13 أهمية أمن المعلومات

5-1-1-2. تطور مفهوم الأمن المعلوماتي:

إن استخدام مفهوم أمن المعلومات وإن كان استخداما قديما سابقا لوسائل تكنولوجيا المعلومات ، إلا إنه وجَد استخدامه الشائع بل والفعلي في نطاق أنشطة معالجة ونقل المعلومات والبيانات بواسطة وسائل الإتصال؛ وقد بدأت رحلت أمن المعلومات من البداية حيث كانت الحواسيب في سنوات الأربعينيات والخمسينات تشغل من قبل نفس الأفراد الذين أعدوا البرامج وصيانتها ؛ وكان أهم ما يشغلهم هو كيفية تنكيد الأجهزة للأوامر المطلوبة منها و لم يكونوا منشغلين بأمن المعلومات بقدر اهتمامهم بعمل الأجهزة، لذلك كانت الأمنية تدور حول تحديد الوصول أو الإطلاع على البيانات من خلال منع الغرباء الخارجيين من التلاعب بالأجهزة بالإضافة إلى توفير البيئة من تبريد وإدامة للقدرة الكهربائية، لذلك كان ظهور مصطلح أمن الحواسيب خلال الستينات ليعني أمن الحاسوب ذاته ولإجراءات مختلفة لمواقع الحواسيب وقاعاتها , ونتيجة التوسع في الاستخدام والتطبيقات الحواسيب وما تؤديه من فوائد جمة نتيجة التعامل مع كمية كبيرة من البيانات تغير التركيز في الأمنية من السيطرة الكافية للحواسب إلى السيطرة على البيانات وحمايتها , وبهذا شهدت السبعينات الإنتقال إلى أمن البيانات ورافق ذلك استخدام كلمات سر بسيطة للسيطرة على الوصول إلى البيانات بالإضافة إلى إجراءات إضافية لحماية حواسيب من الكوارث.

أما مرحلة الثمانينات والتسعينات وحتى المرحلة الحالية فهي مرحلة أمن المعلومات حيث أن التركيز على المعالجة المتكاملة والاعتماد على المعلومات الدقيقة أدى إلى إنتقال أمنية البيانات إلى أمنية المعلومات ، وعليه وجب المحافظة على المعلومات وتكاملها وتوافرها ودرجة توثيقها [98].

5-1-1-3. عناصر أمن المعلومات.

إن أمن المعلومات يشمل عناصر عديدة نوجزها في مايلي:

1- أمن الحواسيب:

---

1 - البياتي , **هلال عبود الوسائل الفنية لحماية البرامج ودور التشريع في حمايةالمعلومات** . مجلة أبحاث الحاسب.مج 1 ,1996.ص.38.

إن أجهزة الحواسيب تتطور بشكل سريع مما يجعل تطور الأجهزة والمعدات التي يمكن أن تستخدم في عملية السرقة والتخريب تفوق إمكانيات المستخدم وهذا يتطلب تطوير القابليات الذاتية ومتابعة التطورات التي تحصل في تقنية الحواسيب والاتصالات لكي يتمكن الإطار المسؤول عن الأجهزة من القيام بأعمال الصيانة لأعطال الطارئة والتأكد من عدم تعرض الأجهزة للعبث والتلاعب بها.[99]

2- أمن البيانات:

تعرف أمنية البيانات على أنها العلم الذي يهتم بدراسة طرق حماية البيانات المخزنة ضمن أجهزة الحواسيب وأنظمة الاتصالات ويتناول سبل التصدي للمحاولات الرامية إلى الإطلاع على هذه البيانات بطرق غير مشروعة؛ أو إلى نقل أو تغيير أو تخريب برمجيات حماية البيانات[100].

3- أمن الأفراد:

لعل الأفراد من أثمن ما تملكه المؤسسات ، كما يمكن أن يكونوا في الوقت نفسه من بين الإخطار التي تهدد أمن البرامج ؛ حيث أنه من متطلبات أمن المعلومات تحديد مواصفات محددة ووضع تعليمات واضحة لاختيارهم وذلك لتقليل من المخاطر التي يم كن أن يكون مصدرها الأفراد بالإضافة إلى وضع خطط لزيادة الحس الأمني والحصانة من التخريب[101].

4- أمن البرمجيات:

إستحدثت نظم جديدة لتطوير حماية البرمجيات أمنيا من السرقات والنسخ غير القانوني , وذلك باعتبار أن البرمجيات هي جزء من الحواسيب وسيكون الأمن ناقصا إذا ما أهملت أنظمة التشغيل وبقية البرامج , وقد سنت العديد من الدول قوانين خاصة لحقوق النشر لمنع أي عمل غير قانوني كما استخدمت أقفال خاصة لحمايتها[102]؛ ومن الأساليب المستحدثة للحفاظ على سرية وأمنية المعلومات أسلوب التشفير والذي اثبت كفاءة وقدرة عالية في حماية المعلومات.

5- أمن الأمن الاتصالات:

إن تطور الحواسيب أقترن بتطور هائل وكبير للاتصالات وقد وفر هذا التطور إمكانيات التراسل بين الحواسيب وبين الحواسيب وملفاتها والمستفيد عبر خطوط الهاتف وعبر الهواء مهما كانت المسافات، ومن هنا ظهرت إمكانية سرقة المعلومات عن طريق التدخل عبر منظومات الإتصال المختلفة , لذلك وجب توفير عناية كبيرة لأمن الاتصالات وإجراء الفحوصات الدورية لهذه المنظومات.

---

[99]- البياتي ,هلال عبود.المرجع السابق.ص.42.

[100]- النعيمي ,محمد عبد العال. **أتمتة المكاتب**.الأردن:دار المناهج ,1999.ص.49.

[101]- داود ,حسن الطاهر. **الحاسب وامن المعلومات**.الرياض: معهد الإدارة العامة,2000.ص..49.

[102]- النعيمي ,محمد عبد العال.المرجع السابق.ص.236.

6- أمن المواقع (المباني):

لضرورة إكتمال الإجراءات الأمنية لابد أن يتم إعطاء أهمية للمواقع والمباني التي تحتوي على منظومات الحواسيب، ووفقا لطبيعتها يتم إتحاد إجراءات احترازية لحماية الموقع وتحصينه من أي تخريب أو سطو.[103]

5-1-2. أنواع أمن المعلومات:

يمكننا أن نحقق أمن المعلومات بعدة طرق وعلى عدة مستويات نتطرق إليها في هذا العنصر.

5-1-2-1. العمليات الأساسية لأمن المعلومات.

تعددت عمليات التعامل مع المعلومات في بيئة النظم وتقنيات المعالجة والاتصال وتبادل البيانات ولكن يمكن بوجه عام تحديد العمليات الرئيسية التالية[104]:

1- تصنيف المعلومات: وهي عملية أساسية لذي بناء أي نظام أو في بيئة أي نشاط يتعلق بالمعلومات وتختلف التصنيفات حسب المنشأ فمثلا قد تصنف المعلومات إلى معلومات متاحة وموثقة وسرية للغاية

2- التوثيق: ويتطلب عمليات المعلومات أساسا إتباع نظام توثيق خطي لتوثيق بناء النظام وكافة وسائل المعالجة والتبادل ومكوناتها ويتطلب التوثيق أن تكون إستراتيجية أو سياسة الأمن موثقة ومكتوبة

3- المهام والواجبات الإدارية والشخصية : إن مهام المتصلين بنظام المعلومات تبدأ في الأساس من حسن اختيار الأفراد المؤهلين وعمق معارفهم النظرية والعملية وهذا التأهيل يتطلب تدريبا مستمرا

3- سجل الأداء: تحتوي مختلف أنواع الحواسيب نوعا من السجلات التي تكشف استخدامات الجهاز وبرمجاتهم والنفاذ إليه وهي ما تعرف بسجلات الآداء أو سجلات الإنقاذ

4- عمليات الحفظ: و عمليات الحفظ تتعلق بعمل نسخة إضافية من المواد المخزنة على أحد وسائط التخزين سواء داخل النظام أو خارجه وتخضع عمليات الحفظ لقواعد يتعين أن تكون محددة سلفا ومكتوبة ويجري الالتزام بهذا لضمان توحيد معايير الحفظ وحماية النسخ الاحتياطية

5- وسائل التعريف والتوثق من المستخدمين وحدود صلاحية الاستخدام:

---

[103]- البياتي ,هلال عبود.المرجع السابق.ص.43.

1 - **أمن المعلومات: ماهيتها** , عناصرها وإستراتيجياتها. على الخط المباشر زيارة يوم: 2005/12/25. متوفر على الموقع: http://www.arablaw.org.computer

إن الدخول إلى أنظمة الكمبيوتر وقواعد البيانات ومواقع معلوماتية عموما يمكن تقييده بالعديد من وسائل التعرف على شخصية المستخدم وتحديد نطاق الاستخدام وهو ما يعرف بأنظمة التعريف والتخويل.

5-1-2-2. أنماط ومستويات أمن المعلومات:

لأمن المعلومات عدة مستويات أهمها:

1- الحماية المادية:

وتشمل كافة الوسائل التي تمنع الوصول الى نظم المعلومات وقواعدها كالاقفال والحواجز والغرف المحصنة وغيرها من وسائل الحماية المادية التي تمنع الوصول الى الاجهزة الحساسة.

2- الحماية الشخصية:

وهي تتعلق بالموظفين العاملين على النظام التقني المعني من حيث توفير وسائل التعريف الخاصة بكل منهم وتحقيق التدريب والتأهيل للمتعاملين بوسائل الأمن الى جانب الوعي بمسائل الأمن ومخاطر الاعتداء على المعلومات.

3 - الحماية الإدارية:

ويراد بها سيطرة جهة الإدارة على إدارة النظم المعلومات وقواعدها مثل التحكم بالبرمجيات الخارجية أو الأجنبية عن المنشأة، ومسائل التحقيق باخلالات الأمن، ومسائل الإشراف والمتابعة لأنشطة الرقابة إضافة إلى القيام بأنشطة الرقابة ضمن المستويات العليا ومن ضمنها مسائل التحكم بالاشتراكات الخارجية.

4 - الحماية الإعلامية(المعرفية) :

كالسيطرة على إعادة إنتاج المعلومات وعلى عملية إتلاف مصادر المعلومات الحساسة عند اتخاذ القرار بعدم استخدامها[105].

ويمكننا ان نلاحظ عدة أنواع للأمن داخل شبكة داخلية [106]:

- أمن الدخول: وهو النوع الأول من الأمن ويهتم بحماية مدخل النظم.

- أمن نظام الملف: ويتمثل هذا الامن في التحكم في الوصول إلى ملفات النظام.

- أمن الحاسب الخادم: يتحكم في حماية الحاسوب الموزع

1- أمن المعلومات: ماهيتها , عناصرها وإستراتيجياتها. المرجع السابق

[106]- سيد حسين ,**فاروق الأنترنت وأحدث ما كتب عنها**.بيروت:دار الراتب الجامعية,1999.ص.98.

5-1-2-3.أمن حفظ ونقل البيانات:

1- أمن حفظ البيانات و المعلومات [107]:

ويهتم هذا المجال بالعديد من الآليات العلمية والعملية حول :

1- مكان حفظ البيانات والبيئة المحيطة بها:

من خلال وجود ها في مواقع آمنة والتي يجب أن تخضع لرقابة دقيقة من حيث الوصول الفيزيائي لهذه المواقع بحيث لا يصل إليه إلا من هو مصرح له من خلال البوابة الآمنة والتي تعتمد أحياناً على التقنيات المتقدمة مثل قراءة بصمة اليد **(Printfinger)**أ وقزحية العين **(Printeye)** أو تردد الصوت أو من خلال الأرقام المتسلسلة أو البطاقات الممغنطة ، وغيرها.

2- طريقة حفظ البيانات:

وذلك من خلال التقنيات المتقدمة في أنظمة تشفير المعلومات المحفوظة **(Encryptions)** بمختلف أنواع التشفير المتماثل أو غير المتماثل سواء المعتمد دولياً أو التشفير المبتكر محلياً.

3- المواد التي تحفظ عليها البيانات:

من خلال الحفظ على الأنسب من الأقراص الصلبة **(HDD)** الذاكرة **(CASH)** أو الأقراص المدمجة **(CD)**وغيرها من بيئات الحفظ المناسبة.

4- حماية المعلومة: ويتم بعدة آليات من خلال:

أ- استخدام برامج الحماية الجدران النارية **(Firewalls)** للحماية من الاختراق للأجهزة المرتبطة فيزيائياً بشبكات ، واستخدام المرشحات **(filters)** لضمان عدم نقل المعلومات غير المسموح بها ، واستخدام برامج مكافحة الفيروسات **(Anti-Virus)** للحماية من الفيروسات المختلفة.

ب. النسخ الاحتياطي **(BACK UP)** وهذا يعالج مشكلة فقد البيانات الرقمية غير المكتوبة **Hard (Copy)**والتي تكون أكثر عرضة من غيرها للتلف أو العطب أو الفقد ويتم ذلك بعدد من الآليات:

2- : أمن نقل المعلومات والبيانات [108]:

قديماً كانت تستخدم آليات النقل الفيزيائي المباشر للبيانات وتحاط بسرية وحماية وتتم ببطء نسبي، والمتأمل حالياً يرى أن تلك الطريقة كانت أكثر أمناً من الطرق الحديثة من حيث التواصل الإلكتروني وبعد التقدم التقني أصبحت آليات النقل الحديثة بما تميزت به من سرعة في نقل المعلومة ودقة هي الأنسب عند أخذ الاحتياطات اللازمة في عمليات نقل البيانات ولذا نرى بأن هذا المجال يهتم بالبيئات الآمنة لنقل البيانات

:1- أبو عبادة ,أيمن بن عبد الغزيز.على الخط المباشر. زيارة يوم:2006/04/14.متوفر على الموقع http://informatics.gov. sa magazine

[108]-. أبو عبادة ,أيمن بن عبد الغزيز.المرجع السابق

والمعلومات من خلال :

1- أمن نظم الاتصالات وبيئات النقل المستخدمة:

عندما يكون الاتصال مباشر **(direct connection)** بواسطة خطوط الهاتف **(Dialup)** أو بالاتصال المباشر بالأقمار الصناعية **(Satellite)** ، وذلك عندما يكون حجم البيانات متوسطاً نسبياً وتكمن الخطورة هنا عند وجود متلصصين يقومون بعمليات التلصص **(Sniffing)** على خطوط الاتصال وتبرز هنا أهمية تشفير البيانات بقوة تشفير عالية والمحافظة على سلامة خط الاتصال من وجود المعترضين أو المتجسسين .

2- التطبيقات المستخدمة والبروتوكولات المناسبة:

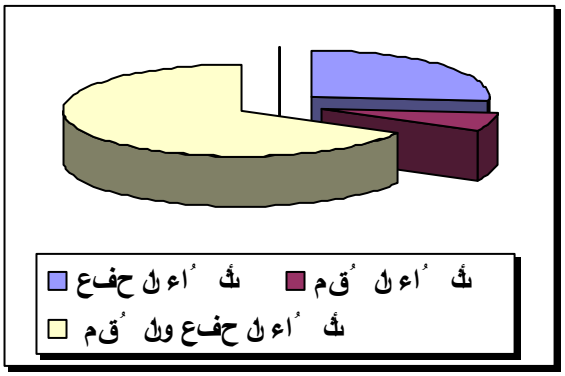
عندما يكون الاتصال غير مباشر وفي وسيط مثل الإنترنت أو يكون نقل البيانات لموقع خدماتي عالي الأهمية الأمنية مثل البنوك أو للشراء المباشر ببطاقات الائتمان الإلكترونية وهنا مكمن الخطر حيث يكون التجسس والإختراق من أبرز المشاكل الأمنية والتي لا يمكن القضاء عليها بشكل كامل بل يمكن الحد منها بشكل كبير عن طريق استخدام البروتوكولات الآمنة **SSL (Secure Sockets Layer)** أو ما يسمى بـــ**(HTTPS)** ، وتظهر أهمية التوقيعات الرقمية **(PKI)** والشهادات الإلكترونية للمواقع الآمنة وغيرها من وسائل الحماية .

3- البحث عن مصادر الخطر المتوقعة على المعلومة لمكافحتها:

تعتبر مصادر الخطر على أمن البيانات كثيرة جداً و لعل من أهمها خطورة الوصول إلى البيانات من قبل أشخاص غير مسموح لهم بالوصول إليها وبالتالي يتم تسريب المعلومات أو إتلافها أو تغييرها.

إن المعلومات مورد إستراتيجي وحيوي ،وقد غدت العصب المحرك لكل مناحي الحياة ولهذا وجبت حمايتها والحفاظ عليها ،وحماية المعلومات يجب أن يتوفر في كل حلقات مسيرها مند إنتاجها وإلى غاية توزيعها ونشرها والجدول رقم: 19 في الصفحة 145 يوضح وقت حفظ المعلومات

إن المعلومات التي لا تنشر تولد وتموت مع أصحابها وبالتالي فنشر المعلومات يعتبر حياة لها؛ ولكن المعلومات أثناء نقلها وتبادلها تتعرض لأخطار كثيرة فقد يقوم العابثين بتغييرها أو حذفها أو تدميرها تماما، ولهذا فقد أعرب أغلب الطلبة بنسبة (78,9 %) بضرورة حماية المعلومات في كل أطوارها أي أثناء حفظها ونقلها معًا ،وتتم الحماية أثناء الحفظ في الحماية الفيزيائي ة من الأخطار الطبيعية كالحرائق والغبار أو من الأخطار البشرية كالسرقة والتعديل والتدمير؛ أما حماية المعلومات أثناء فتتم باستعمال ميكانزمات وطرق متعارف عليها مثل التوقيع الإلكتروني والجدران النارية والتشفير ...والرسم البياني التالي يوضح نتائج الجدول بشكل أفضل:



الشكل رقم:14 أوقات حفظ المعلومات

5-1-3. طرق حماية المعلومات:

هناك العديد من الطرق التي يمكن بواسطتها ضمان حماية المعلومات أهمها:

5-1-3-1. التوقيع الإلكتروني.

يمر العالم في الوقت الراهن بمرحلة انتقالية بين التعامل الورقي والتعامل الإلكتروني ، وقد ظهر هذا التحول جليا في مجالات التبادل التجاري والعلاقات الاقتصادية في الدول الكبرى؛ وفي ظل هذه التطورات الشديدة السرعة كان من الطبيعي أن يصاحبها وسائل جديدة أو مبتكرة غير مادية تتناسب مع طبيعة المعاملات التي تجري عبر وسائط إلكترونية؛ وقد ظهر التوقيع الإلكتروني كبديل للتوقيع الكتابي , فماذا نعني بالتوقيع الإلكتروني ؟, وما هي أنواعه ؟, وما مدى إعتراف الجهات القانونية به ؟

1- تعريف التوقيع الإلكتروني:

إن كافة التعريفات الفقهية تتجه نحو تعريف التوقيع الكتابي بأنه علامة خطية تميز الشخص الموقِع سواء كان بإمضاء أو بالختم أو ببصمة الأصبع وتكون على محررات ورقية أي دعامات مادية ؛ وذكر قاموس روبير **Robert** الفرنسي التوقيع على أنه: علامة شخصية أو خطية يضعها الموقِع ليأكد مضمون الورقة وصدق ما كتب بها مع إقراره بتحمل المسؤولية والتزامه بما جاء فيها [109].

أما التوقيع الإلكتروني وباعتباره الوسيلة الضرورية التي لا غنى عنها في مجال المعاملات التجارية الإلكترونية فقد عرفته المادة الأولى من مشروع القانون المصري بشأن التجارة الإلكترونية بأنه يمثل حروف أو أرقام أو رموز أو إشارات لها طابع منفرد يسمح بتحديد الشخص صاحب التوقيع وتميزه عن غيره , وبالتالي فإنه يمكن القول بأنه إجراء معين يقوم به شخص المراد توقيعه على المحرَر سواء كان هذا الإجراء على شكل رقم أو إشارة إلكترونية معينة أو شيفرة خاصة , المهم في الأمر أن يحتفظ بالرقم أو الشفرة بشكل آمن وسري تمنع استعماله من قبل الغير , وتعطي الثقة في أن هذا التوقيع يفيد أنه بالفعل صدر عن صاحبه أي حامل الرقم

1- أبو هبة, نجوى **التوقيع الإلكتروني = La signature électronique: تعريفه ,مدى حجيته في الإثبات**.القاهرة:دار النهضة العربية ,2002.ص.40.

كما يعرفه البعض بأنه مجموعة من الإجراءات الشخصية تمكن من تحديد شخصية من تصدر عنه هذه الإجراءات وقبوله بمضمونة التصرف الذي يصدر التوقيع يشأنه[110].

2- صور التوقيع الإلكتروني:

يتحد التوقيع الإلكتروني عدت صور فقد يأتي في صورة رقم سري أو مجموعة أحرف وقد يأخذ شكل التوقيع البيومتري وقد يأخذ أشكال أخرى سنتطرق إليها في مايلي:

1 التوقيع الخطي بالماسح الضوئي [111]:

أنشئ الماسح الضوئي خصيصا لنقل الصورة الفوتوغرافية والوثائق الأصلية كما هي الدعامات الإلكترونية الموجودة على جهاز الكمبيوتر , وتحقيقا لنفس هذا الهدف العلمي أمكن نقل التوقيع الخطي كما هو على الوثيقة الموجودة على الجهاز لكي يتم توقيعها للإقرار بمضمونها وإذا كان الأمر يبدو سهلا من الناحية النظرية إلا أن مثل هذا التوقيع لا يحقق الإمان الكافي من الناحية العملية فلا يوجد أدنى شك من إمكانية وضع هذا التوقيع على أية وثيقة عند المتقاعد بسوء نية بحفظ نسخة من التوقيع المصور بالماسح الضوئي وهذا يعني وجود عملية تزوير , ولذلك فقد استقر الوضع على عدم الاعتماد على مثل هذا التوقيع.

2- التوقيع بإستخدام بطاقات الائتمان الممغنطة ذات التوقيع السري[112]:

تسهيلا لإبرام الصفقات التجارية بشكل عام , والحصول على نقود في أي وقت على وجه الخصوص ,درجت البنوك على منح عملائها بطاقات الإئتمان الممغنطة لها التوقيع السري لا يعلمه من العملاء إلا صاحب البطاقة فقط وتستخدم هذه البطاقات إما لسحب مبالغ مالية في الحدود المتفق عليها بين العميل والبنك أو في دفع قيمة المشتريات التي يقوم العميل بشرائها وقد اعترض البعض حول إبرام الصفقات الإلكترونية عن طريق الدفع الإلكتروني ببطاقات الإئتمان حيث أن هذا الشكل ينفصل ماديا عن صاحبه الأمر الذي يترتب عليه إمكانية حصول أي شخص على البطاقة ولكن الاعتراف بهذه الطريقة رد على المعترضين.

3-التوقيع الكودي[113]:

هو ما يغرف بالكود السري وهو عبارة عن مجموعة أرقام أو حروف يختارها صاحب التوقيع ويتم تركبها أو ترتيبها بشكل كود معين يتم عن طريقه تحديد شخصية صاحبه , بحيث لا يكون هذا الكود معروفا إلا له ؛ وغالبا ما يستخدم التوقيع الكودي في المراسلات والمعاملات البنكية كالصرف الآلي والدفع الإلكتروني.

---

[110]- أبو هبة, نجوى التوقيع الإلكتروني. المرجع السابق.ص.41.

1 - قنديل , سعيد السيد. **التوقيع الإلكتروني: ماهيته ,صوره, حجيته في الإثبات بين التدويل والإقتباس.** الإسكندرية: دار الجامعة الجديدة ,2004.ص. 66.

[112] - - قنديل , سعيد السيد.المرجع السابق.ص.67.

[113]- أبو هبة, نجوى التوقيع الإلكتروني. المرجع السابق.ص.48.

4- التوقيع بالقلم الإلكتروني:

هذه صورة أخرى للتوقيع الإلكتروني ويتم ذلك عن طريق استخدام قلم إلكتروني حسابي يكمن عن طريقه الكتابة على شاشة الكمبيوتر وذلك بإستخدام برنامج معين , يقوم هذا البرنامج بوظيفتين الأولى خدمة التقاط التوقيع والثانية خدمة التحقق من التوقيع.

5- التوقيع البيومتري [114]:

يقوم هذا النظام بالاعتماد على الصفات والخواص الفيزيائية والطبيعية والسلوكية للإنسان والتي من المفروض والطبيعي أن تختلف من شخص لآخر, ومن هذه الخواص بصمة الأصبع ومسح العين أو ما يعرف ببصمات القزحية وخواص اليد وبصمات أو نبرة الصوت....

ويتم تخزين هذه الخواص في الحاسب وذلك بطريقة التشفير, ويعاد حل هذا التشفير للتأكد من صحة التوقيع.

3- وظائف التوقيع الإلكتروني:

يتحدد دور التوقيع الإلكتروني عامة في ثلاثة وظائف أساسية هي[115]:

- تمييز هوية صاحب التوقيع: وذلك بأن يدل التوقيغ الموجود على المحَرر أنة ينسب لشخص معين بالذات , فيجعل الورقة الموفعة منسوبة إليه وهذه الوظيفة يقوم بها التوقيع الكتابي في شكل علامة خطية وشخصية وإذا تفحصنا التوقيع الإلكتروني وجدناه يقوم بنفس الشيء وذك في شكل رموز أو أرقام أو حروف.

- التغبير عن إرادة صاحب التوقيع: تتعلق هذه الوظيفة بمسألة التأكد من رضى صاحب التوقيع وقبةل الإلتزام بمضمون التصرف القانوني وإقراره.

- التوقيع يدل على حضور صاحب التوقيع: هذه الوظيفة تتفق تماما مع طبيعة التوقيع اليدوي إذ يستلزم لصحته ضرورة وجود شخص الموقع او من ينوب عنه قانونيا , فأدا وجد التوقيع على الورقة وثبتت صحته ونسب لموقعه كان ذلك دليلا على حضور صاحب التوقيع شخصيا ؛ أما في حالة التوقيع الإلكتروني فإن قيام العميل بإدخال الرقم السري بنفسه يعد في حد ذاته توقيعا ودليلا على أنه صدر عنه شخصيا , وأنه كان فعلا متواجدا حين صدر منه التوقيع في صورة أرقام سرية لا يعلمها سواه.

حجية التوقيع الإلكتروني[116]:

---

[114]- أبو هبة, نجوى التوقيع الإلكتروني. المرجع السابق.ص.49.

[115]- أبو هبة, نجوى التوقيع الإلكتروني. المرجع نفسه.ص.82.

[116]- حجازي , عبد الفتاح البيومي. **التوقيع الإلكتروني في النظم القانونية المقارنة**.الإسكندرية: دار الفكر الجامعي.ص.ص.36.

لقد نص القانون الفرنسي على أن التوقيع الإلكتروني إنما يمثل شخصية صاحبه ويضمن علاقته بالواقعة التي أجراها ويأكد شخصية صاحبه وصحة الواقعة المنسوبة إليه إلى إن يثبت عكس ذلك؛ ووفقا لمشروع قانون التجارة الإلكترونية المصري والذي صدر بديلا عنه قانون التوقيع الإلكتروني ,فإن التوقيع الإلكتروني له ذات حجية التوقيع التقليدي ؛ ووقفا لنص الفقرة الإ ولى من فانون التجارة الإلكترونية التونسي فقد ساوى القانون بين حجية التوقيع التقليدي و التوقيع الإلكتروني ؛ كذلك فإن القانون الأمريكي الصادرسنة 2000 في شان التوقيع الإلكتروني يساوي في الحجية بين التوقيعين.

وبذلك يكمن القول أن التوقيع الإلكتروني يمكن في ظل ضمانات معينة أن يقوم بذات الدور الذي يؤديه التوقيع التقليدي بأن البعض يرى أن التوقيع التقليدي قد لا يجد اي مكانا في ظل المعالجة الإلكترونية للمعلومات وبذلك يمكن الإعتماد على الرقم السري كوسيلة بديلة أو إضافية للتوقيع التقليدي.

ونخلص مما سبق إن التوقيع الإلكتروني له ذات الوظيفة للتوقيع التقليدي شرط أن تكون القواعد العامة للإثبات قادرة على إستعاب أحكام التوقيع الإلكتروني.

5-1-3-2. تشفيرالبيانات:

بعد التشفير من أهم وسائل الحماية المتعارفة فما هو ؟

1- تعريف التشفير:

يعرف التشفير بأنه عملية تشكيل البيانات باستخدام خوارزمية معينة تسمى المفتاح , وتصبح بها غير قابلة للقراءة إلا بعد استخدام الخوارزميّ لفكها ؛ ويتم عادة تشفير البيانات فبل إرسالها عبر الشبكة وذلك لضمان سلامة وصولها دون التعرض لأية عمليات تجسس أو تخريب لمضمونها , على أن يكون تفكيك الشفرة لدى مستقبل الرسالة باستخدام مفتاح فك الشفرة [117].

والتشفير باختصار يعني تغيير مضمون الرسالة باستخدام برنامج معين يسمى مفتاح التشفير وذلك قبل إرسال الرسالة على أن يكون لمستقبلها القدرة على استعادة محتوى الرسالة في صورتها الأصلية.

وقد ظهرت المعاملات المالية على الأنترنت الحجة لتوفير حماية للمعلومات الإلكترونية والبيانات الاسمية , لذلك يعد التشفير من وسائل حفظ وسرية المعلومات في نطاق الأنظمة الإلكترونية.

2- تطور التشفير:

---

[117]- – حجازي.عبد الفتاح البيومي. الحكومة الإلكترونية.المرجع السابق.ص. 141.

مر التشفير بعدة تطورات إلى أن وصل إلى ما هو عليه الآن[118]:

- 50- 58 سنة قبل الميلاد: يستخدم الإمبراطور يوليوس قيصر **Jules césar** الرموز المشفرة في رسالته على حاكمه سيسرون **ciceron** في حروبه ضد بلاد الغال وكان يستخدم في ذلك طريقة إستبدال الحروف الأصلية بالحروف التي تليها مباشرة أو تنفيذ عمليات تجعل النص المكتوب غير مفهوم.
- 1499: نشر الراهب الألماني جون تريمام **Jean Tritheme** أول كتاب خاص بالتشفير يعرض فيه كيفية التشفير.
- 1914- 1918: تطور علم التشفير خلال الحرب العالمية الأولى بشكل كبير وهذا باستخدام تقنيات جديدة تهدف على سرعة الاتصالات العسكرية.
- 1977: تصميم نظام التشفير **RSA** .
- 1997: استخدام مفتاح تشفير بطول 40 بت ثم فك تشفيره من طرف طالب جامعي في عدد من الدقائق.
- 1999: استخدام مفتاح تشفير بطول 512 بت والذي تم فك شفرته من طرف مجموعة من الباحثين بعدة أربعة أشهر.

---

[118]- عبد الحق, ط.**مدخل إلى المعوماتية: برمجيات الحاسب الشخصي. = Logiciel de PC** .البليدة: فصر الكتاب ,2005.ص.327.

- 2001الإستخدام الواسع لنظام التشفير **open pgp** من طرف الكثير من العاملين على شبكة الأنترنت بقصد تأمين سرية المعلومات.

3- أنواع التشفير:

التشفير نوعان[119]:

1 -**التشفير المتماثل:** يستخدم فيه المفتاح نفسه للتشفير وكذا لفك الشفرة, وبذلك فإن المفتاح يكون معروفا من طرف كل من مرسل الرسالة ومستقبلها ولا يرسل المفتاح مع الرسالة ولكن يرسل بطرق أخرى حرصا على حماية سرية المفتاح وعدم إطلاع الغير عليه؛ وقد استعملت كتب للأكود **sécure code book** وتتضمن قائمة بمفاتيح التسفير التي يجب أن تستخدم بطرق محددة ؛فعلى سبيل المثال فإن الرسالة التي ترسل يوم الأربعاء يتم استخدام المفتاح **A** يفك شفرتها ,وتفقد كتب الأكواد فيمتها إذا ما تمت سرقتها لأن ذلك يعني كشف المفتاح من قبل الغير.

2 -التشفير غير المتماثل: ويستخدم فيه مفتاحان لكل مستخدم , أحدهما +مفتاح عام معروف من قبل الآخرين حيث يسجله الشخص عادة مع توقيعه على البريد الإلكتروني , في حالة الرغبة في إرسال رسالة مشفرة إلى ذلك الشخص يتم استخدام ذلك المفتاح العام لكتابة الرسالة أما لفكها فيستخدم مفتاح خاص لا يعرفه إلا المستقبل نفسه ؛وغلى الرغم من ارتباط كل نمن المفتاح العام والخاص ببعضهما إلا أن أي منهما لا يدل على الآخر.

وهناك طرق متعددة للتشفير تتراوح في درجة تعقيدها فقد تكون سهلة للغاية لا تتعدى فكرة الاستبدال كما هو الحال في شيفرة قيصر التي تمثل في أبسط صورها إستبدال كل حرف في الأبجدية بحرف آخر وفقا لمفتاح الشيفرة المحدد ,وقد تم تطوير فكرة الاستبدال حتى تصبح أكثر تعقيدا وبالتالي يصبح كسرها أمرا في غاية الصعوبة.

4- أهمية التشفير:

إن أهم الأخطار التي يمكن أن نتغلب عليها بواسطة التشقير هي[120]:

- الإطلاع على المعلومات المحضورة.
- محاولات تعديل البيانات إلى وجهة إخرى
- تأخير محتويات الرسائل المتبادلة.
- تغيير كلمات السر الخاصة بالمستفدين.

---

[119]- بومفلاح, فاتن.المرجع السابق.ص.561.

[120]- داود ,حسن الطاهر.الحاسب وأمن المعلومات.المرجع السابق.ص.178.

- إنتحال شخصية المستخدم الحقيقي.

- تعديل البيانات المخزنة على الحاسب.

5-1-3-3. الجدران النارية:

1- تعريف الجدران النارية:

يخطر في بال معظم الناس عند الحديث عن أمن شبكة الأنترنت برامج جدران النار وعلي الرغم من أن برامج جدران النار لا تعتبر علاجا لجميع مشاكل أمن المعلومات علي شبكة الانترنت، إلا إنها ضرورية لأي إستراتيجية متعبة، في مجال أمن انترنت، تعتبر برمجيات جدران النار ببساطة حاجزا بين شبكتين وهما في اغلب الأحيان شبكة داخلية وتسمي الشبكة الموثقة **trusted network** شبكة خارجية تسمي **entrusted network**وهي شبكة انترنت في هذه الحالة وتقوم برمجيات جدران النار بفحص رزم البيانات القادمة والخارجة اعتمادا علي مجموعة قواعد التي يضعها المشرف علي الشبكة، للسماح لهذه الرزم بالمرور أو يقوم بحجبها ومنعها من الوصول إلي الشبكة الداخلية.

في الأيام الغابرة كانت تقام أسوار حجرية تفصل بين الأبنية والبيوت الخشبية , فتمع في حالة إندلاع حريق امتداد اللهب من بيت لآخر وكانت تسمى بجدران النار , وفي الشبكات الحديثة مثل الأنترنت يمكن اعتماد الطريقة نفسها لحماية مصادر الشبكات الداخلية من الأخطار الناتجة عن ضياع المعلومات الحيوية[121].

ويمكن تعريف الجدار على أنه برنامج **software** أو عتاد **hardware** لحماية موارد الشبكة الداخلية من مستخدمي الشبكات الأخرى , وتستخدم في حالة ارتباط الشبكة بشبكات واسعة وتعمل على منع المستخدمين الخارجيين من الوصول إلى مولد الشبكة وبياناتها الخاصة [122].

إذن فالجدران النارية عبارة عن نظام أو مجموعة أنظمة تفيد تعزيز ضبط الوصول إلى المعلومات بين شبكتين أما الوسائل المعتمدة فمختلفة إنما من حيث المبدأ يمكن تعريفه بأنه عبارة عن آليتين , واحدة تعيق الحركة والأخرى تسمح بها [123].

2- أنواع الجدران النارية:

تستخدم معظم برمجيات جدران النار اليوم طريقة واحدة أو أكثر من الطرق الثلاث المتبعة في فحص الرزم وتستخدم العديد من الموجهات تقنية جدران النار المسماة بترشيح الرزم **packet filtering** والتي

---

[121]- المسفر ,**يوسف.الشبكات المعلوماتية والجدران النارية**.من مجلة علوم وتكنولوجيا.ع53. اتلسنة الخامسة 1996.ص.48.

[122]- بومفلاج , فاتن.**حماية المعلومات في شبكة ام القرى**.مقتطف من كتلب الوقائع.مج 2.الشلرقة ,2001.ص.562.

[123]- المسفر ,يوسف. المرجع السابق.ص.48.

تفحص عناوين وبوابات المصدر **Source** والوجهة النهائية **destination** لرزم **TCP** ورزم **UDP** القادمة ثم ترفض أو تسمح للرزم بالمرور وفقا لمجموعة من القواعد مسبقة التحضير وتعتبر تقنية ترشيح الرزم طريقة رخيصة نسبيا وشفافة بالنسبة للمستخدم ولها تأثير طفيف غير ذي بال علي أداء الشبكة ولكن تجهيز تقنية ترشيح الرزم يعتبر عملية معقدة نسبيا ويتطلب معرفة دقيقة بالشبكة وبرتوكولات النقل بل يتطلب في بعض الأحيان معرفة ببروتوكولات التطبيق.

تكمن المشكلة الأخرى في تقنية مرشحات الرزم في أنها عرضة لما يسمي خداع بروتوكول انترنت **IP Spoofing**وهي طريقة يستخدمها الهاكرز ليتمكنوا من الوصول إلى شبكة شركة عن طريق تغيير عناوين بروتوكولات انترنت في ترويسة الرزم إلى عناوين أخرى مقبولة من قبل شركة أخرى

أما النوع الأكثر تقدما وأمنا من أنواع جدران النار فهي برامج بوابات التطبيقات **application gateways**، تستخدم معظم منتجات جدران النار العاملة بتقنيات بوابات التطبيقات بما فيها برامج **eagle**الشهيرة من شركة **Raptor** ما يسمي توكيلات التطبيقات **application proxies** وهي عبارة عن برامج مكتوبة لخدمات معينة من خدمات انترنت (مثل خدمات **HTTP** ، **FTP**وخدمة **telnet**وتعمل علي مزود مرتبط بشبكتين كمزود **Server** لزبون تطبيقات **application client** وكزبون لمزود التطبيقات **application server**

ونظرا لان برامج توكيلات التطبيق تقوم بتقييم رزم الشبكة لتحديد شرعية البيانات المتعلقة بتطبيق معين فإنها تعتبر شكل عام أكثر أمنا من مرشحات الرزم. وتمتاز معظم جدران النار لبوابات التطبيقات باحتوائها علي ميزة تدعي "ترجمة العناوين الشبكة **Network Address Translator** "والتي تمنع ظهور عناوين **IP**الداخلية .أمام المستخدمين من خارج الشبكة الموثقة. تكمن إحدي السلبيات الرئيسية في تقنية بوابات التطبيقات في انخفاض مستوي الأداء بسبب المعالجة المضاعفة التي تتطلبها وظيفة التوكيل **proxy function**وهناك سلبية أخري تكمن في انه قد يتوجب عليك أن تنتظر عدة أشهر حتى تزودك الشركة الصانعة لبرنامج جدران النار بتوكيل التطبيق **application proxy** لأي خدمة جديدة من خدمات انترنت مثل استخدام خدمات **RealAudio.** وإذا كنت تنوي استخدام جدران النار دفاع محيطي خارجي فقط وراء توصيلات **T1** الي مزود خدمة انترنت فلا داعي للقلق علي الأداء، لان عرض الحزمة المنخفض لهذه التوصيلات سيصل إلي حد الإشباع قبل وصول جدران النار الي ذلك الحد. قد تجد الكثير من المؤسسات ضرورة في استخدام جدران النار إضافية علي مستوي شبكاتها الداخلية لفرض حزام امني علي مزودات أقسامها المختلفة مثل مزود المورد البشرية الذي يحتوي عادة علي معلومات حساسة، ويصبح الأداء في هذه الحالة عاملا مهما نظرا لان الربط سيعتمد علي شبكة ايثرنت بسرعة 10 ميجابت/ثانية أو شبكة ايثرنت السريع 100 ميجابت/ثانية .وإذا كنت تنوي استخدام توكيلات التطبيقات داخليا فعليك أن تعتمد علي حل مبني علي عتاد سريع مثل **pix firewall** من شركة **Cisco** أو **firebox** من شركة **Seattle software** أو قد تلجا الي تركيب برمجيات جدران النار علي نظام يتضمن عدة معالجات .

أما النوع الثالث من تكنولوجيا جدران النار والذي أسمته شركة **check point software** باسم تفقد

الحالة الكاملة **state full inspection** فهو موجود في برنامج **firewall-1** من شركة نفسها وبرنامج **pix firewall** من شركة سيسكو وبرنامج **On Guard** من شركة **On technology** وبرنامج **firewall/plus** من شركة **network-1** وكما هو الحال في تقنية ترشيح الرزم فان هذه التقنية تستقبل أولا الرزم علي مستوي طبقة الشبكة **Network layer** ثم تقوم بتفحص جميع الرزم ومقارنتها مع نماذج معروفة من الرزم الصديقة وفيما تعطي طريقة تفقد الحالة الكاملة أداء اعلي بقليل من أداء توكيلات التطبيقات إلا أن الجدل يبقي قائما فيما إذا كانت آمنة مثلها أم اقل أمنا منها[124].

3- الوظائف الأساسية للجدران النارية: تتلخص أهم الوظائف التي تؤديها الجدران النارية في 125:

- منع دخول المستعملين غير المصرح لهم بالدخول إلى الشبكة.
- حماية استخدام الخدمات الهامة عند الدخول إلى الشبكة ومغادرتها.
- حماية عامة من جميع الهجمات.

وبذلك يمكن لأي شركة أو بنك أو مؤسسة حكومية حماية وتامين المعلومات الخاصة بها من أي مستعمل غير مصرح له بالدخول وهذا يعني أن برمجيات جدران النار تحتو يعلى مجموعة من السياسات التي تجعلها بمثابة مصفاة لمنع الطلبات المشبوهة من الوصول إلى الجهاز الخادم ؛ كما يمكن إعدادها بحث يتم إسقاط ووقف أية طلبات واردة تحاول النفاذ إلى الخادم من منفذ لم يحدد ضمن سياسات هذه البرمجيات , ويمكن لبرنامج الجدار الناري أن يقوم بحماية الشبكة من الفيروسات والحماية من البرمجيات الدخيلة بحسب ما سطر داخل البرمجة.

3- مزايا وعيوب الجدران النارية:

يمكن القول وكما في أية تقنية جديدة أن الجدران النارية لها عيوب ومزايا نلخصها في ما يلي[126]:

1- فيما يخص المزايا:

- توفير الحماية اللازمة للشبكة والمعلومات.
- توفير خدمات تشفير عالية القوة.
- الجدار الناري يتوافق مع جميع الشبكات المفتوحة.
- تخزين المعلومات والعمليات التي تمر من خلاله.

---

[124]- **أمن الشبكات..**[على الخط المباشر]. زيارة يوم: 2006/03/18 متوفر على الموقع: http://www.jubailnet.com/vb/forumdisplay.php

[125]- **حجازي.عبد الفتاح البيومي. الحكومة الإلكترونية.المرجع السابق.ص. 60.**

[126]- **حجازي.عبد الفتاح البيومي. الحكومة الإلكترونية.المرجع نفسه.ص. 63.**

- متابعة المستخدمين للشبكة وكل من يحاول العبث بها.

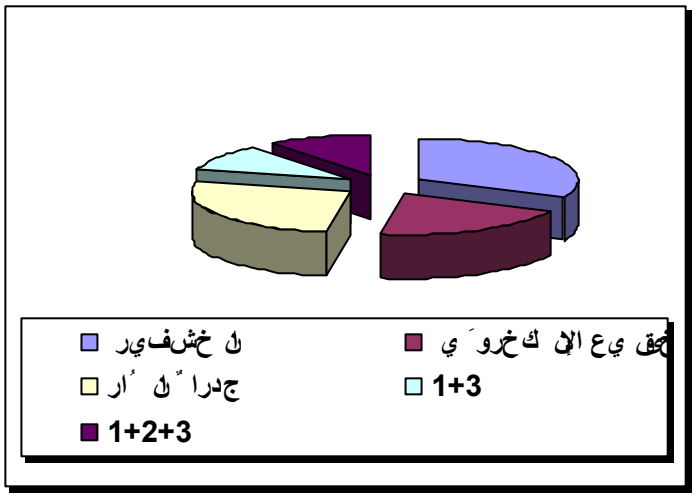
أما فيما يخص العيوب:

- لا يتعامل الجدار الناري مع البرامج الداخلية التي تهاجم النظام.

- لا يقدم الحماية للنقل الإذاعي والتلفزيوني.

التشفير ،التوقيع الإلكتروني، جدران النار أهم الطرق المعتمدة لحماية المعلومات وضمان سلامتها أثناء مسارها وعند سؤال الطلبة عن أهم وأنجع الطرق لحمايتها كانت الإجابة كما هي موضحة في الجدول رقم 20 من الصفحة 146

إذن فإن أنجع طرق الحماية حسب الطلبة هو عملية التشفير(31,5 %) والتشفير هو إعادة كتابة البيانات باستعمال أحد مفاتيح التشفير، ثم تليها جدران النار بنسبة (26,3 %) وهو محاولة تصفية البيانات الداخلة إلى الداخلية لمؤسسة ما عن طريق مصفاة يطلق عليها جدران النار، ومع تطور معاملات التجارية وظهور الإقتصاد الشبكي كالتجارة الإلكترونية والتسوق الإلكتروني أدى إلى ظهور وسيلة جديدة هي التوقيع الإلكتروني والذي يعد وسيلة لا غنى عنها في مثل هذه المعاملات كما يمكن الجمع بين وسيلتين آو أكثر من الوسائل السالفة الذكر وذلك لضمان حماية أكبر وهذا ما نوضحه في الشكل البياني التالي :



الشكل رقم:15 وسائل حماية المعلومات

5-2. أمن المعلومات: الأخلاق (أخلاق التعامل في مجتمع المعلومات)

إن الأخلاق تعد قوة ردعية في المجتمعات لا يستهان بها غي إرشاد وتوجيه سلوكيا ت الناس فما هو الدور الذي تلعبه الأخلاق في مجتمع المعلومات؟

5-2-1. مجتمع المعلومات.

أن مجتمع ما بعد الصناعة هو مجتمع المعلومات وفي مايلي نتطرق إلى اهم عناصر هذا المجتمع الجديد

5-2-1-1. مفهوم مجتمع المعلومات.

لابد في البداية إلى الإشارة أن هناك العديد من التعريفات لمجتمع المعلومات وأن تعريف مجتمع المعلومات لا غير واضح المعالم بشكل عام

إنه مفهوم يرى التحول من مجتمع صناعي إلى مجتمع حيث المعلومات هي القوة الدافعة والمسيطرة وهناك من يرى أنه المجتمع الذي ينشغل معظم أفراده بإنتاج المعلومات أو جمعها أو اختزانها أو معالجتها أو توزيعها [127]. كما يرى البعض بأن مجتمع المعلومات هو المجتمع الذي تستخدم فيه المعلومات بكثافة كوحي للحياة الاقتصادية والاجتماعية والثقافية والسياسية، ويرى الدكتور ناريمان متولي أن مجتمع المعلومات هو المجتمع الذي يعتمد في تطوره بصفة رئيسية على المعلومات الحاسبات الآلية وشبكات الإتصال أي أنه يعتمد على التكنولوجيا الفكرية التي تضم سلع وخدمات جديدة مع التزايد المستمر للقوة العاملة المعلوماتية التي تقوم بإنتاج وتجهيز ومعالجة ونشر وتوزيع وتسويق هذه السلع والخدمات

وقد أدى عدم الاتفاق على مجتمع المعلومات إلى اختلاف الرؤى حوله فقد أشارت دراسة حديثة عن الموضوع إلى ثلاث رؤى لمجتمع المعلومات

الرؤية الأولى: وهي رؤية أوربية يمثلها العالم الاجتماعي(إيان مايلز **Ian miles**) وترتكز على الإنتشار الواسع لتكنولوجيا المعلومات والإتصالات ومالها تأثيرات هي التي تشكل مجتمع المعلومات

الرؤية الثانية: هي رؤية يابانية ويمثلها العالم الاتصالات اليابانية جوهوكا شاكاي **johoka shakia** وهي يرتكز على تدفق أو انسياب المعلومات بكميات هائلة عبر كل الوسائل في المجتمع وترتكز.

الرؤية الثالثة: وهي رؤية أمرقية ويمثلها عالم الإقصاد (فريتز ماكلون) على أن نسبة متزايدة من الناتج القومي الكلي للدولة تجيء من إنتاج المعلومات ، ومن ثم أضافت الإقصاديات الحديثة قطاعا جديدا إلى القطاعات المعروفق[128].

ومن وجهة نظرنا أن لكل هذه الرؤى روافد تصب في نهر واحد ,وان كل واحدة من الرؤى الثلاثة السابقة إما أن تكون سببا لأخرى أو أن تكون حتمية لسابقتها .

إن عصر ما بعد الصناعي أو مجتمع المعلومات كما يطلق عليه هو حصيلة لتراكمات إحتماعية وعلمية وثقافية طيلة سنوات، وقد ساهم غب دخول هذا العصر التطورات التقنية والتكنولوجية التي عرفها العالم المعاصر؛

---

[127]– عبد الهادي ,محمد فتحي.**المعلومات وتكنولوجيا المعلومات على أعتاب قرن جديدة**. القاهرة:الدار العربية للكتاب ,2000.ص.18.

[128]– عبد الهادي ,محمد فتحي. المرجع السابق.ص.18.

وتعد الولايات المتحدة الأمريكية وكندا ودول أوروبا من بين الدول السباقة للإنخراط في مجتمع المعلومات الكوني؛ أما دول العالم الثالث بصفة عامة والدول العربية خصوصا فقد خطت خطوت محتشمة للإنضمام لهذا الركب وعند سؤال الطلبة عن ضرورة آو حتمية الإنخراط في مجتمع المعلومات كانت الإجابة كما هي موضحة في الجدول رقم21 من الصفحة 146
إذن وحسب نتائج الجدول فإن الأغلبية الساحقة لعينة الدراسة (97,3 %) ترى أن دخول عالم المعلومات هو ضرورة ملحة تفرضها الظروف المعاشة وهذا من أجل اللحاق بركب الحضارة وعدم الاضمحلال في بوتقة العولمة .

5-2-1-2. خصائص مجتمع المعلومات:

يقدر علماء الاقتصاد أن حجم التعاملات المالية التي تتم يوميا عبر الأجهزة والشبكات الإلكترونية للمؤسسات المالية يصل إلى 25بليون دولار , ولعل هذا الرقم العالي يظهر اعتماد المجتمعات في هذا العصر على التجهيزات المنية على تقنيات الحاسب [129] ؛ويمكن تلخيص أهم خصائص التي تطبع مجتمع المعلومات[130]:

1- **انفجار المعرفة:** يرى العديد من لباحثين أن المعلومات المنتجة في الحقبة المعاصرة أكثر أهمية مما أنتج في كل تاريخ البشرية ,كما أنها تتزايد بمعدلات كبيرة نتيجة التطورات التي يشهدها العالم ونتيج ة بروز تخصصات جديدة.

2- **زيادة أهمية المعلومات:** في مجتمع المعلومات ازدادت أهمية المعلومات وأصبحت المعلومة تدخل في كل الأنشطة والصناعات، كما تمثل المادة الخام لقطاعات كثيرة من قطاعات المجتمع المعاصر مشكِلة ما يمكن أن يطلق عليه" صناعة المعلومات " وأصبح ينظر إلى المعلومات كمورد أساسي وإستراتيجي يمكن أن يباع ويشترى.

3- **نمو المجتمعات والمنظمات المعتمدة على المعلومات** :يتميز مجتمع المعلومات كذلك بظهور منظمات تعتمد كليةً على المعلومات مثل مؤسسات الجرائد والأخبار والإستعلامات والبنوك وشركات التأمين....

ويلاحظ أن انفجار أو تضخم هذه المنظمات قد بدأ في الظهور في نفس الوقت الذي شهد بدايات ثورة المعلومات المعاصرة.

4- **تعدد فئات المتعاملين مع المعلومات** : أوجد مجتمع المعلومات فئات كثيرة تتعامل مع البيانات والمعطيات والمعلومات وتشتعل بها منها:

- العلماء والفنانون والمصممين وغيرهم ممن يقدرون على إنتاج وإيجاد معلومة جديدة أو يعيدون تشكيل نماذج معرفية جديدة من واقع المعلومات الحالية.

---

[129]- عباس , طاهر محمود.**المكتبات الرقمية وشبكة الأنترنت**.القاهرة: المركز الأصيل ,2003.ص.45.
[130]- لغقاب، محمد. مجتمع **الإعلام والمعلومات:ماهيته وخصائصه**.الجزائر:در هومة ،2003.ص.88.

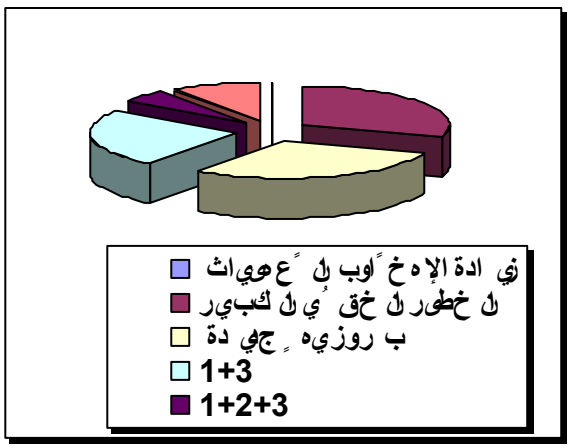
- العاملون في نقل وتوصيل المعلومة.

- العاملون في تخزين المعلومات كأخصائي المعلومات وأمناء المكتبات ومبرمجي الحاسب.

5- قلة الاعتماد على الورق: حيث تزايدت بصفة مطردة كميات المعلومات المنتجة على وسائط غير ورقية وفي المقابل فإن استعمال الورق أخد يتقلص.

إن العصر الذي نعيشه بكل حيثيات ه هو مجتمع المعلومات هو مجتمع المعلومات بحق؛ فقد غدت المعلومات العصب المحرك لكل مناحي الحياة الاجتماعية والسياسية والثقافية والعلمية، وقد تزايد الاهتمام بالمعلومات مند أن أصبحت تمثل مصدرا أساسيا للدخل القومي للدول المنتجة للمعلومات، وقد ظهرت قطاعات تُعنى بالمعلومات عي كل مراحلها أي مند إنتاجها وإلى غاية نشرها وتوزيعها؛ وقد اتسم مجتمع المعلومات بعدة خصائص نوجزها في الجدول22 من الصفحة 146

إذن فحسب عينة مجتمع الدراسة فإن الخاصيتين اللتان تطبعان مجتمع المعلومات هي زيادة الاهتمام بالمعلومات وكذا التطور التقني المذهل (31,5 %) وهذا ما يؤكده حشد ميزانيات ضخمة والتي تخصصها الدول المتقدمة من أجل تنمية البحوث العلمية وكذلك إنشائها لأكبر مراكز البحوث العلمية والتكنولوجية، إن هذا الاهتمام الكبير بالمعلومات أدى إلى ظهور مهن جديدة كصناعة المعلومات وهذا ما عبرت عنه (26,3 %) من عينة الدراسة، أما باقي الطلبة فيرون أن كل هذه الخصائص السالفة الذكر لها نفس الأهمية في مجتمع المعلومات ،ويمكنا أن نوضح ذلك بشكل أفضل كما يلي:



الشكل رقم:16 خصائص مجتمع المعلومات

5-2-1-3. أبعاد مجتمع المعلومات:[131] :

يصوغ بيل (**Bell, 1973**) فكرة الأركان الإحداثية التي تفسر الأطر الاجتماعية وتدرس تماسك المجتمع من خلال وضع مفهوم يوضح تنظيم المجتمع، فيصنف المجتمع ما بعد الصناعي (مجتمع المعلومات) إلى ثلاثة

[131]- عبد الباري ,**وائل إسماعيل حسن.أسس مجتمع المعلومات العربي قراءة للأبعاد المعرفية والتقنية في المجتمع العصري**.[على الخط المباشر]. زيارة يوم: 2006/03/18 متوفر على الموقع:
http://www.arabcin.net/arabic/5nadwhauthors albari.htm.

كيانات: اجتماعية، سياسية، ثقافية. و يشتمل الكيان الاجتماعي على النواحي الاقتصادية والتكنولوجية ونظم العمل، أما الكيان السياسي فهو المعنى بتوزيع السلطات والكيان الثقافي يهتم بالمعاني والرموز.
وفى ضوء هذه الكيانات يرى بيل **Bell** أن في مجتمع المعلومات يحدث التالي:
1- تتغير أدوار الأفراد في المجتمع لبلوغ غايات محددة، ويعتمد على ذلك ظهور أنماط جديدة في السلوك على الأفراد مراعاتها لمواءمة حالة المجتمع الجديد ومثال ذلك انتشار النواحي التخصصية والعوامل المعرفية والتي تتطلب نشاطا مماثلا من الأفراد.
2- تنشأ علاقة تنافسية بين البناء الاجتماعي والكيان السياسي وذلك لأن مجتمع المعلومات قائم على تطور البناء الاجتماعي وظهور الجوانب المعرفية والأهمية المعلوماتية مما يسحب البساط من تحت أرجل النخبة السياسية الحاكمة.
3- يعتمد ظهور أنماط جديدة في حياة أفراد المجتمع على درجة المعرفة النظرية والإدراكية **Cognitive Theoretical knowledge** التي ترتبط بجوانب الثقافة المجتمعية، مما قد يؤدى إلى ظهور النزعة الفردية .

وينظر بيل **Bell** إلى مجتمع المعلومات على أن محوره الرئيسي ولب تكوينه يتمثل في عملية المعرفة ويعلل ذلك بالقول أن المعرفة هي الضابط الاجتماعي والموجه لعمليات الإبداع والتجديد والتغيير التي تعمل على نشأة علاقات وهياكل مجتمعية جديدة. ويتمركز مفهوم هذا المجتمع الجديد حول القطاع الاقتصادي والمعنى بالإنتاج والخدمات وتقسيم فئات العمل.

أما الأبعاد المعرفية والتكنولوجية فى مجتمع المعلومات فيرى بيل **Bell** المجتمع ما بعد الصناعي بأنه مجتمع معرفي من خلال بعدين:
أ- تنامي مصادر التجديد والاختراعات القائمة على البحث والتطوير وازدياد العلاقة الوثيقة بين العلم والتكنولوجيا وذلك بسبب مركزية المعرفة النظرية.
ب- كون مؤشرات معدل الناتج القومي ونوع العمل قائمة بصفة كبيرة على الحقل المعرفي، ويتجلى ذلك بوضوح فى طبيعة تقسيم المهن التي تركز على الخدمات المعلوماتية.

5-2-2. أخلاق مجتمع المعلومات.

5-2-2-1. تعريف أخلاق مجتمع المعلومات.

إن مصطلح الأخلاق يتناول المبادئ التي توجه السلوك البشري وهو يتعلق بقضايا الصواب والخطأ ,العدل والظلم ,الصحيح وغير الصحيح وذلك بالنسبة لمجتمع ما أو جماعة معينة[132].

وإذا كانت دراسة الأخلاقيات في مهن المعلومات تعتبر فرعية لدراسة الأخلاقيات بصفة عامة ، فليس هناك اتفاق على تعريف محدد لمصطلح الأخلاقيات فالبعض يستخدم المصطلح بطريقة عامة للدالة على[133]:

---

[132]- عبد الهادي ، فتحي. **المعلومات وتكنولوجيا المعلومات على أغتاب قرن جديد.القاهر**ة: مكتبة الدار العربية للكتاب.،2000.ص.37.

- طريقة الحياة التي يرتضيها مجتمع معين.

- مجموعة من القواعد السلوكية التي تضمن تسيير المجتمع نحو الخير والصواب في مواجهة الشر والخطأ.

وكلمة الأخلاق **Ethics** مستخلصة من الجذر اليوناني **Ethos** والذي يعني خَلق؛ وتكون الأخلاق طقما من المعتقدات أو النمطيات أو المثاليات الموجِهة للأفراد.

ويذهب (كلايد كنغ **Clyde king**) إلي أنه يمكن تعريف الأخلاق بأنه نظام من المبادئ الأخلاقية التي تحدد السلوك الصواب والسلوك الخطأ وذلك بالنسبة لمجتمع أو أمة أو جماعة معينة.

وتزداد أهمية الأخلاق في الوقت الحالي أي في مجتمع المعلومات مع تزايد المشكلات الأخلاقية التي يواجهها العالم المعاصر ؛وعندما يذهب الباحثون في الغرب بعيدا في البحث عن أخلاق مجتمع المعلومات فإنهم يبحثون ويدرسون انطلاقا من مجتمعاتهم ومفاهيمهم وتوجهاتهم ؛ وهم يحاولون بذلك ان يحددوا إالأخلاق بما ينفع هذه المجتمعات ويحافظ على تماسكها ؛وأخلاق مجتمع المعلومات لاتختلف عن الأخلاق بصفة عامة وفي الواقع يمكن إيجازها بأنها أخلاق رجل المعلومات وهي مجموعة من المبادئ والقيم التي يجب أن يتخلق بها الشخص في خضم هذا المجتمع وهي تختلف عن القانون لأنها تحدد تصرفات الناس دون إجبار أوإلزام قانوني.

5-2-2-2. أهم المبادئ الأخلاقية في مجتمع المعلومات:

إن الإنسان المعاصر ينظر إلى مجتمع المعلومات على أنه نموذج أخلاقي علمي واجتماعي متقدم ،سيتيح لمجتمعاتنا المخالفة إمكانات أكبر في تبادل المعلومات وتحقيق حرية إنسيابها ،وتحقيق فوائد متوازنة لمختلف المجتمعات وخاصة تلك الاضعف ثقافيا وإقتصاديا وتقنيا ،إلا أن الوقائع تختلف تماما عن النمودج الاخلاقي ويمكن ان نلخص أهم المبادئ والقيم الأخلاقية التي يجب ان تتوفر في مجتمع المعلومات في[134]:

- يشكل تعدد اللغات والثقافات في دائرة المعلومات العالمية ميزة أخلاقية وعلمية وثقافية هامة لابد من المحافظة عليها ضمانا لتنوع وتكامل دائرة المعلومات الدولية وللحفاظ على التراث الثقافي للبشرية ,وحرصا على تطور المشهد الثقافي العالمي.

- تشكل الفجوة الرقمية إحدى اهم المشكلات الأخلاقية التي يواجهه العالم وتتفرع عنها مشكلات أخلاقية وإقتصادية وإجتماعية وعلمية لايمكن للعالم ان يشيح نظره عنها ؛ وإن حل هذه المشكلات يعد الخطوة الأولى الضرورية لبناء مجتمع المعلومات.

---

[133] -الهوش ،أبو بكرمحمود. **التقنية الحديثة في المعلومات والمكتبات:نحو إستراتيجية عربية لمستقبل مجتمع المعلومات**.القاهرة: دار الفجر،2002ص.244.

[134] - **مشروع ميثا الشرف العربي لأخلاق مجتمع المعلومات**.[على الخط المباشر].ريارة يوم:2006/02/16. متوفر على الموقع: http://www.arabcin.net/arabia3000/arabia1htm.

– دعم التعاون العالمي في في مجال تبادل المعلومات ليس مسألة نظرية تطرح في المنتديات والمؤتمرات العالمية بل هي مسؤولية أخلاقية جماعية يتوجب على البلدان المتقدمة دعمها من خلال إتاحت المعلومات العلمية وعدم حجبها عن الدول النامية.

– إن مقهوم القرية الكونية يفرض أساسا نشوء مسؤولية إجتماعية جماعية إخلاقية لحل المشكلات التي يعاني منها سكان هذه القرية وأهم المسائل التي يجب الإنتباه لها في مجتنع المعلومات هي:

* الحق في الملكية الفكرية وإحترام أعمال الغير وعدم التعرض لها بأي نوع من أنواع الإعتداد والإستحواد.

* الحق في حماية خصوصية الأفراد والمؤسسات وإحترام الحياة الخاصة بهم.

* حرية إكتساب المعلومة.

* مصادقة المعلومة وكيفية التعامل معها في ظل الإنفجار المعرفي.

* كيف يمكن حماية الشبكة من التلوث ومن التخريب فهي شيئ مشترك في مجتمع المعلومات.

5-2-2-3. الإفرازات الأخلاقية الجديدة في مجتمع المعلومات:

من الواضح أن التقنية المتقدمة والوصول إلى المعلومات المتنوعة أو حتى التمكن من هذه المعلومات وإمتلاكها كل هذا لا يجعل من الإنسان المستفيد معلوماتيا أكمل او أكثر صفاء وثراء روحيا ؛ إذا المهم هو مضمون المعلومات وأهدافها الإجتماعية ونوع علاقات الإنسان بها والموشور الذي يتعامل معها من خلاله وهذا ما يحدد الغالم الروحي للإنسان ، بل وغالبا ماتطرح التكنولوجيا المتقدمة ضروريات جديدة تلزم مالكها بالتمتع بأخلاقيات منظبطة إذ أن هناك فرق بين التعامل مع الحواسيب كهدف والتعامل معها كمجرد وسيلة.

لا شك ان إنتسار الحواسيب الشخصية والوسائل الحديثة يمكن أن يقوي الفردية لذى الناس ويضعف الروح الجماعية وكثلفة الإختلاط قي مابينهم لأن تكنولوجيا المعلومات مبنية أساسا على الإستخدام الفري وتحد من الإختلاطات المباشرة ؛ فالرفيق والزميل والصديق يصبح غالبا الآلة أو التجهيزات في حين يصعب التخلي عن معاشرة الناس كقيمة روحية عالية تَلزم الإنسان وترافقه مند الأزمة الغابرة.

إن موجة التكنولوجيا الجديدة تبرز على السطح ضروبا من الإغتراب أو الإستلاب ، ولا سيما ما يسمى بالإغتراب المعرفي ،وأحد جوانب هذا الإغتراب شعور الشخص بالدونية أو النقص إتجاه إمكانيات الآلة المتنامية بإستمرار ؛ ويرى بعض علام النفس أن منطق الآلة الصارم وتعامل الإنسان معه قد يؤدي مع الزمن من الوجهة النفسية على الأقل إلى فقدان حس الإبداع كما أن مايدعم هذه العولة الإجتماعية أو تشارك في وضع واقع تخيلي بديلا للواقع الفعلي هو ألعاب الكمبيوتر والموديلات والنمادج[135].

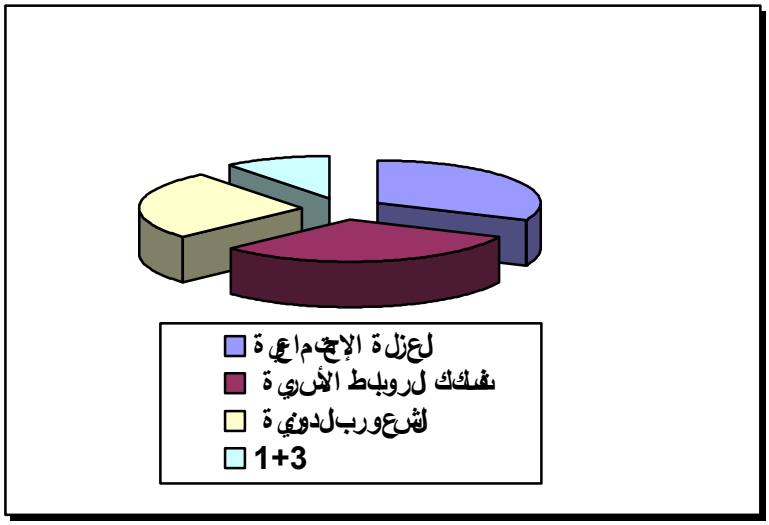
---

[135]– النقري،معن.**المعلوماتية والمجتمع / مجتمع ما بعد الصناعة ومجتمع المعلومات**.المغرب؛ لبنان:المردز الثقفي العربي،2001.ص.20.

إن كل هذه الإفرازات السالفة الذكر والتي يتركها الإنخراط في مجتمع المعلومات على السلوكيا ت البشرية تعد من بين سلبيات هذا المجتمع الجديد وعند الإستفسار عن رأي الطلبة حول الموضوع كانت الإجابة بالإجماع على أنه لمجتمع المعلومات إفرازات سلوكية على الأفراد والنتائج كما هو موضح في الجدول رقم 23 في الصفحة 147

أما عن أهم هذه الإفرازات على السلوك البشري فإنه يمكن أن يتسبب فيخلق عزلة اجتماعية لدى الأفراد كما يمكن أن تساعد في تفكك الروابط الأسرية والاجتماعية داخل المجتمع كما تساهم في خلق نوع من الشعور بالدونية والإنهزامية داخل الفرد هذا أمام إمكانا ت الآلة اللامحدودة والجدول 24 في الصفحة 147 يوضح ذلك

إذن فإن الطلبة يرون أن خلق العزلة الإجتماعية لدى الفرد أهم مشكل يخلقه مجتمع المعلومات بنسبة (31.5 %) وهذه العزلة تنتج من بقاء الفرد لمدة ساعات أمام الآلة مما يجعله يبتعد تدريجيا عن محيطه، إضافة على الطرق المستحدثة غب التعليم كالتعليم عن بعد والذي يفقد الفرد الصديق والأستاذ والزميل وكل هذه العناصر تصبح متوفرة بطريقة إفتراضية؛ كما يؤدي الإنخراط في مجتمع المعلومات إلى تفكك الروابط الأسرية والإجتماعية (31,5 %) وهذا لنفس السبب وهو بقاء الفرد لأرقات طويلة أمام شاشة الحاسب مما يؤدي إلى القضاء على الروابط داخل الأسرة ؛إن هذه الإمكانيات الهائلة للآلة تجعل الإنسان يقف أمامها عاجزا مما يخلق لديه نوع من الإنهزامية والشعور بالدونية أمامها ويمكننا تمثيل هذه النتائج كما يلي:



الشكل رقم 17 الإفرازات الأخلاقية لمجتمع المعلومات

5-2-3. أخلاق الحاسب والانترنت.

لقد أدت الانترنت إلى خلق إفرازات جديدة في العالم منها ما هو سلبي ومنها ما هو إيجابي .

5-2-3-1. الأنترنت: الماهية والخدمات.

1- تعريف الأنترنت:

إن الأصل اللغوي لكلمة شبكة هو الفعل الثلاثي شبك بمعنى تداخل يقال تشبيك الشيء تداخل بعضه في بعض.

في حين تتكون كلمة الأنترنت الإنجليزية الأصل من قسمين **Inter** وهو إختصار لكلمة الدولية **International** والقسم الثاني وهو **net** وهو إختصار **Network** وهذا التعريف اللغوي يقودنا لبيان التعريف العلمي لهذه الشبكة إذا وردت تعاريف متعددة أهما أنه:" إرتباط لأف من الكمبيوترات في الإتصال مع بعضها البعض وهي شبكة الشبكات تشمل ملايين من المستخدمين يوميا "[136].

وقد مرت شبكة الأنترنت بعدت مراحل إلى أن وصلت إلا ما هي عليه الآن [137]: - بدأت فكرة الأنترنت كفكرة عام 1964 عندما تمكن الباحثون في مؤسسة **Rand comporation** من تقديم مفهوم الشبكة وتحويل مجموع البيانات.

- بدأ التنفيد المادي عام 1969 بإعتبارها بمثابة شبكة من 4 نقاط معتمدة على تحويل مجموع البيانات يطلق عليها **ARPANET**.

- أثناء الثمانينات إلتحقت عدة شبكات منها **BIRNET- CSNET** بالأنترنت

- عام 1984 تم ربط مايزيد عن 1000كمبيوتر بشبكة **ARPANET**.

- 1983 كانت **MILNET** جزء من الأنترنت وكانت تربط بين منظمات عسكرية ومنظمات بحثية وجامعات في المجال العسكري.

- عام 1984 تك إغلاق **ARPANET** رسميا مع إستمرار نقاط الوصل والشبكات الفرعية في آداء عملها.

- عام 1986 قانت مؤسسة العلوم القومية **national science fondation(NSF)** يربط خمسة من شبكاتها المعتمدة على الحاسبات فائقة السرعة والتي أصبحت فيما بعد تعرف بالأنترنت

- عام 1987 تحملت **NSf** المسؤولة عن إدارة هذه الشبكة.

- عام 1989 بلغ عدد المستخدمين 80.000 مستخدم.

---

[136]- مومني.بشار طلال.مشكلات التعاقد عبر الأنترنت:دراسة مقارنة.الأردن:دار العالم الكتب ,2004.ص.10.

[137]- مرسي, نبيل محمد.التقنيات الحديثة للمعلومات.الإسكندرية:دار الجامعة الجديدة، 2005.ص.181.

- عام 1991 رفعت **Nsfnetr** مقيودها على الأنترنت لأغراض تجارية.

- 1992 ظهرت لأول مرة تطبيقات الإقتصاد الإلكتروني المعتمدة على الانترنت.

- 1997 كان هناك حوالي 16 مليةن مستخدم في كافة أنحاء العالم.

- ومن ذلك الوقت وعدد المستخدمين يتزايد يوما بعد يوم والخدمات المقدمة في تطور وأصبحت الأنترنت شبكة عامة محققة للمشاركة ومستقلة.

الانترنت ذلك الفضاء المترامي الأطراف والذي غير مجرى الحياة، وجعل من الحياة أكثر سهولة ويسرًا، فقد فرضت نفسها كمصدر للمعلومات وأداة للاتصال حتى غدت الأداة الأكثر شعبية مند بدأ تواجدها؛ وقد نمت حتى غدت أهم مظاهر التكنولوجيا العالمية، وعند الإستفسار عن استعمال الطلبة لانترنت كانت الإجابة كما هي موضحة في الجدول رقم 25 من الصفحة147

إذن فقد أجاب اغلب الطلبة (94,8 %) على أنهم من مستعملي الأنترنت وذلك لأن عينة الدراسة تشمل طلبة الدراسات العليا،وهذه الفئة لا غنى لها عن الانترنت باعتبارها مصدر هام للمعلومات خصوصا وأغلب الطلبة في إطار تحصير مذكرات تخرجهم مما يجعلهم على إرتيادها.

2- خدمات الانترنت[138]:

1- البريد الإلكتروني: لإرسال وإستقبال الرسائل بسرعة كبيرة.

2- القوايم البريدية:إنشاء وتحديث قوائم العناوين البريدية الخاصة بمجموعلات الأشخاص.

3- خدمة مجموعة الأخبار: وهي شبيهة بخدمة القوائم البريدية إلا إنها تختلف في أن كل عضو يستطيع التحكم في نوع المقالات التي يريدإستلامها.

4- خدمة الأستلام الشخصي:حيث يمكن من خلال هذه الخدمة للإستعلام عن العناوين البريدية لأي شخص أو جهة تستخدم الأنترنت والمسجلين لديها.

5- خدمة المحادثات الشخصية: حيث يمكن التحدث مع الآخر بالصوت والصورة والكتابة.

6- خدمة الدردشة الجماعية:تشبه الخدمة السابقة إلا إنها في الغالب مكن لأي شخص أن يدخل في المحادثة أو يستمع عليها دون إختيار الآخرين.

7- خدمة نقل الملفات: لنقل الملفات من حاسب إلى آخر.

---

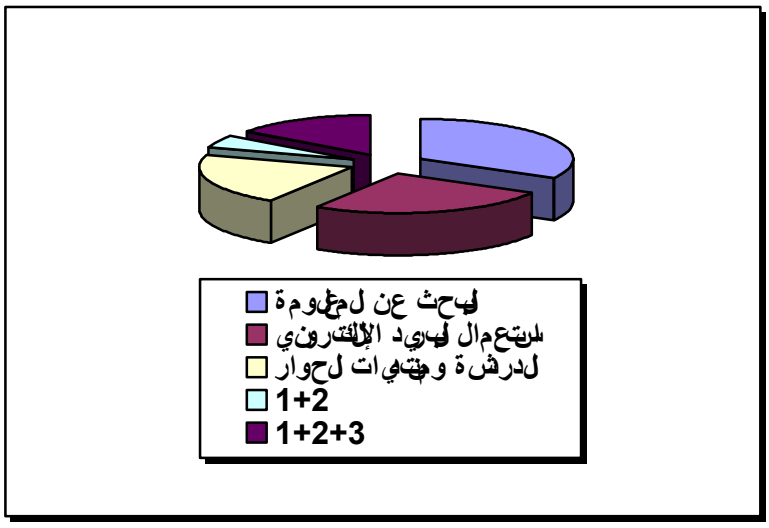
[138]- الجنبهي، منير محمد.الجنبهي، ممدوح ،منير محمد.الطبيعة القانونية للعقد الإلكتروني.الإسكندرية:دار الفكر الجامعي ،[د.ت.].ص.16-17.

8- خدمة شبكة الإستعلامات الشاملة **Gopher** تفيد في خدمات كثيرة كنقل الملفات والمشاركة في القوائم البريدية.

إضافة إلى خدات أخرى كخدمة الدخول عن بعد والصفحة الإعلامية العالمية...إلخ.

إذن فقد وفرت الانترنت العديد من الخدمات التي ت قدمها لمرتاديها بدأبالبريد الإلكتروني والذي حل العديد من مشاكل وعقبات البريد التقليدي حيث أصبح أكثر سرعة وسهولة، إضافة إلى منتديات الحوار والدردشة ومواقع التسلية،هذا إلى جانب أهم خدمة تقدمها الانترنت على الإطلاق وهي البحث الحر عن المعلومات وعند الإستفسار عن أهم الخدمات المحبذة لدى الطلبة كانت الإجابة كما هي مبينة في الجدول رقم 26 من الصفحة 147

ومن تحليل نتائج الجدول نلاحظ أن أكبر استعمال للانترنت هو لغرض البحث العلمي أي البحث الحر عن المعلومة (31,5%)، وهذا باعتبار الطلبة في الدراسات العليا وهم بصدد الإعداد لمذكرات التخرج،وبالتالي تزداد حاجتهم للمعلومات؛ ثم يليها استعمال البريد الإلكتروني(26,6%)وهي الخدمة الأكثر شعبية لدي جميع الناس وبمختلف الفئات والأعمار وها للمميزات التي تتصف بها هذه الخدمة إضافة إلى مجانية الإرسال؛ ثم تأتي إغراض التسلية والترفيه في المرتبة الموالية (21%)؛ لكن استعمال الأنترنت يشمل عادة جميع هذه الخدمات وهذا حسب الحاجة، والرسم البياني التالي يوضح توزيع هذه الخدمات:



الشكل رقم 18 خدمات الأنترنت

2-3-2-5. مخاطر الأنترنت:

ينتج عن استعمال شبكة الأنترنت مخاطر لا يمكن تداركها فالجرائم التي ترتكب عن طريق الشبكة تسمح للمجرمين بالإقدام على جرائمهم وهم على يقين بأنهم لا يمكن كشفهم وتبقى السرية مضمونة فهي لا تعطي أي دليل حسي وأهم هذه المخاطر[139]:

1-الصور اللاأخلاقية: إن إرسال صور لا أخلاقية عبر الانترنت غير مكلف بحيث يمكن إرسالها بالبريد الإلكتروني من شبكة سرية تتلقى هذه المراكز الرسالة فتلقي عنوان المرسل ثم تقوم بنشرها مرة ثانية وبالتالي يصبح من المستحيل معرفة المصدر الأصاي للرسالة او الصورة.

2-الإحتيال: يتم الإحتيال بعدة طرق مثلا يتم عرض بضاعة او صورة إباحية أو غيرها فيطابها أحد المشتركين بالبريد الإلكتروني حيث يطلب منه تحويل ثمنها إلى حساب مصرفي يحدد رقمه في أي مصرف موجود فيقدم طالب البضاعة على إرسال المبلغ حيث يتم سحبها ولا ترسل في المقابل البضاعة أو ترسلة خاطئة أو غير مطلوبة.

التعدي على الحقوق الأدبية والفكرية يمكن بواسطة شبكة الأنترنت بث الأعمال الأدبية والفكرية والأفلام السنمائية للجمهور ويستطيع أي منهم الحصول على نسخة من هذه الأعمال وهذا يشكل تزويرا وتعديا على حقوق المؤلف ، كما يمكن إستعمال شبكة الأنترنت لمارية ألعاب القمار ونشر المعلوملت التي تشكل خطرا كالمعلومات التي تحرض على ارتكاب الجرائم كالتسلح الغير شرعي أو العصيان أو الثورة او الإنتحار وكذاك يمكن إستعمال طالب البضاعة وإستعمال إسمه للقيام بنشطات إجرامية وإستعمال بطاقات الإئتمان بطرق غير فانونية مثل الهبات الخيرية والأرباح الوهمية والإستثمار في الشركات الخاسرة.

5-2-3-3. أخلاقيات الأنترنت[140]:

لقد فتحت الأنترنت أفاقا كبيرة غير مسبةقة في المجالات المختلفة وعلى الأخص في مجالات التعليم والبحث العلمي ونشر الوعي الثقافي وكذا النواحي السياسية والإجتماعية , ولكن ثم إستغلالها في الوقت نفسه من جانب الجماعلت الإجرامية عبر العالم في أغراض أخرى من بينها بث المعلومات المنافية للآداب والمساعدة على العمليات الغرهابية المختلفة.

إن طبيعة الأنترنت التفاعلية واللامركزية على مستوى العالم بالإضافة إلى أهميتها في توفير كم هائل من المحتوى المتاح من وإلى مكان أي مكان قد يؤدي إلى عدد كبير من القضايا القانونية والأخلاقية من بين بينها المحتوى الغير القانوني في الأنترنت.

وتضع معضم دول العالم بعض القيود على نوع المحتوى الذي يعالج ويوزع في نطاق حدودها السياسية الوطنية ، وتعكس هذه القيود المفروضة في أي دولة التقاليد والأعراف الثقافية والقانونية ,بالإضافة إلى القيم الدينية والأخلاقية السائدة فيها وقد تختلف من دولة إلى أخرى.

---

[139]- مغبغب ،نعيم.**مخاطر المعلوماتية والأنترنت**.لبنان:[د.ن.] 1998.ص.213.

[140]- الهوش ،أبو بكر محمود.المرجع السابق.ص.256.

ويمكن أن نخلص أهم عمليات التعامل مع الأنترنت في:

- إتخاد كافة التدابير الوقائية لحماية أفراد المجتمع وحمايته من البيانات الضارة.
- كفالة أمن البيانات والمعلومات وسريتها ومراعات الخصوصية وإحترامها.
- ضمان أن تكون المعلومات التي تقدمها لرفع مستوى المجتمع الإقتصادي والسياسي والإجتماعي.
- ضمان حماية حقوق الملكية الفكرية وقوانين الفضاء الإلكتروني.
- تحرى الضدق والموثوقية والامان في طلب البيانات.
- عدم إشتغلال الحوار عن بعد لغرض التمويه والتنكر وتأجيج نيران الكراهية.

5-3. أمن المعلومات والتشريعات.

إن التشريع بصفة عامة هو مجموع القواعد المكتوبة التي تنضم العلاقات القائمة بين الأطراف المعنية والداخلة فيه ولهذه القواعد القوى الجبرية اللازمة لتنفيده والتقيد به والعقاب في حالة المخالفة ولكي تكون القواعد تشريعا لابد ان تكون مكتوبة حيث يعتبر الدستور في الدول الحديثة هوأعلى مستويات التشريع[141].

بصفة عامة كل مناحي الحياة الإقتصادية و الإجتماعية و السياسية ولحاول المشرع تطوير هذه القواعد من حين لأخر حتى تتماشى مع التطورات الحاصلة في المجتمع وبما أن الجرائم المعلوماتية هي مكن أهم الجرائم التي أفرزتها الثورة المعلوماتية الحالية فإن المشرعين في كافة أنحاء العالم عكفوا على إيجاد تشريعات تهتم بهذه الفئة من الجرائم نظرا للخصوصية التي تكتسيها سواء من حيث طبيعة الفعل أو من حيث مرتكب الجريمة.

5-3-1. تعريف التشريعات الخاصة بالجرائم المعلوماتية:

---

[141]– قنديل ,يوسف. **نحو إستراتجية لدخول النتاج الفكري باللغة العربية**. تونس ؛ الرياض: مكتبة عبد العزيز العامة , 2001.ص. 535.

أطلقت العديد من التسميات على هذه التشريعات منها قوانين جرائم الكمبيوتر, تشريعات الجرائم المعلوماتية وهي توصف بشكل عام بأنها تشريعات حماية أنظمة المعلومات والحماية من استخدامتها الإجرامية وجاءت هذه التشريعات للتصدي لأنشطة إساءة استخدام الكمبيوتر وأنظمة تبادل المعلومات وكذا لمواجهة التحديات في ميدان استخدام الكمبيوتر كوسيلة لإرتكاب الجرائم ؛ وهذه التشريعات هي عبارةعن نصوص قانونية تحدد صور الجرائم والعقوبات إضافة إلى نصوص متعلقة بالمسؤولية الجزائية عند الشروع[142].

ويرجع مبرر هذه التشريعات إلى ماظهر من عجز قوانين العقوبات القائمة عن التطبيق على جرائم الكمبيوتر لأن محل جرائم الكمبيوتر ذو طبيعة معنوية تتمثل في المعلومات في حين أن النصوص القائمة في ميدان السرقة والتدمير والإتلاف تتطلب أن يكون محل الجريمة

ماديا ؛وفي الوقت الحالي تهدف هذه التشريعات إلى تحقيق ثقة عالية قي استخدام شبكات المعلومات في ميدلن أنشطة التجارة والإستمرار الإلكتروني ووصف غرضها العام بتحقيق أمن وحماية المعلومات

5-3-1. التشريعات الخاصة بأمن المعلومات:

إن المعلومات كما يرى العلم البرا يطاني **John naisbitt** هي مورد الإستراتيجي في مجتمع اليوم لا رأس مال فحسب ؛ وإنتاج المعرفة قد أصبح مفتاح الإنتاجية والمنافسة والإنجاز الإقتصادي وعليه كان لابد من وضع التشريعات اللازمة للحفاظ عليها وحمايتها وأهم هذه التشريعات [143]:

1- **التشريعات الخصوصية:** هناك ثلاث نمادج تشريعية لتدابير حماية الخصوصية المعلوماتية وهذه التدابير تعتمد في تطبيقها على إذا ما كان منطق النظام القانوني مجرد الإعتراف بالخصوصية معتمدا على إباحة كل ما يدخل في نطاق الحق ,وتستخدم وسائل لمواجهة الأنشطة التي تمثل الإعتداء على الخصوصية.

2- **القوانين الشاملة** compréhensive laws: في العديد من دول العالم ثمة قوانين عامة تحكم عمليات جمع وإدارة ومعالجة البيانات الشخصية في القطاعين العام و الخاص مع وجود جهة لضمان التواؤم بين القوانين وتطبيقها وهذا هو النموذج الشائع في الدول التي تتبنى حماية البيانات كما هو الحال في دول الإتحاد الأروبي وفي الدول المتعين عليها التوافق مع دليا حماية البيانات الإرشادي الصادر عن الإتحاد الأروبي ولقد وضعت العديد من مثل هذه القوانين في دول خارج الإتحاد الأروبي كما هو الحال في كندا وأسترليا.

3- **القوانين المتخصصة:** وهي التي تتعلق بقطاع معين إذ أن بعض الدول كالولايات المتحدة الامريكية تجنبت سنتشريغ عام للخصوصية وفضلت إصدار قوانين معينة تحكم قطاعات بعينها كما هو الحال بتسجيلات الفيديو والخصوصية المالية وغيرها ؛وفي مثل هذه الحالة فإن إتخاد القواغد القانونية يتحقق من خلال آليات مختلفة وليس كما هو الحال بالنسبة للقانون الشامل والتي تنشأ جهة رقابة عامة , ويأخذ على هذا النموذج أنه

---

[142] – بهاء ,شهين **الأنترنيت والعولنة القاهرة**:عالم الكتب ,1999.ص. 73.

[143] – الجنبيهي ,منير محمد.أمن المعلومات الإلكترونية.المرجع السابق.ص. ص.77-79.

يتطلب جهة أمنية تسن تشريعات جديدة كلما نشأت تقنيات جديدة ولهذا فإن الحماية تظل متخلفة عن تقنيات الاعتداد.

4- لوائح التنظيم الذاتي:

إن مصطلح التنظيم الذاتي **Autoregulation** يعني إنشاء واحترام إرادي للقواعد المتفق عليها في مجال معين دون رقابة.

وموضوع التنظيم الذاتي للتشريعات هو موقف شأن تقنيات المعلومات عموما , وقد ظهرت الحاجة إلى هذا النموذج في حقول التجارة الإلكترونية ومعايير الخدمات الفنية وحماية البيانات وأمن المعلومات وغيرها , وتضمن لوائح التنظيم الذاتي عموما لوائح تنظيم محتوى الأنترنت وكذلك تنظيم التقنيات وأخلاقيات التعامل مع الأنترنت.

5-3-2. قوانين الكمبيوتر[144]:

وأهم هذه القوانين:

1- تشريعات حماية برامج الكمبيوتر:

قوانين الملكية الفكرية في حقل حماية البرمجيات طورت حتى شملت بقية المصنفات الرقمية وقد عكس تطورها الاتجاهات العالمية في إدراج

الملكية الفكرية من تنظيمات التجارة الدولية للتوجه الحاصل نحو الاقتصاد الرقمي والاقتصاد المؤسس على المعرفة ونحو رأس المال الفكري.

2- تشريعات الأصول الإجرائية الجزائية:

هي تشريعات الإثبات المتفقة مع عصر الكمبيوتر والمعلومات التي هي في الحقيقة تطوير لقواعد الإجراءات والإثبات التقليدية واكنها أيضا تتصل عضزيا بالحقوق الجديدة المعترف بها ميدان تقنيات المعلومات

3- تشريعات المحتوى الضار:

ثمة إتجاهين متباينين بين توجه لدمجها مع تشريعات إمكانية المعلومات كما هو في أوروبا أو فصلها عنها كماهو في أمريكا.

4- تشريعات معايير الأمن المعلومات:

وهي تعتير إمتداد لتطور تشريعات المواصفات القياسية لتبادل البيانات والتشفير.

144_ 144_ الجنبيهي ,منير محمد.أمن المعلومات الإلكترونية. المرجع السابق ص.81.

5-3-3. التشريعات المالية الإلكترونية[145]:

1- **تشريعات الإستثمار** : والتجارة والضرائب والجمارك والإتصالات والأظمة الحكومية المتأثرة بتقنية المعلومات.

2- **تشريعات التجارة الإلكترونية:** وتتضمن التوقيع الإلكيروني والتعاقد الإلكتروني والتسوق الإلكتروني.

3- **تشريعات الإختصاص والقانون المطبق على المنازعات القضائية في بيئة المعلومات:**

بشكل خاص منازعات الملكية الفكرية ومنازعات التجارة والأعمال والبنوك الإلكترونية.

إذن وبعد إستعراض أهم القانونية العالمية الصادرة في ما يخص حماية المعلومات ارتأيت أن نستطلع مدى علم طلبة الحقوق في جامعة منتوري قسنطينة على هذه القوانين فكانت النتائج موضحة في الجدول رقم 27 في الصفحة ؟؟؟؟؟؟؟؟؟؟؟

من تحليل نتائج الجدول يتضح لنا أن (60%) من طلبة الحقوق على دراية بالقوانين والتشريعات الدولية المستحدثة لحماية المعلومات، حيث تعتبر الدول الغربية الدول الرائدة في مجال استحداث هذه القوانين والتشريعات وهذا لما شهده هذا العصر من جرائم لا تحصى والتي يكون هدفها المعلومات؛ بينما(40 %) من الطلبة ليسوا على دراية بهذه المستجدات وهذا قد يكون راجع إلى عدم الاهتمام بمثل هذه المواضيع لحداثتها وعدم انتشارها في الدول العربية عمامة والجزائر خاصة.

5-3. الملكية الفكرية للمصنفات الرقمية:

إن تدفق المعلومات وتداولها هي الغاية الجوهرية من وراء شبكة الأنترنت حيث يتم نقل وإرسال المعلومات من مكان إلى آخر وهذه المعلومات هي ملك لأشخاص ونتاج فكرٍ إنساني الذي يجب إحترامه وقد بدأت حماية هذه الأفكارتأخد طابعها القانوني مند القرن الثامن عشر تحت ما يسمى بحقوق الملكية الفكرية ؛والتي تعرف بأنها حقوق دهنية أو حق الملكية الفكرية لتأليف ما.

ونظرا لتطور أوعية المعلومات التي أصبحت تعتمد الوسائل الرقمية كان لزاما على المشرعين والمهتمين بحقوق التأليف تطوير حقوق التأليف لتشمل الأعمال الرقمية قصد مسايرة العصر والوسائل المستجدة وهي قضية تثير جدلا واسعا في اوساط القانونيين والوالناشرين والمكتبيين والمستفيدين.

وب ع ميلاد شبكة المعلومات الدولية المعروفة بالأنترنت ظهرت بعض المشاكل تتعلق بيطبيق حقوق الملكية الفكرية والعلامات الصناعية والتجارية على هذه الشبكة للأسباب التالية [146]:

---

[145]-- الجنبيهي ,منير محمد.أمن المعلومات الإلكترونية. المرجع السابق ص.82.

[146]- منصور ,محمد حسين. **المسؤولية الإلكترونية..الإسكندرية**:دار الجامعة الجديدة ,2003.ص..313.

– تغيير شكل وأسلوب إخراج وعرض المصنفات حيث أصبح الأمر يتعلق الأمر بمنظومة بيانات يتم نشرها علىالأنترنت يتم نشرها ويمكن نسخها وتحويلها بسرعة وسهولة فائقة , ويستطيع ملايين الأشخاص الحصول على نسخة كاملة من المصنف في الحال.

– إن شبكة الأنترنت مفتوحة ومترامية الأطراف تتمتع بحرية إنسياب المعلومات دون ان تحكمها أي سلطة مركزية ومن ثم لا توجد جهة محددة لتفصي عمليات التقليد والنسخ الذي يشكل مساسا بحق المولف , فقد إنتشرت يلك الممارسات وإنتشرت وباتت تشكل خطورة كبيرة خصوصا على الموديلات والماركات.

– أن قانون الملكية الفكرية لايصلح لمواجهة التحديات الجديدة.

المصنفات التي تتمتع بالحماية على الأنترنت:

إن تشريعات حماية حق المؤلف تسري على كل المبتكرات أيا كان موقعها وصورتها , وأيا كانت الاداة التي يتم التعبير عتها من خلالها , ومن تم فهي تحمي كافة صور التعبير عن الأفكار والمعلومات بما في ذلك برامج الحاسبات الآلية وبنوك المعلومات ومن محل الحماية [147]:

– المصنف المكتوب:حيث تتمتع كافة المصنفات المكتوبة بحماية حق المؤلف على الأنترنت , ويدخل في ذلك الكتب والكتيبات والمقالات والنشرات وغيرها من المصنفات المكتوب مثل البريد الإلكتروني وملحقاته.

– المصنفات الموسيقية المسوموعة والمرئية المقترنة بالألفاظ وغير المقترنة والمصنفات السمعية البصرية كالأفلام والمقطوعات الموسيقية المارة بالأنترنت والمودعة عليه.

– الصور التي تمر عبر الأنترنت ومن ثم فإن نشر الصورة إلكترونيا يمثل تعديا على حق المؤلف ويدخل في ذلك الرسم بالخطوط أو الألوان والنحت والطباعةعلى الحجر وعلى الأقمشة ولأية مصنفات مماثلة في مجال الفنون الجميلة والمواصفات الفوتوغرافية ومواصفات الفن التشكيلي والتركيبي

– الصور التوضيحية والخرائط الجغرافية والرسومات التخطيطية والمصنفات الثلاثية الأبعاد المتعلقة بالجغرافيا أو الطبوغرافيا أو التصميمات المعمارية

– المصنفات المشتقة وذلك دون الإخلال بالحماية المقرونة للمصنفات التي شتقت منها والمصنف المشتق هو الذي يستمد أصله من مصنف سابق الوجود كالترجمات والتجميعات بما في ذلك قواعد البيانات وساء في الحاسب أو غيره

– مصنفات العمارة وذلك ببرنامج الحاسب الآلي

---

[147]– منصور ,محمد حسين. المسؤولية الإلكترونية.المرجع السابق.ص.318.

- قواعد البيانات وساء كانت مقروءة من الحاسب الآلي أو من غيره ويكون الكثير من هذه القواعد منشورا على الأنترنت.

المعاهدات والقوانين الخاصة بحماية حق الملكية الفكرية:

تعتبر حماية الملكية الفكرية من أكبر الحقوق التي يتم إنتهاكها يوميا على شبكة الأنترنت وعليه فوجود معاهدات دولية تمنع تلك الإنتهاكات وإصدار كل دولة قوانين خاصة بها أمر ضروري وقد عقدت عدة معاهدات تنص على حماية الملكية نحاول إيجازها فيما يلي:[148]

1- معاهدة برن:

تعتبر هذه المعاهدة والتي تم التوقيع عليها عام 1971 في سويسرا حجر الأساس في مجال الحماية الدولية لحق المؤلف وقد وقعت الإتفاقية 120 دولة ونصت على منح أصحاب المؤلف حق إستشاري في التصريح بعمل نسخ بأي طريقة

2- معاهدة تربس:وتعتبر هذه المعاهدة كذلك من بين المعاهدات التي تم عقدها في مجال حماية الملكية الفكرية من السطو عليها خصوصا بعد إنشار عمليات السطو الإلكتروني وقد تم التوقيع عليها سنة 1994 وقد إهتمت الإتفاقية بالجوانب التجارية التي لها علاقة بالملكية الفكرية

3- معاهدات الوبيو:

وقد ضمت هذه المعاهدات ثلاث مجموعات[149]:

- معاهدة الوبيو بشأن حق المؤلف , معاهدة الوبيو بشأن الآداء والتسجيل الصوتي , معاهدة الوبيو بشأن الحماية الدولية لحق المؤلف والحقوق المجاورة.

- معاهدة الوبيو بشأن حق المؤلف: وقد وقعت هه المعاهدة في ديسمبر 1996 وتتكون من ثمانية عشر مادة , تبدأ بالديباجة ثم تتنارل علاقة تلك المعاهدة بمعاهدة برن ثم تتعرض لنطاق تطبيق الحماية حق المؤلف كحق التوزيع أو الأجير ونقل المصنف والإلتزامات المتعلقة بالتكنولوجيا ومدة الحماية والإستثناءات.

- معاهدة الوبيو بشأن بشأن الآدىء والتسجيل الصوتي: ثم التوقيع غليها في ديسمير 1996 وتقع في أربعة فصول يتناول الفصل الأول علاقة المعاهدة بالمعاهدات الأخرى أما الفصل الثاني فيتناول حقوق فنانوا الآداء معنويا وماديا وحققق الإستنساخ والتوزيع والتأجير.

- معاهدة الوبيو بشأن حقوق المألف والحقوق المجاورة يبدأ بمقدمة ثم تناول الطابع القانوني للمعاهدة وعلاقتها بمعاهدات أخرى ثم إتفاقية جدول الأعمال الرقمي.

---

[148] الجنبيهي منير محمد. جرائم الأنترنت والحاسب الآلي. المرجع السابق. ص 116

[149] المرجع نفسه. ص 119.118.

3 – المكافحة القانونية للجرائم الإلكترونية:

3-1 المعاهدات والمؤتمرات الدولية لمكافحة الجرائم الإلكترونية:

تعد المعاهدات الدولية هي الأساس الذي يرتكز عليه التعاون الدولي في مجال مكافحة الجرائم الإلكترونية وقد تم عقد العديد من المعاهدات التي تعمل على تنسيق التعاون في ما يخص مكافحة الجرائم الإلكترونية ومن تلك المعاهدات:

* معاهدة بودابست**BUODAPEST** لمكافحت جرائم الأنترنت:

شهدت العاصمة المجرية بودابست في أوخر عام 2001 ميلاد أول المعاهدة الدولية التي تكافح جرائم الأنترنت , وتبلورت التعاون الدولي في محابتها ومحاولة الحد منها خاصة

المعاهدات والمؤتمرات الدولية:

تعد المعاهدات الدولية هي الأساس الذي يتركز عليه التعاون الدولي في مجال مكافحة الجرائم الإلكترونية وقد تم عقد العديد من المعاهدات التي تعمل على التعاون الدولي في مجال مكافحة الجرائم الإلكترونية ومن تلك المعاهدات:

– معاهدة بودابست لمكافحة جرائم الأنترنت **Budapest**:

شهدت العاصمة المجرية بودابست في أواخر عام 2001 م أول المعاهدات الدولية التي تكافح جرائم الأنترنت وتبلور التعاون الدولي في محاربتها ومحاولة الحد منها خاصة بعد أن وصلت تلك الجرائم إلى حد خطير حيث أصبحت تهدد الأشخاص والممتلكات وبعد التوقيع على تلك الإتفاقية من مسؤولين في الدول الأروبية إضافة إلى أمريكا واليابان وكندا وجنوب أفريقيا هو نتاج مباثات ومفاوضات إستغرقت ما يزيد عن أربعة أعوام حتى يتم التوصل إلى الصيغة النهائية المناسبة لتلك الإتفاقيات حتى يتم التوقيع عليها من طرف جميع الأطراف دون إعتراض وقد كان الخلاف الوحيد هو مجال محاربة العنصرية ومن المعروف أن هذه الجريمة يعاقب عليها القانون الدولي ولابد من النص في الإتفاقية على لزوم العمل على إزالة تلك المواقع التي على التحريض على الكراهية ومن ضمن الجوانب العديدة التي تناولت تلك الإتفاقيات الإرهاب الإلكتروني وعمليات تزوير بطاقات الإئتمان ودعارة الأطفال وتلك الجرائم تعتبر من أكثر الجرائم إنشارا على المستوى العالمي بصة عامة وأروبا بصفة خاصة وتحدد الإتفاقية أفضل الطرق الواجب إتباعها في التخفيف من جرائم الأنترنت [150]

– المعاهدة الأروبية لمكافحة جرائم الأنترنت:

وقعت اللجنة الخاصة المعنية بقضابا الجريمة بتكليف من المجلس الأروبي علىالمسودة النهائية لمعاهدة شاملة تهدف إلى مساعدة البلدان في مكافحة الجرائم وسط إنقادات من دعاة حماية الحرية الشخصية وبعد أن يتم

[150]– الجنبيهي منير محمد. جرائم الأنترنت والحاسب الآلي ووسائل مكافحتها المرجع السابق. ص.9796.

المصادقة المصادقة عليها من قبل رئاسة المجلس وتوقيعها من البلدان المعنية تستلزم الإتفاقية الدول الموقعة عليها بين الحد الأدنى من القوانين الضرورية للتعامل نع جرائم التقنيةالعالية بما في التحول غير المصرح به ألى الشبكة [151].

3-2 القوانين العالمية لمواجهة جرائم المعلوماتية:

إتجهت كافة الدول المتقدمة تكنولوجيا إلى إستحدات نصوص قانونية جديدة تجرم الجرائم الإلكترونية[152]:

*** على المستوى العالمي:**

تعتبر دولة السويد من أوائل الدول التي إتجهت إلى سن تشريعات قانونية جديدة خاصة بجرائم الأنترنت والحاسب الآلي لتستطيع ان تعاقب المهتتمين بإرتكاب مثل هذه الجرائم ؛ حيث صدر أول قانون خاص ويسمى بقانون البيانات وقد صدر هذا القانون عام 1973 وقد عالج هذا القانون قضايا الإحتلال عن طريق الأنترنت؛ وفي عام 1989 صدر قانون آخريحمل رقم 1213 عرف كافة المصطلحات الضرورية لتطبيق القانون على الجرائم المعلوماتية.

وقد خولت وزارة العدل الأمريكية عام2000 خمس جهات حكومية للتعامل مع جرائم الأنترنت منها مكتب التحقيقات الفدرالية **FBI** .

أما بريطانيا فهي ثالث دولة تسن قانون خاص بها لجرائم الأنترنت والحاسب وهذا عام 1981.

أما فرنسا فقد طورت قولنينها الجنائية للتوافق مع المستجدات الإجرامية حيث أصدرت قانون خاص بها سنة1988 ؛ وقد سارت العديد الطرق على نفس النهج حيث عدلت كل من هولندا وألمانيا وبولندا قوانينها لتتماشى مع هذه الجرائم.

*** على المستوى العربي** [153]:

أما الحال في الدول العربية فإنه وللأسف لا توجد أي دولة عربية قامت بسن قوانين جديدة أو قامت بتحديث قوانينها الخاصة لتستوعب تلك المستجدات الإجرامية فالدول العربية مازالت بعيدة كل البعد عن عن ذلك التطور القانوني الذي يحاول اللحاق بالتطورالإجرامي ؛ أما الأمر في المملكة العربية السعودية فلا توجد نفس المشاكل على أساس أن كافة التشريعات تنطلق من الشريعة الإسلامية وبالتالي فهي لاتحتاج إلى تحديث , فالشريعة الإسلامية صالحة لكل زمان ومكان, وقد إتخدت مدينة الملك عبد العزيز للعلوم والتقنية من خلال وحدة الأنترنت المشرفة على عمل مقدمي خدمة الأنترنت عددا من الإجراءات الفنية التي تهدف إلى محاصرة أعمال المخربين والميسللين ومن بين هذه الإجراءات:

---

[151] المرجع نفسه ص 104 -

[152] - الجنبيهي منير محمد. جرائم الأنترنت والحاسب الآلي ووسائل مكافحتها المرجع السابق.ص. 102.

[153] - الجنبيهي منير محمد. المرجع نفسه. ص.107.

- منع إنتحال أرقام الأنترنت.

- العمل على منع إستءة استخدام البريد الإلكتروني.

3-3 الجهود العربية لمكافحة الجريمة الإلكترونية[154]:

لعل من أبرز ما يمكن أن يقال عن الجهود العربية المبدولة من أجل الحماية من جرائم الحاسب إعتماد مجلس وزراء العدل العرب للقانون العربي الموحد كقانون نمودجي بموجب القرار رقم 229 وبالرجوع إلى المذكرة الإيضاحية لهذا القانون نجد أن الباب السابع الخاص بالجرائم ضد الإشخاص الناتج عن المعالجات المعلوماتية حيث على وجوب حماية الحياة الخاصة الأسرار من أخطار المعالجة الإلكترونية ؛أما المادة 464 فقد نصت على عقابمن يقوم بفعل الدخول بطريقة الغش إلى نظام أوجزء من نظام المعالجة الألية وتعد هذه المحاولة بالرغم من تواضعها من أبرز ما ثم على صعيد تعزيز التعاون على المستوى العربي من الناحية التشريعية

وتكللت الجهود العربية في إطار الحماية الفكرية وحق المؤلف خصوصا في إبرام الإتفاقية العربية لحماية حقوق المؤلف التي أوصى بها مؤتمر الوزراء المسؤولين عن الشؤون الثقافية المنعقد في بغداد عام 1981 ؛ كذلك فإن الجمعية المصرية للقانون الجنائي لها إتجاه محمود في هذا الموضوع وتمثل ذلك في مؤتمرها السادس في القاهرة من 25-28 أكتوبر عام 1993 حول جرائم الكمبيوتر والجرائم الأخرى التي أكد المؤتمرون على عالميتها ووجوب تكاثف الجهود لمكافحتها لأنها تمثل وجها سلبيا للتقدم الحضاري ؛ وقد خرجج المؤتمرون بصور السلوك الإجرامي وتوصيات بضرورة التعاون الدولي في مجال أنظمة المعلومات.

إلى جانب هذه الجهود هناك جهود أخرى تتض ح معالمها في الجهود المتعلقة بالملكية الفكرية كالمؤتمر الدولي الأول للملكية الفكرية سنة 1995 ؛ كما عقد في بغداد مؤتمرين لمستجدات الملكية الفكرية سنة1997 ومن توصيات المؤتمر إنشاء محاكم خاصة للبث في النزاعات المتعلفة بالحماية ؛وبعدها عقد المؤتمر الثاني للملكية الفكرية عام 1998.

وكما سبق الإشارة إليه فإن الجرائم المعلوماتية الحديثة طرحت مشاكل كبيرة من الناحية القضائية وذلك لعدم تناسب القوانين القديمة مع هذه المستجدات ومحاولة لمعرفة إذا ما كان المشرع الجزائري يعاني من مشاكل عند عرض هذا النوع من القضايا على المحاكم وكانت الإجابة كما يوضحه الجدول 28 في الصفحة 148

إذن وحسب نتائج الجدول فإن اغلب الطلبة (66,6%) ليسوا على دراية إن كان المشرع الجزائري يتعرض لمشاكل عند طرح القضايا المعلوماتية على المحاكم ، وهذا راجع إلى قلة هذه القضايا في الجزائر من جهة وعدم محاولة الطلبة التعرف على المستجدات الحاصلة في مصرح الجريمة والتشريعات من جهة أخرى؛ أما (33,3%) يرون أن المشرع الجزائري تعترضه العديد من المشاكل والعراقيل عند الفصل في مثل هذه القضايا

---

[154]- عبابنة , محمود محمد.**جرائم الحاسب وأبعادها الدولية**.عمان:دار الثقافة,2005.ص.180.

أما عن أسباب هذه المشاكل فيرجعها الطلبة إلى الأسباب الموضحة في الجدول رقم 27 (أنظر الصفحة 148)

إذن فإن الطلبة يرون بأن القاضي معرض للمشاكل وعراقيل عند الفصل في قضايا المعلوماتية أما عن مرد هذه المشاكل فهي تقادم النصوص القانونية (60%)، ذلك لأن القوانين والتشريعات الجزائرية تعد قديمة ولا تتماشى مع التطورات الحاصلة على ساحة الجريمة وبالتالي خلق صعوبة تطبيق هذه القوانين على الجرائم التي استحدثتها البيئة الإلكترونية؛ كما يرى (60%) من الطلبة ان سبب هذه المشاكل يرجع إلى عدم تمكن القضاة من التقنيات الحديثة،وهذا راجع إلى حداثة دخول الانترنت إلى الجزائر،ومنه فإن أغلب القضاة لدينا تنقصهم الخبرة والتجربة في ما يتعلق بمثل هذه التقنيات وبالتالي يصعب عليهم الفصل فيها كما أن خصوصية هذه الجرائم تؤدي على خلق عراقيل للقضاة؛والشكل البياني التالي يوضح هذه النسب:

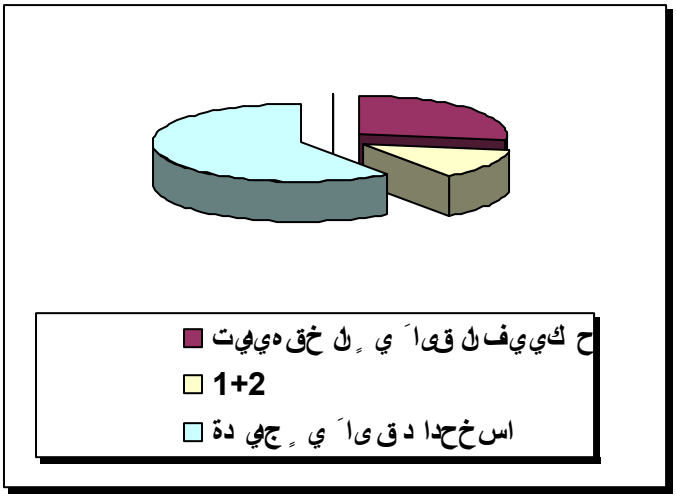
الشكل رقم: 19 أسباب المشاكل التي تعترض القضاة في الفصل في القضايا المعلوماتي

ومن اجل تدارك النقص في التشريعات الجزائرية فيما يخص تشريعات حماية المعلومات ،حاولنا معرفة إذا كانت هناك مساعي لاحتواء مثل هذه الجرائم من خلال سؤال الطلبة وكانت الإجابة كما هي موضحة في الجدول رقم30 الصفحة 149

ومن تحليل نتائج الجدول السابق نلاحظ أن أغلب الطلبة (66,6%) ليسوا على دراية إن كانت هناك مساعي أو مشاريع لاستحداث أو تطوير القوانين أو المراسيم من أجل احتواء ظاهرة الإجرام المعلوماتي، والتي أصبحت بحق جرائم العصر التي تهدد المجتمع الكوني ككل ؛ أما (20%) من عينة الدراسة فقد نفوا وجود أي مساعي لإحداث تغييرات على القوانين في الوقت الراهن إلا أن الغد كفيل بأن تتغير هذه النظرة خصوصا وأن هذه الجرائم في توسع رهيب و لم يسلم منها أحد غي العالم، أما عند محاولة معرفة اقتراحات الطلبة من أجل حل هذه المشكلة كانت الإجابة كما هو موضح غي الجدول رقم 31 الصفحة149

إذن فإن أغلب الطلبة (60%) يرون أن أحسن حل لاحتواء ظاهرة الإجرام المعلوماتي هو استحداث قوانين جديدة وهذا باعتبار أنه الاختيار الأنجع؛ لأن هذه الطاهرة جديدة وتحتاج إلى حلول جذرية تستطيع

الإلمام بكل جوانبها ولا تحتاج إلى حلول مؤقتة أو هامشية؛ أما (26%) من الطلبة فيرون أن تكييف القوانين التقليدية يعتبر كافيا لاحتواء الجرائم الحديثة؛ أما باقي الطلبة فإن الحل بالنسبة لهم هو تعديل وتكييف فالقوانين التقليدية في مواضع معينة واستحداث أخرى في مواضع حيث لا مجال للتعديل وهذا الحل هو الأقرب للصواب والشكل البياني التالي يوضح ذلك:



الشكل رقم:20 اقتراحات الطلبة حول احتواء ظاهرة الإجرام المعلوماتي

مر التشفير بعدة تطورات إلى أن وصل إلى ما هو عليه الآن[155]:

[155]– عبد الحق, ط.**مدخل إلى المعوماتية: برمجيات الحاسب الشخصي. = Logiciel de PC** .البليدة: فصر الكتاب ,2005.ص.327.

- 50- 58 سنة قبل الميلاد: يستخدم الإمبراطور يوليوس قيصر **Jules césar** الرموز المشفرة في رسالته على حاكمه سيسرون **ciceron** في حروبه ضد بلاد الغال وكان يستخدم في ذلك طريقة إستبدال الحروف الأصلية بالحروف التي تليها مباشرة أو تنفيذ عمليات تجعل النص المكتوب غير مفهوم.

- 1499: نشر الراهب الألماني جون ترايمام **Jean Tritheme** أول كتاب خاص بالتشفير يعرض فيه كيفية التشفير.

- 1914- 1918: تطور علم التشفير خلال الحرب العالمية الأولى بشكل كبير وهذا باستخدام تقنيات جديدة تهدف على سرعة الاتصالات العسكرية.

- 1977: تصميم نظام التشفير **RSA** .

- 1997: استخدام مفتاح تشفير بطول 40 بت ثم فك تشفيره من طرف طالب جامعي في عدد من الدقائق.

- 1999: استخدام مفتاح تشفير بطول 512 بت والذي تم فك شفرته من طرف مجموعة من الباحثين بعدة أربعة أشهر.

- 2001الإستخدام الواسع لنظام التشفير **open pgp** من طرف الكثير من العاملين على شبكة الأنترنت بقصد تأمين سرية المعلومات.

3- أنواع التشقير:

التشفير نوعان[156]:

3 -**التشفير المتماثل**: يستخدم فيه المفتاح نفسه للتشفير وكذا لفك الشفرة, وبذلك فإن المفتاح يكون معروفا من طرف كل من مرسل الرسالة ومستقبلها ولا يرسل المفتاح مع الرسالة ولكن يرسل بطرق أخرى حرصا على حماية سرية المفتاح وعدم إطلاع الغير عليه؛ وقد استعملت كتب للأكود **sécure code book** وتتضمن قائمة بمفاتيح التسفير التي يجب أن تستخدم بطرق محددة ؛فعلى سبيل المثال فإن الرسالة التي ترسل يوم الأربعاء يتم استخدام المفتاح **A** يفك شفرتها ,وتفقد كتب الأكواد فيمتها إذا ما تمت سرقتها لأن ذلك يعني كشف المفتاح من قبل الغير.

4 -التشفير غير المتماثل: ويستخدم فيه مفتاحان لكل مستخدم , أحدهما +مفتاح عام معروف من قبل الآخرين حيث يسجله الشخص عادة مع توقيعه على البريد الإلكتروني , في حالة الرغبة في إرسال رسالة مشفرة إلى ذلك الشخص يتم استخدام ذلك المفتاح العام لكتابة الرسالة أما لفكها فيستخدم

---

[156]- بومفلاح, فاتن.المرجع السابق.ص.561.

مفتاح خاص لا يعرفه إلا المستقبل نفسه ؛وغلى الرغم من ارتباط كل نمن المفتاح العام والخاص ببعضهما إلا أن أي منهما لا يدل على الآخر.

وهناك طرق متعددة للتشفير تتراوح في درجة تعقيدها فقد تكون سهلة للغاية لا تتعدى فكرة الاستبدال كما هو الحال في شيفرة قيصر التي تمثل في أبسط صورها إستبدال كل حرف في الأبجدية بحرف آخر وفقا لمفتاح الشيفرة المحدد ,وقد تم تطوير فكرة الاستبدال حتى تصبح أكثر تعقيدا وبالتالي يصبح كسرها أمرا في غاية الصعوبة.

4- أهمية التشفير:

إن أهم الأخطار التي يمكن أن نتغلب عليها بواسطة التشقير هي[157]:

- الإطلاع على المعلومات المحضورة.
- محاولات تعديل البيانات إلى وجهة إخرى
- تأخير محتويات الرسائل المتبادلة.
- تغيير كلمات السر الخاصة بالمستفدين.
- إنتحال شخصية المستخدم الحقيقي.
- تعديل البيانات المخزنة على الحاسب.

5-1-3-3. الجدران النارية:

1- تعريف الجدران النارية:

يخطر في بال معظم الناس عند الحديث عن أمن شبكة الأنترنت برامج جدران النار وعلي الرغم من أن برامج جدران النار لا تعتبر علاجا لجميع مشاكل أمن المعلومات علي شبكة الانترنت، إلا إنها ضرورية لأي إستراتيجية متعبة، في مجال أمن انترنت، تعتبر برمجيات جدران النار ببساطة حاجزا بين شبكتين وهما في اغلب الأحيان شبكة داخلية وتسمي الشبكة الموثقة **trusted network** شبكة خارجية تسمي **entrusted network**وهي شبكة انترنت في هذه الحالة وتقوم برمجيات جدران النار بفحص رزم البيانات القادمة والخارجة اعتمادا علي مجموعة قواعد التي يضعها المشرف علي الشبكة، للسماح لهذه الرزم بالمرور أو يقوم بحجبها ومنعها من الوصول إلي الشبكة الداخلية.

---

[157]- داود ,حسن الطاهر.الحاسب وأمن المعلومات.المرجع السابق.ص.178.

في الأيام الغابرة كانت تقام أسوار حجرية تفصل بين الأبنية والبيوت الخشبية , فتمع في حالة إندلاع حريق امتداد اللهب من بيت لآخر وكانت تسمى بجدران النار , وفي الشبكات الحديثة مثل الأنترنت يمكن اعتماد الطريقة نفسها لحماية مصادر الشبكات الداخلية من الأخطار الناتجة عن ضياع المعلومات الحيوية[158].

ويمكن تعريف الجدار على أنه برنامج **software** أو عتاد **hardware** لحماية موارد الشبكة الداخلية من مستخدمي الشبكات الأخرى , وتستخدم في حالة ارتباط الشبكة بشبكات واسعة وتعمل على منع المستخدمين الخارجيين من الوصول إلى مولد الشبكة وبياناتها الخاصة [159].

إذن فالجدران النارية عبارة عن نظام أو مجموعة أنظمة تفيد تعزيز ضبط الوصول إلى المعلومات بين شبكتين أما الوسائل المعتمدة فمختلفة إنما من حيث المبدأ يمكن تعريفه بأنه عبارة عن آليتين , واحدة تعيق الحركة والأخرى تسمح بها [160].

2- أنواع الجدران النارية:

تستخدم معظم برمجيات جدران النار اليوم طريقة واحدة أو أكثر من الطرق الثلاث المتبعة في فحص الرزم وتستخدم العديد من الموجهات تقنية جدران النار المسماة بترشيح الرزم **packet filtering** والتي تفحص عناوين وبوابات المصدر **Source** والوجهة النهائية **destination** لرزم **TCP** ورزم **UDP** القادمة ثم ترفض أو تسمح للرزم بالمرور وفقا لمجموعة من القواعد مسبقة التحضير وتعتبر تقنية ترشيح الرزم طريقة رخيصة نسبيا وشفافة بالنسبة للمستخدم ولها تأثير طفيف غير ذي بال علي أداء الشبكة ولكن تجهيز تقنية ترشيح الرزم يعتبر عملية معقدة نسبيا ويتطلب معرفة دقيقة بالشبكة وبرتوكولات النقل بل يتطلب في بعض الأحيان معرفة ببروتوكولات التطبيق.

تكمن المشكلة الأخرى في تقنية مرشحات الرزم في أنها عرضة لما يسمي خداع بروتوكول انترنت **IP Spoofing**وهي طريقة يستخدمها الهاكرز ليتمكنوا من الوصول إلى شبكة شركة عن طريق تغيير عناوين بروتوكولات انترنت في ترويسة الرزم إلى عناوين أخرى مقبولة من قبل شركة أخرى

أما النوع الأكثر تقدما وأمنا من أنواع جدران النار فهي برامج بوابات التطبيقات **application gateways**، تستخدم معظم منتجات جدران النار العاملة بتقنيات بوابات التطبيقات بما فيها برامج **eagle**الشهيرة من شركة **Raptor** ما يسمي توكيلات التطبيقات **application proxies** وهي عبارة عن برامج مكتوبة لخدمات معينة من خدمات انترنت (مثل خدمات **HTTP** ، **FTP**وخدمة **telnet**وتعمل علي مزود مرتبط بشبكتين كمزود **Server** لزبون تطبيقات **application client** وكزبون لمزود التطبيقات **application server**

---

[158]- المسفر ,**يوسف.الشبكات المعلوماتية والجدران النارية**.من مجلة علوم وتكنولوجيا.ع53. اتلسنة الخامسة 1996.ص.48.

[159]- بومفلاج , فاتن.**حماية المعلومات في شبكة ام القرى**.مقتطف من كتلب الوقائع.مج 2.الشلرقة ,2001.ص.562.

[160]- المسفر ,يوسف. المرجع السابق.ص.48.

ونظرا لان برامج توكيلات التطبيق تقوم بتقييم رزم الشبكة لتحديد شرعية البيانات المتعلقة بتطبيق معين فإنها تعتبر شكل عام أكثر أمنا من مرشحات الرزم. وتمتاز معظم جدران النار لبوابات التطبيقات باحتوائها علي ميزة تدعي "ترجمة العناوين الشبكة **Network Address Translator** "والتي تمنع ظهور عناوين **IP**الداخلية .أمام المستخدمين من خارج الشبكة الموثقة. تكمن إحدي السلبيات الرئيسية في تقنية بوابات التطبيقات في انخفاض مستوي الأداء بسبب المعالجة المضاعفة التي تتطلبها وظيفة التوكيل **proxy function**وهناك سلبية أخري تكمن في انه قد يتوجب عليك أن تنتظر عدة أشهر حتى تزودك الشركة الصانعة لبرنامج جدران النار بتوكيل التطبيق **application proxy** لأي خدمة جديدة من خدمات انترنت مثل استخدام خدمات **RealAudio.** وإذا كنت تنوي استخدام جدران النار دفاع محيطي خارجي فقط وراء توصيلات **T1** الي مزود خدمة انترنت فلا داعي للقلق علي الأداء، لان عرض الحزمة المنخفض لهذه التوصيلات سيصل إلي حد الإشباع قبل وصول جدران النار الي ذلك الحد. قد تجد الكثير من المؤسسات ضرورة في استخدام جدران النار إضافية علي مستوي شبكاتها الداخلية لفرض حزام امني علي مزودات أقسامها المختلفة مثل مزود المورد البشرية الذي يحتوي عادة علي معلومات حساسة، ويصبح الأداء في هذه الحالة عاملا مهما نظرا لان الربط سيعتمد علي شبكة ايثرنت بسرعة 10 ميجابت/ثانية أو شبكة ايثرنت السريع 100 ميجابت/ثانية .وإذا كنت تنوي استخدام توكيلات التطبيقات داخليا فعليك أن تعتمد علي حل مبني علي عتاد سريع مثل **pix firewall** من شركة **Cisco** أو **firebox** من شركة **Seattle software** أو قد تلجا الي تركيب برمجيات جدران النار علي نظام يتضمن عدة معالجات .

أما النوع الثالث من تكنولوجيا جدران النار والذي أسمته شركة **check point software** باسم تفقد الحالة الكاملة **state full inspection** فهو موجود في برنامج **firewall-1** من شركة نفسها وبرنامج **pix firewall** من شركة سيسكو وبرنامج **On Guard** من شركة **On technology** وبرنامج **firewall/plus** من شركة **network-1** وكما هو الحال في تقنية ترشيح الرزم فان هذه التقنية تستقبل أولا الرزم علي مستوي طبقة الشبكة **Network layer** ثم تقوم بتفحص جميع الرزم ومقارنتها مع نماذج معروفة من الرزم الصديقة وفيما تعطي طريقة تفقد الحالة الكاملة أداء اعلي بقليل من أداء توكيلات التطبيقات إلا أن الجدل يبقي قائما فيما إذا كانت آمنة مثلها أم اقل أمنا منها[161].

3- الوظائف الأساسية للجدران النارية: تتلخص أهم الوظائف التي تؤديها الجدران النارية في [162]:

- منع دخول المستعملين غير المصرح لهم بالدخول إلى الشبكة.
- حماية استخدام الخدمات الهامة عند الدخول إلى الشبكة ومغادرتها.

---

[161]- **أمن الشبكات..**[على الخط المباشر]. زيارة يوم: 2006/03/18 متوفر على الموقع: http://www.jubailnet.com/vb/forumdisplay.php

[162]- حجازي.عبد الفتاح البيومي. الحكومة الإلكترونية.المرجع السابق.ص.60.

- حماية عامة من جميع الهجمات.

وبذلك يمكن لأي شركة أو بنك أو مؤسسة حكومية حماية وتامين المعلومات الخاصة بها من أي مستعمل غير مصرح له بالدخول وهذا يعني أن برمجيات جدران النار تحتو يعلى مجموعة من السياسات التي تجعلها بمثابة مصفاة لمنع الطلبات المشبوهة من الوصول إلى الجهاز الخادم ؛ كما يمكن إعدادها بحث يتم إسقاط ووقف أية طلبات واردة تحاول النفاذ إلى الخادم من منفذ لم يحدد ضمن سياسات هذه البرمجيات , ويمكن لبرنامج الجدار الناري أن يقوم بحماية الشبكة من الفيروسات والحماية من البرمجيات الدخيلة بحسب ما سطر داخل البرمجة.

3- مزايا وعيوب الجدران النارية:

يمكن القول وكما في أية تقنية جديدة أن الجدران النارية لها عيوب ومزايا نلخصها في ما يلي[163]:

1- فيما يخص المزايا:

- توفير الحماية اللازمة للشبكة والمعلومات.

- توفير خدمات تشفير عالية القوة.

- الجدار الناري يتوافق مع جميع الشبكات المفتوحة.

- تخزين المعلومات والعمليات التي تمر من خلاله.

- متابعة المستخدمين للشبكة وكل من يحاول العبث بها.

أما فيما يخص العيوب:

- لا يتعامل الجدار الناري مع البرامج الداخلية التي تهاجم النظام.

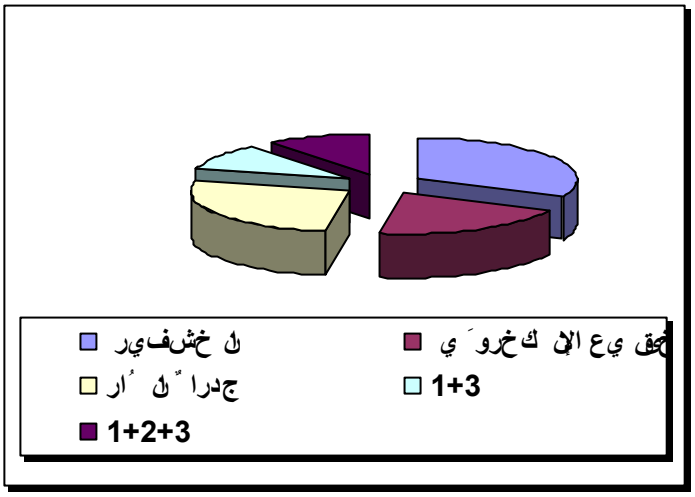
- لا يقدم الحماية للنقل الإذاعي والتلفزيوني.

التشفير ،التوقيع الإلكتروني، جدران النار أهم الطرق المعتمدة لحماية المعلومات وضمان سلامتها أثناء مسارها وعند سؤال الطلبة عن أهم وأنجع الطرق لحمايتها كانت الإجابة كما هي موضحة في الجدول رقم 20 من الصفحة 146

إذن فإن أنجع طرق الحماية حسب الطلبة هو عملية التشفير(31,5 %) والتشفير هو إعادة كتابة البيانات باستعمال أحد مفاتيح التشفير، ثم تليها جدران النار بنسبة (26,3 %) وهو محاولة تصفية البيانات الداخلة إلى الداخلية لمؤسسة ما عن طريق مصفاة يطلق عليها جدران النار، ومع تطور معاملات التجارية وظهور الإقتصاد الشبكي كالتجارة الإلكترونية والتسوق الإلكتروني أدى إلى ظهور وسيلة جديدة هي التوقيع

[163]- حجازي.عبد الفتاح البيومي. الحكومة الإلكترونية.المرجع نفسه.ص. 63.

الإلكتروني والذي يعد وسيلة لا غنى عنها في مثل هذه المعاملات كما يمكن الجمع بين وسيلتين آو أكثر من الوسائل السالفة الذكر وذلك لضمان حماية أكبر وهذا ما نوضحه في الشكل البياني التالي :



الشكل رقم:15 وسائل حماية المعلومات

5-2. أمن المعلومات: الأخلاق (أخلاق التعامل في مجتمع المعلومات)

إن الأخلاق تعد قوة ردعية في المجتمعات لا يستهان بها غي إرشاد وتوجيه سلوكيا ت الناس فما هو الدور الذي تلعبه الأخلاق في مجتمع المعلومات؟

5-2-1. مجتمع المعلومات.

أن مجتمع ما بعد الصناعة هو مجتمع المعلومات وفي مايلي نتطرق إلى اهم عناصر هذا المجتمع الجديد

5-2-1-1. مفهوم مجتمع المعلومات.

لابد في البداية إلى الإشارة أن هناك العديد من التعريفات لمجتمع المعلومات وأن تعريف مجتمع المعلومات لا غير واضح المعالم بشكل عام

إنه مفهوم يرى التحول من مجتمع صناعي إلى مجتمع حيث المعلومات هي القوة الدافعة والمسيطرة وهناك من يرى أنه المجتمع الذي ينشغل معظم أفراده بإنتاج المعلومات أو جمعها أو اختزانها أو معالجتها أو توزيعها [164].
كما يرى البعض بأن مجتمع المعلومات هو المجتمع الذي تستخدم فيه المعلومات بكثافة كوحي للحياة

---

[164]– عبد الهادي ,محمد فتحي.**المعلومات وتكنولوجيا المعلومات على أعتاب قرن جديدة**. القاهرة:الدار العربية للكتاب ,2000.ص.18.

الاقتصادية والاجتماعية والثقافية والسياسية، ويرى الدكتور ناريمان متولي أن مجتمع المعلومات هو المجتمع الذي يعتمد في تطوره بصفة رئيسية على المعلومات الحاسبات الآلية وشبكات الإتصال أي أنه يعتمد على التكنولوجيا الفكرية التي تضم سلع وخدمات جديدة مع التزايد المستمر للقوة العاملة المعلوماتية التي تقوم بإنتاج وتجهيز ومعالجة ونشر وتوزيع وتسويق هذه السلع والخدمات

وقد أدى عدم الاتفاق على مجتمع المعلومات إلى اختلاف الرؤى حوله فقد أشارت دراسة حديثة عن الموضوع إلى ثلاث رؤى لمجتمع المعلومات

الرؤية الأولى: وهي رؤية أوربية يمثلها العالم الاجتماعي(إيان مايلز**Ian miles**) وترتكز على الإنتشار الواسع لتكنولوجيا المعلومات والإتصالات ومالها تأثيرات هي التي تشكل مجتمع المعلومات

الرؤية الثانية: هي رؤية يابانية ويمثلها العالم الاتصالات اليابانية جوهوكا شاكاي **johoka shakia** وهي يرتكر على تدفق أو انسياب المعلومات بكميات هائلة عبر كل الوسائل في المجتمع وترتكز.

الرؤية الثالثة: وهي رؤية أمرقية ويمثلها عالم الإقصاد (فريتز ماكلون) على أن نسبة متزايدة من الناتج القومي الكلي للدولة تجيء من إنتاج المعلومات ، ومن ثم أضافت الإقصاديات الحديثة قطاعا جديدا إلى القطاعات المعروفق[165].

ومن وجهة نظرنا أن لكل هذه الرؤى روافد تصب في نهر واحد ,وان كل واحدة من الرؤى الثلاثة السابقة إما أن تكون سببا لأخرى أو أن تكون حتمية لسابقتها .

إن عصر ما بعد الصناعي أو مجتمع المعلومات كما يطلق عليه هو حصيلة لتراكمات إحتماعية وعلمية وثقافية طيلة سنوات، وقد ساهم غب دخول هذا العصر التطورات التقنية والتكنولوجية التي عرفها العالم المعاصر؛ وتعد الولايات المتحدة الأمريكية وكندا ودول أوروبا من بين الدول السباقة للإنخراط في مجتمع المعلومات الكوني؛ أما دول العالم الثالث بصفة عامة والدول العربية خصوصا فقد خطت خطوت محتشمة للإنضمام لهذا الركب وعند سؤال الطلبة عن ضرورة آو حتمية الإنخراط في مجتمع المعلومات كانت الإجابة كما هي موضحة في الجدول رقم21 من الصفحة 146
إذن وحسب نتائج الجدول فإن الأغلبية الساحقة لعينة الدراسة (97,3 %) ترى أن دخول عالم المعلومات هو ضرورة ملحة تفرضها الظروف المعاشة وهذا من أجل اللحاق بركب الحضارة وعدم الاضمحلال في بوتقة العولمة .

5-2-1-2. خصائص مجتمع المعلومات:

[165]– عبد الهادي ,محمد فتحي. المرجع السابق.ص.18.

يقدر علماء الاقتصاد أن حجم التعاملات المالية التي تتم يوميا عبر الأجهزة والشبكات الإلكترونية للمؤسسات المالية يصل إلى 25بليون دولار , ولعل هذا الرقم العالي يظهر اعتماد المجتمعات في هذا العصر على التجهيزات المنية على تقنيات الحاسب [166] ؛ويمكن تلخيص أهم خصائص التي تطبع مجتمع المعلومات[167]:

1- **انفجار المعرفة:** يرى العديد من لباحثين أن المعلومات المنتجة في الحقبة المعاصرة أكثر أهمية مما أنتج في كل تاريخ البشرية ,كما أنها تتزايد بمعدلات كبيرة نتيجة التطورات التي يشهدها العالم ونتيج ة بروز تخصصات جديدة.

2- **زيادة أهمية المعلومات:** في مجتمع المعلومات ازدادت أهمية المعلومات وأصبحت المعلومة تدخل في كل الأنشطة والصناعات، كما تمثل المادة الخام لقطاعات كثيرة من قطاعات المجتمع المعاصر مشكِلة ما يمكن أن يطلق عليه" صناعة المعلومات " وأصبح ينظر إلى المعلومات كمورد أساسي وإستراتيجي يمكن أن يباع ويشترى.

3- **نمو المجتمعات والمنظمات المعتمدة على المعلومات** :يتميز مجتمع المعلومات كذلك بظهور منظمات تعتمد كليةً على المعلومات مثل مؤسسات الجرائد والأخبار والإستعلامات والبنوك وشركات التأمين....

ويلاحظ أن انفجار أو تضخم هذه المنظمات قد بدأ في الظهور في نفس الوقت الذي شهد بدايات ثورة المعلومات المعاصرة.

4- **تعدد فئات المتعاملين مع المعلومات** : أوجد مجتمع المعلومات فئات كثيرة تتعامل مع البيانات والمعطيات والمعلومات وتشتعل بها منها:

- العلماء والفنانون والمصممين وغيرهم ممن يقدرون على إنتاج وإيجاد معلومة جديدة أو يعيدون تشكيل نماذج معرفية جديدة من واقع المعلومات الحالية.

- العاملون في نقل وتوصيل المعلومة.

- العاملون في تخزين المعلومات كأخصائي المعلومات وأمناء المكتبات ومبرمجي الحاسب.

5- قلة الاعتماد على الورق: حيث تزايدت بصفة مطردة كميات المعلومات المنتجة على وسائط غير ورقية وفي المقابل فإن استعمال الورق أخد يتقلص.

إن العصر الذي نعيشه بكل حيثيات ه هو مجتمع المعلومات هو مجتمع المعلومات بحق؛ فقد غدت المعلومات العصب المحرك لكل مناحي الحياة الاجتماعية والسياسية والثقافية والعلمية، وقد تزايد الاهتمام بالمعلومات مند أن أصبحت تمثل مصدرا أساسيا للدخل القومي للدول المنتجة للمعلومات، وقد ظهرت

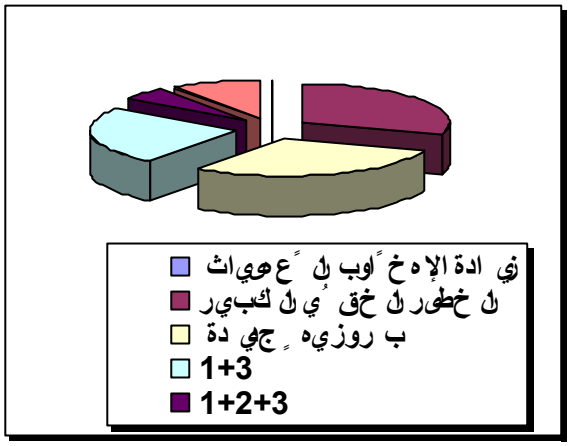
---

[166]- عباس , طاهر محمود.**المكتبات الرقمية وشبكة الأنترنت**.القاهرة: المركز الأصيل ,2003.ص.45.

[167]- لغقاب، محمد. مجتمع **الإعلام والمعلومات:ماهيته وخصائصه**.الجزائر:در هومة ،2003.ص.88.

قطاعات تُعنى بالمعلومات عي كل مراحلها أي مند إنتاجها وإلى غاية نشرها وتوزيعها؛ وقد اتسم مجتمع المعلومات بعدة خصائص نوجزها في الجدول22 من الصفحة 146

إذن فحسب عينة مجتمع الدراسة فإن الخاصيتين اللتان تطبعان مجتمع المعلومات هي زيادة الاهتمام بالمعلومات وكذا التطور التقني المذهل (31,5 %) وهذا ما يؤكده حشد ميزانيات ضخمة والتي تخصصها الدول المتقدمة من أجل تنمية البحوث العلمية وكذلك إنشائها لأكبر مراكز البحوث العلمية والتكنولوجية، إن هذا الاهتمام الكبير بالمعلومات أدى إلى ظهور مهن جديدة كصناعة المعلومات وهذا ما عبرت عنه (26,3 %) من عينة الدراسة، أما باقي الطلبة فيرون أن كل هذه الخصائص السالفة الذكر لها نفس الأهمية في مجتمع المعلومات ،ويمكنا أن نوضح ذلك بشكل أفضل كما يلي:



الشكل رقم:16 خصائص مجتمع المعلومات

3-1-2-5. أبعاد مجتمع المعلومات:[168] :

يصوغ بيل (**Bell, 1973**) فكرة الأركان الإحداثية التي تفسر الأطر الاجتماعية وتدرس تماسك المجتمع من خلال وضع مفهوم يوضح تنظيم المجتمع، فيصنف المجتمع ما بعد الصناعي (مجتمع المعلومات) إلى ثلاثة كيانات: اجتماعية، سياسية، ثقافية. و يشتمل الكيان الاجتماعي على النواحي الاقتصادية والتكنولوجية ونظم العمل، أما الكيان السياسي فهو المعنى بتوزيع السلطات والكيان الثقافي يهتم بالمعاني والرموز.

وفي ضوء هذه الكيانات يرى بيل **Bell** أن في مجتمع المعلومات يحدث التالي:

1- تتغير أدوار الأفراد في المجتمع لبلوغ غايات محددة، ويعتمد على ذلك ظهور أنماط جديدة في السلوك على الأفراد مراعاتها لمواءمة حالة المجتمع الجديد ومثال ذلك انتشار النواحي التخصصية والعوامل المعرفية والتي تتطلب نشاطا مماثلا من الأفراد.

2- تنشأ علاقة تنافسية بين البناء الاجتماعي والكيان السياسي وذلك لأن مجتمع المعلومات قائم على تطور البناء الاجتماعي وظهور الجوانب المعرفية والأهمية المعلوماتية مما يسحب البساط من تحت أرجل النخبة السياسية الحاكمة.

---

[168]- عبد الباري ,**وائل إسماعيل حسن.أسس مجتمع المعلومات العربي قراءة للأبعاد المعرفية والتقنية في المجتمع العصري**.[على الخط المباشر]. زيارة يوم: 2006/03/18 متوفر على الموقع:
http://www.arabcin.net/arabic/5nadwhauthors albari.htm.

3- يعتمد ظهور أنماط جديدة في حياة أفراد المجتمع على درجة المعرفة النظرية والإدراكية **Cognitive Theoretical knowledge** التي ترتبط بجوانب الثقافة المجتمعية، مما قد يؤدى إلى ظهور النزعة الفردية .

وينظر بيل **Bell** إلى مجتمع المعلومات على أن محوره الرئيسي ولب تكوينه يتمثل في عملية المعرفة ويعلل ذلك بالقول أن المعرفة هي الضابط الاجتماعي والموجه لعمليات الإبداع والتجديد والتغيير التي تعمل على نشأة علاقات وهياكل مجتمعية جديدة. ويتمركز مفهوم هذا المجتمع الجديد حول القطاع الاقتصادي والمعنى بالإنتاج والخدمات وتقسيم فئات العمل.

أما الأبعاد المعرفية والتكنولوجية فى مجتمع المعلومات فيرى بيل **Bell** المجتمع ما بعد الصناعي بأنه مجتمع معرفي من خلال بعدين:

أ- تنامي مصادر التجديد والاختراعات القائمة على البحث والتطوير وازدياد العلاقة الوثيقة بين العلم والتكنولوجيا وذلك بسبب مركزية المعرفة النظرية.

ب- كون مؤشرات معدل الناتج القومي ونوع العمل قائمة بصفة كبيرة على الحقل المعرفي، ويتجلى ذلك بوضوح فى طبيعة تقسيم المهن التي تركز على الخدمات المعلوماتية.

5-2-2. أخلاق مجتمع المعلومات.

5-2-2-1. تعريف أخلاق مجتمع المعلومات.

إن مصطلح الأخلاق يتناول المبادئ التي توجه السلوك البشري وهو يتعلق بقضايا الصواب والخطأ ,العدل والظلم ,الصحيح وغير الصحيح وذلك بالنسبة لمجتمع ما أو جماعة معينة[169].

وإذا كانت دراسة الأخلاقيات في مهن المعلومات تعتبر فرعية لدراسة الأخلاقيات بصفة عامة ، فليس هناك اتفاق على تعريف محدد لمصطلح الأخلاقيات فالبعض يستخدم المصطلح بطريقة عامة للدالة على[170]:

- طريقة الحياة التي يرتضيها مجتمع معين.

- مجموعة من القواعد السلوكية التي تضمن تسيير المجتمع نحو الخير والصواب في مواجهة الشر والخطأ.

وكلمة الأخلاق **Ethics** مستخلصة من الجذر اليوناني **Ethos** والذي يعني خَلق؛ وتكون الأخلاق طقما من المعتقدات أو النمطيات أو المثاليات الموجِهة للأفراد.

---

[169]- عبد الهادي ، فتحي. **المعلومات وتكنولوجيا المعلومات على أغتاب قرن جديد.القاهر**ة: مكتبة الدار العربية للكتاب.،2000.ص.37.

[170] -الهوش ،أبو بكرمحمود. **التقنية الحديثة في المعلومات والمكتبات:نحو إستراتيجية عربية لمستقبل مجتمع الملومات**.القاهرة: دار الفجر،2002ص.244.

ويذهب (كلايد كنغ **Clyde king**) إلي أنه يمكن تعريف الأخلاق بأنه نظام من المبادئ الأخلاقية التي تحدد السلوك الصواب والسلوك الخطأ وذلك بالنسبة لمجتمع أو أمة أو جماعة معينة.

وتزداد أهمية الأخلاق في الوقت الحالي أي في مجتمع المعلومات مع تزايد المشكلات الأخلاقية التي يواجهها العالم المعاصر ؛وعندما يذهب الباحثون في الغرب بعيدا في البحث عن أخلاق مجتمع المعلومات فإنهم يبحثون ويدرسون انطلاقا من مجتمعاتهم ومفاهيمهم وتوجهاتهم ؛ وهم يحاولون بذلك ان يحددوا إالأخلاق بما ينفع هذه المجتمعات ويحافظ على تماسكها ؛وأخلاق مجتمع المعلومات لاتختلف عن الأخلاق بصفة عامة وفي الواقع يمكن إيجازها بأنها أخلاق رجل المعلومات وهي مجموعة من المبادئ والقيم التي يجب أن يتخلق بها الشخص في خضم هذا المجتمع وهي تختلف عن القانون لأنها تحدد تصرفات الناس دون إجبار أوإلزام قانوني.

5-2-2-2. أهم المبادئ الأخلاقية في مجتمع المعلومات:

إن الإنسان المعاصر ينظر إلى مجتمع المعلومات على أنه نموذج أخلاقي علمي واجتماعي متقدم ،سيتيح لمجتمعاتنا المخالفة إمكانات أكبر في تبادل المعلومات وتحقيق حرية إنسيابها ،وتحقيق فوائد متوازنة لمختلف المجتمعات وخاصة تلك الاضعف ثقافيا وإقتصاديا وتقنيا ،إلا أن الوقائع تختلف تماما عن النمودج الاخلاقي ويمكن ان نلخص أهم المبادئ والقيم الأخلاقية التي يجب ان تتوفر في مجتمع المعلومات في[171]:

– يشكل تعدد اللغات والثقافات في دائرة المعلومات العالمية ميزة أخلاقية وعلمية وثقافية هامة لابد من المحافظة عليها ضمانا لتنوع وتكامل دائرة المعلومات الدولية وللحفاظ على التراث الثقافي للبشرية ,وحرصا على تطور المشهد الثقافي العالمي.

– تشكل الفجوة الرقمية إحدى اهم المشكلات الأخلاقية التي يواجهه العالم وتتفرع عنها مشكلات أخلاقية وإقتصادية وإجتماعية وعلمية لايمكن للعالم ان يشيح نظره عنها ؛ وإن حل هذه المشكلات يعد الخطوة الأولى الضرورية لبناء مجتمع المعلومات.

– دعم التعاون العالمي في في مجال تبادل المعلومات ليس مسألة نظرية تطرح في المنتديات والمؤتمرات العالمية بل هي مسؤولية أخلاقية جماعية يتوجب على البلدان المتقدمة دعمها من خلال إتاحت المعلومات العلمية وعدم حجبها عن الدول النامية.

– إن مفهوم القرية الكونية يفرض أساسا نشوء مسؤولية إجتماعية جماعية إخلاقية لحل المشكلات التي يعاني منها سكان هذه القرية وأهم المسائل التي يجب الإنتباه لها في مجتنع المعلومات هي:

* الحق في الملكية الفكرية وإحترام أعمال الغير وعدم التعرض لها بأي نوع من أنواع الإعتداد والإستحواد.

---

[171]– **مشروع ميثا الشرف العربي لأخلاق مجتمع المعلومات**.[على الخط المباشر].زيارة يوم:2006/02/16. متوفر على الموقع:
http://www.arabcin.net/arabia3000/arabia1htm.

* الحق في حماية خصوصية الأفراد والمؤسسات وإحترام الحياة الخاصة بهم.

* حرية إكتساب المعلومة.

* مصادقة المعلومة وكيفية التعامل معها في ظل الإنفجار المعرفي.

* كيف يمكن حماية الشبكة من التلوث ومن التخريب فهي شيئ مشترك في مجتمع المعلومات.

5-2-2-3. الإفرازات الأخلاقية الجديدة في مجتمع المعلومات:

من الواضح أن التقنية المتقدمة والوصول إلى المعلومات المتنوعة أو حتى التمكن من هذه المعلومات وإمتلاكها كل هذا لا يجعل من الإنسان المستفيد معلوماتيا أكمل او أكثر صفاء وثراء روحيا ؛ إذا المهم هو مضمون المعلومات وأهدافها الإجتماعية ونوع علاقات الإنسان بها والموشور الذي يتعامل معها من خلاله وهذا ما يحدد الغالم الروحي للإنسان ، بل وغالبا ماتطرح التكنولوجيا المتقدمة ضروريات جديدة تلزم مالكها بالتمتع بأخلاقيات منظبطة إذ أن هناك فرق بين التعامل مع الحواسيب كهدف والتعامل معها كمجرد وسيلة.

لا شك ان إنتسار الحواسيب الشخصية والوسائل الحديثة يمكن أن يقوي الفردية لذى الناس ويضعف الروح الجماعية وكثلفة الإختلاط قي مابينهم لأن تكنولوجيا المعلومات مبنية أساسا على الإستخدام الفري وتحد من الإختلاطات المباشرة ؛ فالرفيق والزميل والصديق يصبح غالبا الآلة أو التجهيزات في حين يصعب التخلي عن معاشرة الناس كقيمة روحية عالية تَلزم الإنسان وترافقه مند الأزمة الغابرة.

إن موجة التكنولوجيا الجديدة تبرز على السطح ضروبا من الإغتراب أو الإستلاب ، ولا سيما ما يسمى بالإغتراب المعرفي ،وأحد جوانب هذا الإغتراب شعور الشخص بالدونية أو النقص إتجاه إمكانيات الآلة المتنامية بإستمرار ؛ ويرى بعض علام النفس أن منطق الآلة الصارم وتعامل الإنسان معه قد يؤدي مع الزمن من الوجهة النفسية على الأقل إلى فقدان حس الإبداع كما أن مايدعم هذه العولة الإجتماعية أو تشارك في وضع واقع تخيلي بديلا للواقع الفعلي هو ألعاب الكمبيوتر والموديلات والنمادج[172].

إن كل هذه الإفرازات السالفة الذكر والتي يتركها الإنخراط في مجتمع المعلومات على السلوكيا ت البشرية تعد من بين سلبيات هذا المجتمع الجديد وعند الإستفسار عن رأي الطلبة حول الموضوع كانت الإجابة بالإجماع على أنه لمجتمع المعلومات إفرازات سلوكية على الأفراد والنتائج كما هو موضح في الجدول رقم 23 في الصفحة 147

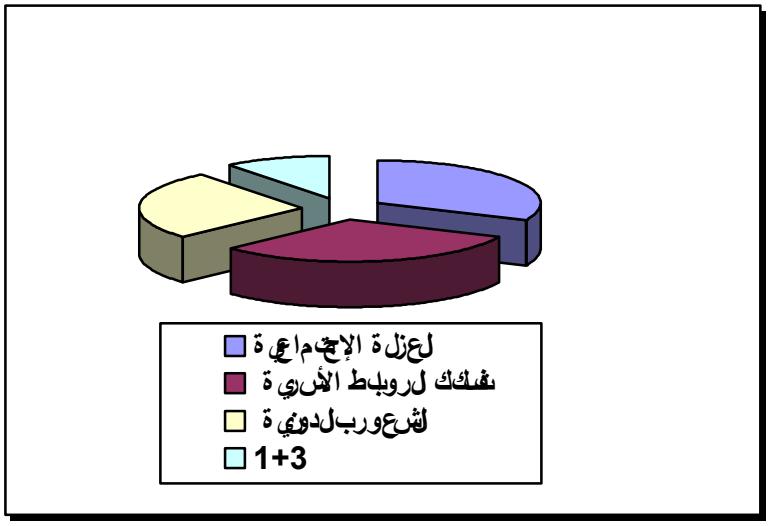
أما عن أهم هذه الإفرازات على السلوك البشري فإنه يمكن أن يتسبب فيخلق عزلة اجتماعية لدى الأفراد كما يمكن أن تساعد في تفكك الروابط الأسرية والاجتماعية داخل المجتمع كما تساهم في خلق نوع من الشعور

---

[172]- النقري،معن.**المعلوماتية والمجتمع / مجتمع ما بعد الصناعة ومجتمع المعلومات**.المغرب؛ لبنان:المردز الثقفي العربي،2001.ص.20.

بالدونية والإنهزامية داخل الفرد هذا أمام إمكانا ت الآلة اللامحدودة والجدول 24 في الصفحة 147 يوضح ذلك

إذن فإن الطلبة يرون أن خلق العزلة الإجتماعية لدى الفرد أهم مشكل يخلقه مجتمع المعلومات بنسبة (31.5 %) وهذه العزلة تنتج من بقاء الفرد لمدة ساعات أمام الآلة مما يجعله يبتعد تدريجيا عن محيطه، إضافة على الطرق المستحدثة غب التعليم كالتعليم عن بعد والذي يفقد الفرد الصديق والأستاذ والزميل وكل هذه العناصر تصبح متوفرة بطريقة إفتراضية؛ كما يؤدي الإنخراط في مجتمع المعلومات إلى تفكك الروابط الأسرية والإجتماعية (31,5 %) وهذا لنفس السبب وهو بقاء الفرد لأرقات طويلة أمام شاشة الحاسب مما يؤدي إلى القضاء على الروابط داخل الأسرة ؛إن هذه الإمكانيات الهائلة للآلة تجعل الإنسان يقف أمامها عاجزا مما يخلق لديه نوع من الإنهزامية والشعور بالدونية أمامها ويمكننا تمثيل هذه النتائج كما يلي:



الشكل رقم 17 الإفرازات الأخلاقية لمجتمع المعلومات

5-2-3. أخلاق الحاسب والانترنت.

لقد أدت الانترنت إلى خلق إفرازات جديدة في العالم منها ما هو سلبي ومنها ما هو إيجابي .

5-2-3-1. الأنترنت: الماهية والخدمات.

1- تعريف الأنترنت:

إن الأصل اللغوي لكلمة شبكة هو الفعل الثلاثي شبك بمعنى تداخل يقال تشبيك الشيء تداخل بعضه في بعض.

في حين تتكون كلمة الأنترنت الإنجليزية الأصل من قسمين **Inter** وهو إختصار لكلمة الدولية **International** والقسم الثاني وهو **net** وهو إختصار **Network** وهذا التعريف اللغوي يقودنا لبيان التعريف العلمي لهذه الشبكة إذا وردت تعاريف متعددة أهما أنه:" إرتباط لأاف من الكمبيوترات في الإتصال مع بعضها البعض وهي شبكة الشبكات تشمل ملايين من المستخدمين يوميا "[173].

وقد مرت شبكة الأنترنت بعدت مراحل إلى أن وصلت إلا ما هي عليه الآن [174]: - بدأت فكرة الأنترنت كفكرة عام 1964 عندما تمكن الباحثون في مؤسسة **Rand comporation** من تقديم مفهوم الشبكة وتحويل مجموع البيانات.

- بدأ التنفيد المادي عام 1969 بإعتبارها بمثابة شبكة من 4 نقاط معتمدة على تحويل مجموع البيانات يطلق عليها **ARPANET**.

- أثناء الثمانينات إلتحقت عدة شبكات منها **BIRNET- CSNET** بالأنترنت

- عام 1984 تم ربط مايزيد عن 1000كمبيوتر بشبكة **ARPANET**.

- 1983 كانت **MILNET** جزء من الأنترنت وكانت تربط بين منظمات عسكرية ومنظمات بحثية وجامعات في المجال العسكري.

- عام 1984 تك إغلاق **ARPANET** رسميا مع إستمرار نقاط الوصل والشبكات الفرعية في آداء عملها.

- عام 1986 قانت مؤسسة العلوم القومية **national science fondation(NSF)** يربط خمسة من شبكاتها المعتمدة على الحاسبات فائقة السرعة والتي أصبحت فيما بعد تعرف بالأنترنت

- عام 1987 تحملت **NSf** المسؤولة عن إدارة هذه الشبكة.

- عام 1989 بلغ عدد المستخدمين 80.000 مستخدم.

- عام 1991 رفعت **Nsfnetr** مقيودها على الأنترنت لأغراض تجارية.

- 1992 ظهرت لأول مرة تطبيقات الإقتصاد الإلكتروني المعتمدة على الانترنت.

- 1997 كان هناك حوالي 16 مليةن مستخدم في كافة أنحاء العالم.

---

[173]- مومني.بشار طلال.مشكلات التعاقد عبر الأنترنت:دراسة مقارنة.الأردن:دار العالم الكتب ,2004.ص.10.

[174]- مرسي, نبيل محمد.التقنيات الحديثة للمعلومات.الإسكندرية:دار الجامعة الجديدة، 2005.ص.181.

- ومن ذلك الوقت وعدد المستخدمين يتزايد يوما بعد يوم والخدمات المقدمة في تطور وأصبحت الأنترنت شبكة عامة محققة للمشاركة ومستقلة.

الانترنت ذلك الفضاء المترامي الأطراف والذي غير مجرى الحياة، وجعل من الحياة أكثر سهولة ويسرًا، فقد فرضت نفسها كمصدر للمعلومات وأداة للاتصال حتى غدت الأداة الأكثر شعبية مند بدأ تواجدها؛ وقد نمت حتى غدت أهم مظاهر التكنولوجيا العالمية، وعند الإستفسار عن استعمال الطلبة لانترنت كانت الإجابة كما هي موضحة في الجدول رقم 25 من الصفحة147

إذن فقد أجاب اغلب الطلبة (94,8 %) على أنهم من مستعملي الأنترنت وذلك لأن عينة الدراسة تشمل طلبة الدراسات العليا،وهذه الفئة لا غنى لها عن الانترنت باعتبارها مصدر هام للمعلومات خصوصا وأغلب الطلبة في إطار تحصير مذكرات تخرجهم مما يجعلهم على إرتيادها.

2- خدمات الانترنت[175]:

1- البريد الإلكتروني: لإرسال وإستقبال الرسائل بسرعة كبيرة.

2- القوايم البريدية:إنشاء وتحديث قوائم العناوين البريدية الخاصة بمجموعلات الأشخاص.

3- خدمة مجموعة الأخبار: وهي شبيهة بخدمة القوائم البريدية إلا إنها تختلف في أن كل عضو يستطيع التحكم في نوع المقالات التي يريدإستلامها.

4- خدمة الأستلام الشخصي:حيث يمكن من خلال هذه الخدمة للإستعلام عن العناوين البريدية لأي شخص أو جهة تستخدم الأنترنت والمسجلين لديها.

5- خدمة المحادثات الشخصية: حيث يمكن التحدث مع الآخر بالصوت والصورة والكتابة.

6- خدمة الدردشة الجماعية:تشبه الخدمة السابقة إلا إنها في الغالب مكن لأي شخص أن يدخل في المحادثة أو يستمع عليها دون إختيار الآخرين.

7- خدمة نقل الملفات: لنقل الملفات من حاسب إلى آخر.

8- خدمة شبكة الإستعلامات الشاملة **Gopher** تفيد في خدمات كثيرة كنقل الملفات والمشاركة في القوائم البريدية.

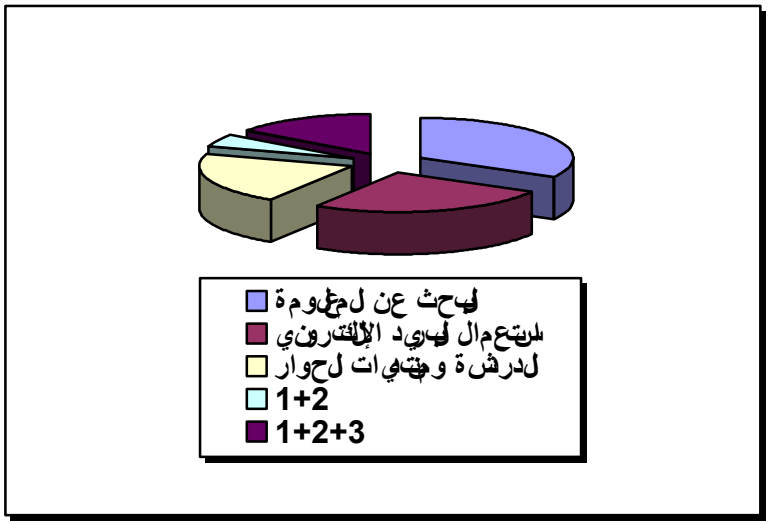
إضافة إلى خدات أخرى كخدمة الدخول عن بعد والصفحة الإعلامية العالمية...إلخ.

---

[175]- الجنبهي، منير محمد.الجنبهي، ممدوح ،منير محمد.الطبيعة القانونية للعقد الإلكتروني.الإسكندرية:دار الفكر الجامعي ،[د.ت.].ص.16-17.

إذن فقد وفرت الانترنت العديد من الخدمات التي ت قدمها لمرتاديها بدأبالبريد الإلكتروني والذي حل العديد من مشاكل وعقبات البريد التقليدي حيث أصبح أكثر سرعة وسهولة، إضافة إلى منتديات الحوار والدردشة ومواقع التسلية،هذا إلى جانب أهم خدمة تقدمها الانترنت على الإطلاق وهي البحث الحر عن المعلومات وعند الإستفسار عن أهم الخدمات المحبذة لدى الطلبة كانت الإجابة كما هي مبينة في الجدول رقم 26 من الصفحة 147

ومن تحليل نتائج الجدول نلاحظ أن أكبر استعمال للانترنت هو لغرض البحث العلمي أي البحث الحر عن المعلومة (31,5%)، وهذا باعتبار الطلبة في الدراسات العليا وهم بصدد الإعداد لمذكرات التخرج،وبالتالي تزداد حاجتهم للمعلومات؛ ثم يليها استعمال البريد الإلكتروني(26,6%)وهي الخدمة الأكثر شعبية لدي جميع الناس وبمختلف الفئات والأعمار وها للمميزات التي تتصف بها هذه الخدمة إضافة إلى مجانية الإرسال؛ ثم تأتي إغراض التسلية والترفيه في المرتبة الموالية (21%)؛ لكن استعمال الأنترنت يشمل عادة جميع هذه الخدمات وهذا حسب الحاجة، والرسم البياني التالي يوضح توزيع هذه الخدمات:



الشكل رقم 18 خدمات الأنترنت

5-2-3-2. مخاطر الأنترنت:

ينتج عن استعمال شبكة الأنترنت مخاطر لا يمكن تداركها فالجرائم التي ترتكب عن طريق الشبكة تسمح للمجرمين بالإقدام على جرائمهم وهم على يقين بأنهم لا يمكن كشفهم وتبقى السرية مضمونة فهي لا تعطي أي دليل حسي وأهم هذه المخاطر[176]:

1-الصور اللاأخلاقية: إن إرسال صور لا أخلاقية عبر الانترنت غير مكلف بحيث يمكن إرسالها بالبريد الإلكتروني من شبكة سرية تتلقى هذه المراكز الرسالة فتلقي عنوان المرسل ثم تقوم بنشرها مرة ثانية وبالتالي يصبح من المستحيل معرفة المصدر الأصاي للرسالة او الصورة.

[176]- مغبغب ،نعيم.**مخاطر المعلوماتية والأنترنت**.لبنان:[د.ن.] 1998.ص.213.

2-الإحتيال: يتم الإحتيال بعدة طرق مثلا يتم عرض بضاعة او صورة إباحية أو غيرها فيطابها أحد المشتركين بالبريد الإلكتروني حيث يطلب منه تحويل ثمنها إلى حساب مصرفي يحدد رقمه في أي مصرف موجود فيقدم طالب البضاعة على إرسال المبلغ حيث يتم سحبها ولا ترسل في المقابل البضاعة أو ترسلة خاطئة أو غير مطلوبة.

التعدي على الحقوق الأدبية والفكرية يمكن بواسطة شبكة الأنترنت بث الأعمال الأدبية والفكرية والأفلام السنمائية للجمهور ويستطيع أي منهم الحصول على نسخة من هذه الأعمال وهذا يشكل تزويرا وتعديا على حقوق المؤلف ، كما يمكن إستعمال شبكة الأنترنت لمارية ألعاب القمار ونشر المعلوملت التي تشكل خطرا كالمعلومات التي تحرض على ارتكاب الجرائم كالتسلح الغير شرعي أو العصيان أو الثورة او الإنتحار وكذاك يمكن إستعمال طالب البضاعة وإستعمال إسمه للقيام بنشطات إجرامية وإستعمال بطاقات الإئتمان بطرق غير فانونية مثل الهبات الخيرية والأرباح الوهمية والإستثمار في الشركات الخاسرة.

5-2-3-3. أخلاقيات الأنترنت[177]:

لقد فتحت الأنترنت أفاقا كبيرة غير مسبةقة في المجالات المختلفة وعلى الأخص في مجالات التعليم والبحث العلمي ونشر الوعي الثقافي وكذا النواحي السياسية والإجتماعية , ولكن ثم إستغلالها في الوقت نفسه من جانب الجماعلت الإجرامية عبر العالم في أغراض أخرى من بينها بث المعلومات المنافية للآداب والمساعدة على العمليات الغرهابية المختلفة.

إن طبيعة الأنترنت التفاعلية واللامركزية على مستوى العالم بالإضافة إلى أهميتها في توفير كم هائل من المحتوى المتاح من وإلى مكان أي مكان قد يؤدي إلى عدد كبير من القضايا القانونية والأخلاقية من بين بينها المحتوى الغير القانوني في الأنترنت.

وتضع معضم دول العالم بعض القيود على نوع المحتوى الذي يعالج ويوزع في نطاق حدودها السياسية الوطنية ، وتعكس هذه القيود المفروضة في أي دولة التقاليد والأعراف الثقافية والقانونية ,بالإضافة إلى القيم الدينية والأخلاقية السائدة فيها وقد تختلف من دولة إلى أخرى.

ويمكن أن نخلص أهم عمليات التعامل مع الأنترنت في:

- إتخاد كافة التدابير الوقائية لحماية أفراد المجتمع وحمايته من البيانات الضارة.
- كفالة أمن البيانات والمعلومات وسريتها ومراعات الخصوصية وإحترامها.
- ضمان أن تكون المعلومات التي تقدمها لرفع مستوى المجتمع الإقتصادي والسياسي والإجتماعي.
- ضمان حماية حقوق الملكية الفكرية وقوانين الفضاء الإلكتروني.

---

[177]- الهوش ،أبو بكر محمود.المرجع السابق.ص.256.

- تحرى الضدق والموثوقية والامان في طلب البيانات.

- عدم إشتغلال الحوار عن بعد لغرض التمويه والتنكر وتأجيج نيران الكراهية.

5-3. أمن المعلومات والتشريعات.

إن التشريع بصفة عامة هو مجموع القواعد المكتوبة التي تنضم العلاقات القائمة بين الأطراف المعنية والداخلة فيه ولهذه القواعد القوى الجبرية اللازمة لتنفيده والتقيد به والعقاب في حالة المخالفة ولكي تكون القواعد تشريعا لابد ان تكون مكتوبة حيث يعتبر الدستور في الدول الحديثة هوأعلى مستويات التشريع[178].

بصفة عامة كل مناحي الحياة الإقتصادية و الإجتماعية و السياسية ولحاول المشرع تطوير هذه القواعد من حين لأخر حتى تتماشى مع التطورات الحاصلة في المجتمع وبما أن الجرائم المعلوماتية هي مكن أهم الجرائم التي أفرزتها الثورة المعلوماتية الحالية فإن المشرعين في كافة أنحاء العالم عكفوا على إيجاد تشريعات تهتم بهذه الفئة من الجرائم نظرا للخصوصية التي تكتسيها سواء من حيث طبيعة الفعل أو من حيث مرتكب الجريمة.

5-3-1. تعريف التشريعات الخاصة بالجرائم المعلوماتية:

أطلقت العديد من التسميات على هذه التشريعات منها قوانين جرائم الكمبيوتر, تشريعات الجرائم المعلوماتية وهي توصف بشكل عام بأنها تشريعات حماية أنظمة المعلومات والحماية من استخدامتها الإجرامية وجاءت هذه التشريعات للتصدي لأنشطة إساءة استخدام الكمبيوتر وأنظمة تبادل المعلومات وكذا لمواجهة التحديات في ميدان استخدام الكمبيوتر كوسيلة لإرتكاب الجرائم ؛ وهذه التشريعات هي عبارةعن نصوص قانونية تحدد صور الجرائم والعقوبات إضافة إلى نصوص متعلقة بالمسؤولية الجزائية عند الشروع[179].

---

[178]– قنديل ,يوسف. **نحو إستراتجية لدخول النتاج الفكري باللغة العربية**. تونس ؛ الرياض: مكتبة عبد العزيز العامة , 2001.ص. 535.

[179] – بهاء ,شهين **الأنترنيت والعولنة القاهرة**:عالم الكتب ,1999.ص. 73.

ويرجع مبرر هذه التشريعات إلى ماظهر من عجز قوانين العقوبات القائمة عن التطبيق على جرائم الكمبيوتر لأن محل جرائم الكمبيوتر ذو طبيعة معنوية تتمثل في المعلومات في حين أن النصوص القائمة في ميدان السرقة والتدمير والإتلاف تتطلب أن يكون محل الجريمة

ماديا ؛وفي الوقت الحالي تهدف هذه التشريعات إلى تحقيق ثقة عالية قي استخدام شبكات المعلومات في ميدلن أنشطة التجارة والإستمرار الإلكتروني ووصف غرضها العام بتحقيق أمن وحماية المعلومات

5-3-1. التشريعات الخاصة بأمن المعلومات:

إن المعلومات كما يرى العلم البرا يطاني **John naisbitt** هي مورد الإستراتيجي في مجتمع اليوم لا رأس مال فحسب ؛ وإنتاج المعرفة قد أصبح مفتاح الإنتاجية والمنافسة والإنجاز الإقتصادي وعليه كان لابد من وضع التشريعات اللازمة للحفاظ عليها وحمايتها وأهم هذه التشريعات [180]:

1- **التشريعات الخصوصية:** هناك ثلاث نمادج تشريعية لتدابير حماية الخصوصية المعلوماتية وهذه التدابير تعتمد في تطبيقها على إذا ما كان منطق النظام القانوني مجرد الإعتراف بالخصوصية معتمدا على إباحة كل ما يدخل في نطاق الحق ,وتستخدم وسائل لمواجهة الأنشطة التي تمثل الإعتداء على الخصوصية.

2- **القوانين الشاملة** compréhensive laws: في العديد من دول العالم ثمة قوانين عامة تحكم عمليات جمع وإدارة ومعالجة البيانات الشخصية في القطاعين العام و الخاص مع وجود جهة لضمان التواؤم بين القوانين وتطبيقها وهذا هو النموذج الشائع في الدول التي تتبنى حماية البيانات كما هو الحال في دول الإتحاد الأروبي وفي الدول المتعين عليها التوافق مع دليا حماية البيانات الإرشادي الصادر عن الإتحاد الأروبي ولقد وضعت العديد من مثل هذه القوانين في دول خارج الإتحاد الأروبي كما هو الحال في كندا وأسترليا.

3- **القوانين المتخصصة:** وهي التي تتعلق بقطاع معين إذ أن بعض الدول كالولايات المتحدة الامريكية تجنبت سنتشريغ عام للخصوصية وفضلت إصدار قوانين معينة تحكم قطاعات بعينها كما هو الحال بتسجيلات الفيديو والخصوصية المالية وغيرها ؛وفي مثل هذه الحالة فإن إتخاد القواغد القانونية يتحقق من خلال آليات مختلفة وليس كما هو الحال بالنسبة للقانون الشامل والتي تنشأ جهة رقابة عامة , ويأخذ على هذا النموذج أنه يتطلب جهة أمنية تسن تشريعات جديدة كلما نشأت تقنيات جديدة ولهذا فإن الحماية تظل متخلفة عن تقنيات الاعتداد.

4- **لوائح التنظيم الذاتي:**

إن مصطلح التنظيم الذاتي **Autoregulation** يعني إنشاء واحترام إرادي للقواعد المتفق عليها في مجال معين دون رقابة.

---

[180]- الجنبيهي ,منير محمد.أمن المعلومات الإلكترونية.المرجع السابق.ص. ص.77-79.

وموضوع التنظيم الذاتي للتشريعات هو موقف شأن تقنيات المعلومات عموما , وقد ظهرت الحاجة إلى هذا النموذج في حقول التجارة الإلكترونية ومعايير الخدمات الفنية وحماية البيانات وأمن المعلومات وغيرها , وتضمن لوائح التنظيم الذاتي عموما لوائح تنظيم محتوى الأنترنت وكذلك تنظيم التقنيات وأخلاقيات التعامل مع الأنترنت.

5-3-2. قوانين الكمبيوتر[181]:

وأهم هذه القوانين:

1- تشريعات حماية برامج الكمبيوتر:

قوانين الملكية الفكرية في حقل حماية البرمجيات طورت حتى شملت بقية المصنفات الرقمية وقد عكس تطورها الاتجاهات العالمية في إدراج

الملكية الفكرية من تنظيمات التجارة الدولية للتوجه الحاصل نحو الاقتصاد الرقمي والاقتصاد المؤسس على المعرفة ونحو رأس المال الفكري.

2- تشريعات الأصول الإجرائية الجزائية:

هي تشريعات الإثبات المتفقة مع عصر الكمبيوتر والمعلومات التي هي في الحقيقة تطوير لقواعد الإجراءات والإثبات التقليدية واكنها أيضا تتصل عضزيا بالحقوق الجديدة المعترف بها ميدان تقنيات المعلومات

3- تشريعات المحتوى الضار:

ثمة إتجاهين متباينين بين توجه لدمجها مع تشريعات إمكانية المعلومات كما هو في أوروبا أو فصلها عنها كماهو في أمريكا.

4- تشريعات معايير الأمن المعلومات:

وهي تعتير إمتداد لتطور تشريعات المواصفات القياسية لتبادل البيانات والتشفير.

5-3-3. التشريعات المالية الإلكترونية[182]:

1- تشريعات الإستثمار : والتجارة والضرائب والجمارك والإتصالات والأظمة الحكومية المتأثرة بتقنية المعلومات.

2- تشريعات التجارة الإلكترونية: وتتضمن التوقيع الإلكيروني والتعاقد الإلكتروني والتسوق الإلكتروني.

---

[181]_ [181]- الجنبيهي ,منير محمد.أمن المعلومات الإلكترونية. المرجع السابق ص.81.

[182]-- الجنبيهي ,منير محمد.أمن المعلومات الإلكترونية. المرجع السابق ص.82.

3- تشريعات الإختصاص والقانون المطبق على المنازعات القضائية في بيئة المعلومات:

بشكل خاص منازعات الملكية الفكرية ومنازعات التجارة والأعمال والبنوك الإلكترونية.

إذن وبعد إستعراض أهم القانونية العالمية الصادرة في ما يخص حماية المعلومات ارتأيت أن نستطلع مدى علم طلبة الحقوق في جامعة منتوري قسنطينة على هذه القوانين فكانت النتائج موضحة في الجدول رقم 27 في الصفحة ؟؟؟؟؟؟؟؟؟؟؟؟

من تحليل نتائج الجدول يتضح لنا أن (60%) من طلبة الحقوق على دراية بالقوانين والتشريعات الدولية المستحدثة لحماية المعلومات، حيث تعتبر الدول الغربية الدول الرائدة في مجال استحداث هذه القوانين والتشريعات وهذا لما شهده هذا العصر من جرائم لا تحصى والتي يكون هدفها المعلومات؛ بينما(40 %) من الطلبة ليسوا على دراية بهذه المستجدات وهذا قد يكون راجع إلى عدم الاهتمام بمثل هذه المواضيع لحداثتها وعدم انتشارها في الدول العربية عمامة والجزائر خاصة.

3-5. الملكية الفكرية للمصنفات الرقمية:

إن تدفق المعلومات وتداولها هي الغاية الجوهرية من وراء شبكة الأنترنت حيث يتم نقل وإرسال المعلومات من مكان إلى آخر وهذه المعلومات هي ملك لأشخاص ونتاج فكرٍ إنساني الذي يجب إحترامه وقد بدأت حماية هذه الأفكارتأخد طابعها القانوني مند القرن الثامن عشر تحت ما يسمى بحقوق الملكية الفكرية ؛والتي تعرف بأنها حقوق دهنية أو حق الملكية الفكرية لتأليف ما.

ونظرا لتطور أوعية المعلومات التي أصبحت تعتمد الوسائل الرقمية كان لزاما على المشرعين والمهتمين بحقوق التأليف تطوير حقوق التأليف لتشمل الأعمال الرقمية قصد مسايرة العصر والوسائل المستجدة وهي قضية تثير جدلا واسعا في اوساط القانونيين والوالناشرين والمكتبيين والمستفيدين.

وب ع ميلاد شبكة المعلومات الدولية المعروفة بالأنترنت ظهرت بعض المشاكل تتعلق بيطبيق حقوق الملكية الفكرية والعلامات الصناعية والتجارية على هذه الشبكة للأسباب التالية [183]:

- تغيير شكل وأسلوب إخراج وعرض المصنفات حيث أصبح الأمر يتعلق الأمر بمنظومة بيانات يتم نشرها علىالأنترنت يتم نشرها ويمكن نسخها وتحويلها بسرعة وسهولة فائقة , ويستطيع ملايين الأشخاص الحصول على نسخة كاملة من المصنف في الحال.

- إن شبكة الأنترنت مفتوحة ومترامية الأطراف تتمتع بحرية إنسياب المعلومات دون ان تحكمها أي سلطة مركزية ومن ثم لا توجد جهة محددة لتفصي عمليات التقليد والنسخ الذي يشكل مساسا بحق المولف , فقد إنتشرت يلك الممارسات وإنتشرت وباتت تشكل خطورة كبيرة خصوصا على الموديلات والماركات.

[183]- منصور ,محمد حسين. **المسؤولية الإلكترونية..الإسكندرية**:دار الجامعة الجديدة ,2003.ص..313.

- أن قانون الملكية الفكرية لايصلح لمواجهة التحديات الجديدة.

المصنفات التي تتمتع بالحماية على الأنترنت:

إن تشريعات حماية حق المؤلف تسري على كل المبتكرات أيا كان موقعها وصورتها , وأيا كانت الاداة التي يتم التعبير عتها من خلالها , ومن تم فهي تحمي كافة صور التعبير عن الأفكار والمعلومات بما في ذلك برامج الحاسبات الآلية وبنوك المعلومات ومن محل الحماية [184]:

- المصنف المكتوب:حيث تتمتع كافة المصنفات المكتوبة بحماية حق المؤلف على الأنترنت , ويدخل في ذلك الكتب والكتيبات والمقالات والنشرات وغيرها من المصنفات المكتوب مثل البريد الإلكتروني وملحقاته.

- المصنفات الموسيقية المسوموعة والمرئية المقترنة بالألفاظ وغير المقترنة والمصنفات السمعية البصرية كالأفلام والمقطوعات الموسيقية المارة بالأنترنت والمودعة عليه.

- الصور التي تمر عبر الأنترنت ومن ثم فإن نشر الصورة إلكترونيا يمثل تعديا على حق المؤلف ويدخل في ذلك الرسم بالخطوط أو الألوان والنحت والطباعةعلى الحجر وعلى الأقمشة ولأية مصنفات مماثلة في مجال الفنون الجميلة والمواصفات الفوتوغرافية ومواصفات الفن التشكيلي والتركيبي

- الصور التوضيحية والخرائط الجغرافية والرسومات التخطيطية والمصنفات الثلاثية الأبعاد المتعلقة بالجغرافيا أو الطبوغرافيا أو التصميمات المعمارية

- المصنفات المشتقة وذلك دون الإخلال بالحماية المقرونة للمصنفات التي شتقت منها والمصنف المشتق هو الذي يستمد أصله من مصنف سابق الوجود كالترجمات والتجميعات بما في ذلك قواعد البيانات وساء في الحاسب أو غيره

- مصنفات العمارة وذلك ببرنامج الحاسب الآلي

- قواعد البيانات وساء كانت مقروءة من الحاسب الآلي أو من غيره ويكون الكثير من هذه القواعد منشورا على الأنترنت.

المعاهدات والقوانين الخاصة بحماية حق الملكية الفكرية:

تعتبر حماية الملكية الفكرية من أكبر الحقوق التي يتم إنتهاكها يوميا على شبكة الأنترنت وعليه فوجود معاهدات دولية تمنع تلك الإنتهاكات وإصدار كل دولة قوانين خاصة بها أمر ضروري وقد عقدت عدة معاهدات تنص على حماية الملكية نحاول إيجازها فيما يلي: [185]

---

[184]- منصور ,محمد حسين. المسؤولية الإلكترونية.المرجع السابق.ص.318.

[185]الجنبيهي منير محمد. جرائم الأنترنت والحاسب الآلي. المرجع السابق. ص 116

1- معاهدة برن:

تعتبر هذه المعاهدة والتي تم التوقيع عليها عام 1971 في سويسرا حجر الأساس في مجال الحماية الدولية لحق المؤلف وقد وقعت الإتفاقية 120 دولة ونصت على منح أصحاب المؤلف حق إستشاري في التصريح بعمل نسخ بأي طريقة

2- معاهدة تربس:وتعتبر هذه المعاهدة كذلك من بين المعاهدات التي تم عقدها في مجال حماية الملكية الفكرية من السطو عليها خصوصا بعد إنشار عمليات السطو الإلكتروني وقد تم التوقيع عليها سنة 1994 وقد إهتمت الإتفاقية بالجوانب التجارية التي لها علاقة بالملكية الفكرية

3- معاهدات الوبيو:

وقد ضمت هذه المعاهدات ثلاث مجموعات [186]:

- معاهدة الوبيو بشأن حق المؤلف , معاهدة الوبيو بشأن الآداء والتسجيل الصوتي , معاهدة الوبيو بشأن الحماية الدولية لحق المؤلف والحقوق المجاورة.

- معاهدة الوبيو بشأن حق المؤلف: وقد وقعت هه المعاهدة في ديسمبر 1996 وتتكون من ثمانية عشر مادة , تبدأ بالديباجة ثم تتنارل علاقة تلك المعاهدة بمعاهدة برن ثم تتعرض لنطاق تطبيق الحماية حق المؤلف كحق التوزيع أو الأجير ونقل المصنف والإلتزامات المتعلقة بالتكنولوجيا ومدة الحماية والإستثناءات.

- معاهدة الوبيو بشأن بشأن الآدىء والتسجيل الصوتي: ثم التوقيع غليها في ديس مير 1996 وتقع في أربعة فصول يتناول الفصل الأول علاقة المعاهدة بالمعاهدات الأخرى أما الفصل الثاني فيتناول حقوق فنانوا الآداء معنويا وماديا وحقةق الإستنساخ والتوزيع والتأجير.

- معاهدة الوبيو بشأن حقوق المألف والحقوق المجاورة يبدأ بمقدمة ثم تناول الطابع القانوني للمعاهدة وعلاقتها بمعاهدات أخرى ثم إتفاقية جدول الأعمال الرقمي.

3 – لالمكافحة القانونية للجرائم الإلكترونية:

3-1 لالمعاهدات والمؤتمرات الدولي لمكافحة لجرائم الإلكترونية:

تعد المعاهدات الدولية هي الأساس الذي يرتكز عليه التعاون الدولي في مجال مكافحة الجرائم الإلكترونية وقد تم عقد العديد من المعاهدات التي تعمل على تنسيق التعاون في ما يخص مكافحة الجرائم الإلكترونية ومن تلك المعاهدات:

* معاهدة بودابستBUODAPESTلمكافحت جرائم الأنترنت:

---

[186] المرجع نفسه. ص 119.118.

شهدت العاصمة المجرية بودابست في أوخر عام 2001 ميلاد أول المعاهدة الدولية التي تكافح جرائم الأنترنت , وتبلورت التعاون الدولي في محابتها ومحاولة الحد منها خاصة

المعاهدات والمؤتمرات الدولية

تعد المعاهدات الدولية هي الأساس الذي يتركز عليه التعاون الدولي في مجال مكافحة الجرائم الإلكترونية وقد تم عقد العديد من المعاهدات التي تعمل على التعاون الدولي في مجال مكافحة الجرائم الإلكترونية ومن تلك المعاهدات:

- معاهدة بودابست لمكافحة جرائم الأنترنت **Budapest:**

شهدت العاصمة المجرية بودابست في أواخر عام 2001 م أول المعاهدات الدولية التي تكافح جرائم الأنترنت وتبلور التعاون الدولي في محاربتها ومحاولة الحد منها خاصة بعد أن وصلت تلك الجرائم إلى حد خطير حيث أصبحت تهدد الأشخاص والممتلكات وبعد التوقيع على تلك الإتفاقية من مسؤولين في الدول الأروبية إضافة إلى أمريكا واليابان وكندا وجنوب أفريقيا هو نتاج مباثات ومفاوضات إستغرقت ما يزيد عن أربعة أعوام حتى يتم التوصل إلى الصيغة النهائية المناسبة لتلك الإتفاقيات حتى يتم التوقيع عليها من طرف جميع الأطراف دون إعتراض وقد كان الخلاف الوحيد هو مجال محاربة العنصرية ومن المعروف أن هذه الجريمة يعاقب عليها القانون الدولي ولابد من النص في الإتفاقية على لزوم العمل على إزالة تلك المواقع التي على التحريض على الكراهية ومن ضمن الجوانب العديدة التي تناولت تلك الإتفاقيات الإرهاب الإلكتروني وعمليات تزوير بطاقات الإئتمان ودعارة الأطفال وتلك الجرائم تعتبر من أكثر الجرائم إنشارا على المستوى العالمي بصة عامة وأروبا بصفة خاصة وتحدد الإتفاقية أفضل الطرق الواجب إتباعها في التخفيف من جرائم الأنترنت [187]

- المعاهدة الأروبية لمكافحة جرائم الأنترنت:

وقعت اللجنة الخاصة المعنية بقضابا الجريمة بتكليف من المجلس الأروبي علىالمسودة النهائية لمعاهدة شاملة تهدف إلى مساعدة البلدان في مكافحة الجرائم وسط إنقادات من دعاة حماية الحرية الشخصية وبعد أن يتم المصادقة المصادقة عليها من قبل رئاسة المجلس وتوقيعها من البلدان المعنية تستلزم الإتفاقية الدول الموقعة عليها بين الحد الأدنى من القوانين الضرورية للتعامل نع جرائم التقنيةالعالية بما في التحول غير المصرح به ألى الشبكة [188].

3-الجهود الدولية لمواجهة جرائم المعلوماتية

---

[187]- الجنبيهي منير محمد. جرائم الأنترنت والحاسب الآلي ووسائل مكافحتها المرجع السابق. ص. 9796.

[188]المرجع نفسه ص 104 -

إتجهت كافة الدول المتقدمة تكنولوجيا إلى إستحدات نصوص قانونية جديدة تجرم الجرائم الإلكترونية[189]:

*** على المستوى العالمي:**

تعتبر دولة السويد من أوائل الدول التي إتجهت إلى سن تشريعات قانونية جديدة خاصة بجرائم الأنترنت والحاسب الآلي لتستطيع ان تعاقب المهتتمين بإرتكاب مثل هذه الجرائم ؛ حيث صدر أول قانون خاص ويسمى بقانون البيانات وقد صدر هذا القانون عام 1973 وقد عالج هذا القانون قضايا الإحتلال عن طريق الأنترنت؛ وفي عام 1989 صدر قانون آخريحمل رقم 1213 عرف كافة المصطلحات الضرورية لتطبيق القانون على الجرائم المعلوماتية.

وقد خولت وزارة العدل الأمريكية عام2000 خمس جهات حكومية للتعامل مع جرائم الأنترنت منها مكتب التحقيقات الفدرالية **FBI** .

أما بريطانيا فهي ثالث دولة تسن قانون خاص بها لجرائم الأنترنت والحاسب وهذا عام1981.

أما فرنسا فقد طورت قولنينها الجنائية للتوافق مع المستجدات الإجرامية حيث أصدرت قانون خاص بها سنة1988 ؛ وقد سارت العديد الطرق على نفس النهج حيث عدلت كل من هولندا وألمانيا وبولندا قوانينها لتتماشى مع هذه الجرائم.

*** على المستوى العربي** [190]:

أما الحال في الدول العربية فإنه وللأسف لا توجد أي دولة عربية قامت بسن قوانين جديدة أو قامت بتحديث قوانينها الخاصة لتستوعب تلك المستجدات الإجرامية فالدول العربية مازالت بعيدة كل البعد عن عن ذلك التطور القانوني الذي يحاول اللحاق بالتطورالإجرامي ؛ أما الأمر في المملكة العربية السعودية فلا توجد نفس المشاكل على أساس أن كافة التشريعات تنطلق من الشريعة الإسلامية وبالتالي فهي لاتحتاج إلى تحديث , فالشريعة الإسلامية صالحة لكل زمان ومكان, وقد إتخدت مدينة الملك عبد العزيز للعلوم والتقنية من خلال وحدة الأنترنت المشرفة على عمل مقدمي خدمة الأنترنت عددا من الإجراءات الفنية التي تهدف إلى محاصرة أعمال المخربين والميسللين ومن بين هذه الإجراءات:

- منع إنتحال أرقام الأنترنت.

- العمل على منع إستءة استخدام البريد الإلكتروني.

---

[189]– الجنبيهي منير محمد. جرائم الأنترنت والحاسب الآلي ووسائل مكافحتها المرجع السابق.ص. 102.

[190]– الجنبيهي منير محمد. المرجع نفسه. ص.107.

3-3 الجهود العربية لمكافحة الجريمة الإلكترونية [191]:

لعل من أبرز ما يمكن أن يقال عن الجهود العربية المبدولة من أجل الحماية من جرائم الحاسب إعتماد مجلس وزراء العدل العرب للقانون العربي الموحد كقانون نموذجي بموجب القرار رقم 229 وبالرجوع إلى المذكرة الإيضاحية لهذا القانون نجد أن الباب السابع الخاص بالجرائم ضد الإشخاص الناتج عن المعالجات المعلوماتية حيث على وجوب حماية الحياة الخاصة الأسرار من أخطار المعالجة الإلكترونية ؛أما المادة 464 فقد نصت على عقابمن يقوم بفعل الدخول بطريقة الغش إلى نظام أوجزء من نظام المعالجة الألية وتعد هذه المحاولة بالرغم من تواضعها من أبرز ما ثم على صعيد تعزيز التعاون على المستوى العربي من الناحية التشريعية

وتكللت الجهود العربية في إطار الحماية الفكرية وحق المؤلف خصوصا في إبرام الإتفاقية العربية لحماية حقوق المؤلف التي أوصى بها مؤتمر الوزراء المسؤولين عن الشؤون الثقافية المنعقد في بغداد عام 1981 ؛ كذلك فإن الجمعية المصرية للقانون الجنائي لها إتجاه محمود في هذا الموضوع وتمثل ذلك في مؤتمرها السادس في القاهرة من 25-28 أكتوبر عام 1993 حول جرائم الكمبيوتر والجرائم الأخرى التي أكد المؤتمرون على عالميتها ووجوب تكاثف الجهود لمكافحتها لأنها تمثل وجها سلبيا للتقدم الحضاري ؛ وقد خرجج المؤتمرون بصور السلوك الإجرامي وتوصيات بضرورة التعاون الدولي في مجال أنظمة المعلومات.

إلى جانب هذه الجهود هناك جهود أخرى تتض ح معالمها في الجهود المتعلقة بالملكية الفكرية كالمؤتمر الدولي الأول للملكية الفكرية سنة 1995 ؛ كما عقد في بغداد مؤتمرين لمستجدات الملكية الفكرية سنة 1997 ومن توصيات المؤتمر إنشاء محاكم خاصة للبث في النزاعات المتعلقة بالحماية ؛وبعدها عقد المؤتمر الثاني للملكية الفكرية عام 1998.

وكما سبق الإشارة إليه فإن الجرائم المعلوماتية الحديثة طرحت مشاكل كبيرة من الناحية القضائية وذلك لعدم تناسب القوانين القديمة مع هذه المستجدات ومحاولة لمعرفة إذا ما كان المشرع الجزائري يعاني من مشاكل عند عرض هذا النوع من القضايا على المحاكم وكانت الإجابة كما يوضحه الجدول 28 في الصفحة 148

إذن وحسب نتائج الجدول فإن اغلب الطلبة (66,6%) ليسوا على دراية إن كان المشرع الجزائري يتعرض لمشاكل عند طرح القضايا المعلوماتية على المحاكم ، وهذا راجع إلى قلة هذه القضايا في الجزائر من جهة وعدم محاولة الطلبة التعرف على المستجدات الحاصلة في مصرح الجريمة والتشريعات من جهة أخرى؛ أما (33,3%) يرون أن المشرع الجزائري تعترضه العديد

---

[191]- عبابنة , محمود محمد.**جرائم الحاسب وأبعادها الدولية**.عمان:دار الثقافة,2005.ص.180.

من المشاكل والعراقيل عند الفصل في مثل هذه القضايا أما عن أسباب هذه المشاكل فيرجعها الطلبة إلى الأسباب الموضحة في الجدول رقم 27 (أنظر الصفحة 148)

إذن فإن الطلبة يرون بأن القاضي معرض للمشاكل وعراقيل عند الفصل في قضايا المعلوماتية أما عن مرد هذه المشاكل فهي تقادم النصوص القانونية (60%)، ذلك لأن القوانين والتشريعات الجزائرية تعد قديمة ولا تتماشى مع التطورات الحاصلة على ساحة الجريمة وبالتالي خلق صعوبة تطبيق هذه القوانين على الجرائم التي استحدثتها البيئة الإلكترونية؛ كما يرى (60%) من الطلبة ان سبب هذه المشاكل يرجع إلى عدم تمكن القضاة من التقنيات الحديثة،وهذا راجع إلى حداثة دخول الانترنت إلى الجزائر،ومنه فإن أغلب القضاة لدينا تنقصهم الخبرة والتجربة في ما يتعلق بمثل هذه التقنيات وبالتالي يصعب عليهم الفصل فيها كما أن خصوصية هذه الجرائم تؤدي على خلق عراقيل للقضاة؛والشكل البياني التالي يوضح هذه النسب:

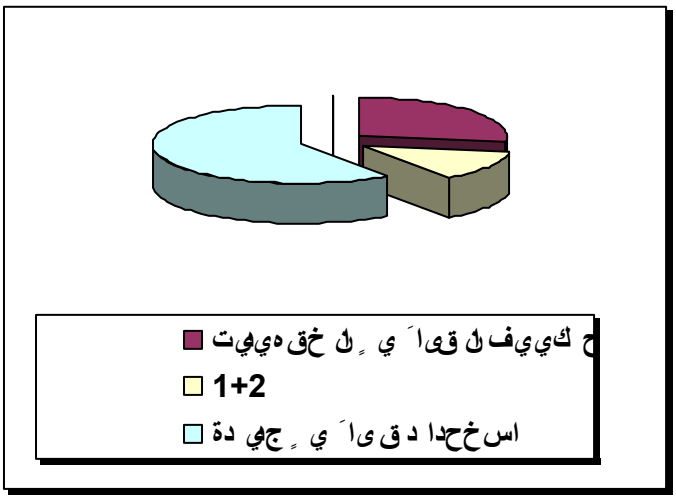
الشكل رقم: 19 أسباب المشاكل التي تعترض القضاة في الفصل في القضايا المعلوماتي

ومن اجل تدارك النقص في التشريعات الجزائرية فيما يخص تشريعات حماية المعلومات ،حاولنا معرفة إذا كانت هناك مساعي لاحتواء مثل هذه الجرائم من خلال سؤال الطلبة وكانت الإجابة كما هي موضحة في الجدول رقم30 الصفحة 149

ومن تحليل نتائج الجدول السابق نلاحظ أن أغلب الطلبة (66,6%) ليسوا على دراية إن كانت هناك مساعي أو مشاريع لاستحداث أو تطوير القوانين أو المراسيم من أجل احتواء ظاهرة الإجرام المعلوماتي، والتي أصبحت بحق جرائم العصر التي تهدد المجتمع الكوني ككل ؛ أما (20%) من عينة الدراسة فقد نفوا وجود أي مساعي لإحداث تغييرات على القوانين في الوقت الراهن إلا أن الغد كفيل بأن تتغير هذه النظرة خصوصا وأن هذه الجرائم في توسع

رهيب ولم يسلم منها أحد غي العالم، أما عند محاولة معرفة اقتراحات الطلبة من أجل حل هذه المشكلة كانت الإجابة كما هو موضح غي الجدول رقم 31 الصفحة149

إذن فإن أغلب الطلبة (60%) يرون أن أحسن حل لاحتواء ظاهرة الإجرام المعلوماتي هو استحداث قوانين جديدة وهذا باعتبار أنه الاختيار الأنجع؛ لأن هذه الطاهرة جديدة وتحتاج إلى حلول جذرية تستطيع الإلمام بكل جوانبها ولا تحتاج إلى حلول مؤقتة أو هامشية؛ أما (26%) من الطلبة فيرون أن تكييف القوانين التقليدية يعتبر كافيا لاحتواء الجرائم الحديثة؛ أما باقي الطلبة فإن الحل بالنسبة لهم هو تعديل وتكييف فالقوانين التقليدية في مواضع معينة واستحداث أخرى في مواضع حيث لا مجال للتعديل وهذا الحل هو الأقرب للصواب والشكل البياني التالي يوضح ذلك:



الشكل رقم:20 اقتراحات الطلبة حول احتواء ظاهرة الإجرام المعلوماتي

مر التشفير بعدة تطورات إلى أن وصل إلى ما هو عليه الآن[192]:

- 50- 58 سنة قبل الميلاد: يستخدم الإمبراطور يوليوس قيصر **Jules césar** الرموز المشفرة في رسالته على حاكمه سيسرون **ciceron** في حروبه ضد بلاد الغال وكان يستخدم في ذلك طريقة إستبدال الحروف الأصلية بالحروف التي تليها مباشرة أو تنفيذ عمليات تجعل النص المكتوب غير مفهوم.

- 1499: نشر الراهب الألماني جون تر يمام **Jean Tritheme** أول كتاب خاص بالتشفير يعرض فيه كيفية التشفير.

- 1914- 1918: تطور علم التشفير خلال الحرب العالمية الأولى بشكل كبير وهذا باستخدام تقنيات جديدة تهدف على سرعة الاتصالات العسكرية.

- 1977: تصميم نظام التشفير **RSA** .

- 1997: استخدام مفتاح تشفير بطول 40 بت ثم فك تشفيره من طرف طالب جامعي في عدد من الدقائق.

- 1999: استخدام مفتاح تشفير بطول 512 بت والذي تم فك شفرته من طرف مجموعة من الباحثين بعدة أربعة أشهر.

- 2001الإستخدام الواسع لنظام التشفير **open pgp** من طرف الكثير من العاملين على شبكة الأنترنت بقصد تأمين سرية المعلومات.

3- أنواع التشقير:

التشفير نوعان[193]:

5 -**التشفير المتماثل:** يستخدم فيه المفتاح نفسه للتشفير وكذا لفك الشفرة, وبذلك فإن المفتاح يكون معروفا من طرف كل من مرسل الرسالة ومستقبلها ولا يرسل المفتاح مع الرسالة ولكن يرسل بطرق أخرى حرصا على حماية سرية المفتاح وعدم إطلاع الغير عليه؛ وقد استعملت كتب للأكود **sécure code book** وتتضمن قائمة بمفاتيح التسفير التي يجب أن تستخدم بطرق محددة ؛فعلى سبيل المثال فإن الرسالة التي ترسل يوم الأربعاء يتم

---

[192]- عبد الحق, ط.**مدخل إلى المعوماتية: برمجيات الحاسب الشخصي. = Logiciel de PC**.البليدة: فصر الكتاب ,2005.ص.327.

[193]- بومفلاح, فاتن.المرجع السابق.ص.561.

استخدام المفتاح A يفك شفرتها ,وتفقد كتب الأكواد فيمتها إذا ما تمت سرقتها لأن ذلك يعني كشف المفتاح من قبل الغير.

6 -التشفير غير المتماثل: ويستخدم فيه مفتاحان لكل مستخدم , أحدهما +مفتاح عام معروف من قبل الآخرين حيث يسجله الشخص عادة مع توقيعه على البريد الإلكتروني , في حالة الرغبة في إرسال رسالة مشفرة إلى ذلك الشخص يتم استخدام ذلك المفتاح العام لكتابة الرسالة أما لفكها فيستخدم مفتاح خاص لا يعرفه إلا المستقبل نفسه ؛وغلى الرغم من ارتباط كل نمن المفتاح العام والخاص ببعضهما إلا أن أي منهما لا يدل على الآخر.

وهناك طرق متعددة للتشفير تتراوح في درجة تعقيدها فقد تكون سهلة للغاية لا تتعدى فكرة الاستبدال كما هو الحال في شيفرة قيصر التي تمثل في أبسط صورها إستبدال كل حرف في الأبجدية بحرف آخر وفقا لمفتاح الشيفرة المحدد ,وقد تم تطوير فكرة الاستبدال حتى تصبح أكثر تعقيدا وبالتالي يصبح كسرها أمرا في غاية الصعوبة.

4- أهمية التشفير:

إن أهم الأخطار التي يمكن أن نتغلب عليها بواسطة التشقير هي[194]:

- الإطلاع على المعلومات المحضورة.
- محاولات تعديل البيانات إلى وجهة إخرى
- تأخير محتويات الرسائل المتبادلة.
- تغيير كلمات السر الخاصة بالمستفدين.
- إنتحال شخصية المستخدم الحقيقي.
- تعديل البيانات المخزنة على الحاسب.

5-1-3-3. الجدران النارية:

1- تعريف الجدران النارية:

يخطر في بال معظم الناس عند الحديث عن أمن شبكة الأنترنت برامج جدران النار وعلي الرغم من أن برامج جدران النار لا تعتبر علاجا لجميع مشاكل أمن المعلومات علي شبكة الانترنت، إلا إنها ضرورية لأي إستراتيجية متعبة، في مجال أمن انترنت، تعتبر

[194]- داود ,حسن الطاهر.الحاسب وأمن المعلومات.المرجع السابق.ص.178.

برمجيات جدران النار ببساطة حاجزا بين شبكتين وهما في اغلب الأحيان شبكة داخلية وتسمي الشبكة الموثقة **trusted network** شبكة خارجية تسمي **entrusted network** وهي شبكة انترنت في هذه الحالة وتقوم برمجيات جدران النار بفحص رزم البيانات القادمة والخارجة اعتمادا علي مجموعة قواعد التي يضعها المشرف علي الشبكة، للسماح لهذه الرزم بالمرور أو يقوم بحجبها ومنعها من الوصول إلي الشبكة الداخلية.

في الأيام الغابرة كانت تقام أسوار حجرية تفصل بين الأبنية والبيوت الخشبية , فتمع في حالة إندلاع حريق امتداد اللهب من بيت لآخر وكانت تسمى بجدران النار , وفي الشبكات الحديثة مثل الأنترنت يمكن اعتماد الطريقة نفسها لحماية مصادر الشبكات الداخلية من الأخطار الناتجة عن ضياع المعلومات الحيوية[195].

ويمكن تعريف الجدار على أنه برنامج **software** أو عتاد **hardware** لحماية موارد الشبكة الداخلية من مستخدمي الشبكات الأخرى , وتستخدم في حالة ارتباط الشبكة بشبكات واسعة وتعمل على منع المستخدمين الخارجيين من الوصول إلى مولد الشبكة وبياناتها الخاصة [196].

إذن فالجدران النارية عبارة عن نظام أو مجموعة أنظمة تفيد تعزيز ضبط الوصول إلى المعلومات بين شبكتين أما الوسائل المعتمدة فمختلفة إنما من حيث المبدأ يمكن تعريفه بأنه عبارة عن آليتين , واحدة تعيق الحركة والأخرى تسمح بها [197].

2- أنواع الجدران النارية:

تستخدم معظم برمجيات جدران النار اليوم طريقة واحدة أو أكثر من الطرق الثلاث المتبعة في فحص الرزم وتستخدم العديد من الموجهات تقنية جدران النار المسماة بترشيح الرزم **packet filtering** والتي تفحص عناوين وبوابات المصدر **Source** والوجهة النهائية **destination** لرزم **TCP** ورزم **UDP** القادمة ثم ترفض أو تسمح للرزم بالمرور وفقا لمجموعة من القواعد مسبقة التحضير وتعتبر تقنية ترشيح الرزم طريقة رخيصة نسبيا وشفافة بالنسبة للمستخدم ولها تأثير طفيف غير ذي بال علي أداء الشبكة ولكن تجهيز تقنية ترشيح الرزم يعتبر عملية معقدة نسبيا ويتطلب معرفة دقيقة بالشبكة وبرتوكولات النقل بل يتطلب في بعض الأحيان معرفة ببروتوكولات التطبيق.

---

[195]- المسفر ,**يوسف.الشبكات المعلوماتية والجدران النارية**.من مجلة علوم وتكنولوجيا.ع53. اتلسنة الخامسة 1996.ص.48.

[196]- بومفلاج , فاتن.**حماية المعلومات في شبكة ام القرى**.مقتطف من كتلب الوقائع.مج 2.الشلرقة ,2001.ص.562.

[197]- المسفر ,يوسف. المرجع السابق.ص.48.

تكمن المشكلة الأخرى في تقنية مرشحات الرزم في أنها عرضة لما يسمي خداع بروتوكول انترنت IP Spoofing وهي طريقة يستخدمها الهاكرز ليتمكنوا من الوصول إلى شبكة شركة عن طريق تغيير عناوين بروتوكولات انترنت في ترويسة الرزم إلى عناوين أخرى مقبولة من قبل شركة أخرى

أما النوع الأكثر تقدما وأمنا من أنواع جدران النار فهي برامج بوابات التطبيقات application gateways، تستخدم معظم منتجات جدران النار العاملة بتقنيات بوابات التطبيقات بما فيها برامج eagle الشهيرة من شركة Raptor ما يسمي توكيلات التطبيقات application proxies وهي عبارة عن برامج مكتوبة لخدمات معينة من خدمات انترنت (مثل خدمات HTTP ، FTP وخدمة telnet وتعمل علي مزود مرتبط بشبكتين كمزود Server لزبون تطبيقات application client وكزبون لمزود التطبيقات application server

ونظرا لان برامج توكيلات التطبيق تقوم بتقييم رزم الشبكة لتحديد شرعية البيانات المتعلقة بتطبيق معين فإنها تعتبر شكل عام أكثر أمنا من مرشحات الرزم. وتمتاز معظم جدران النار لبوابات التطبيقات باحتوائها علي ميزة تدعي "ترجمة العناوين الشبكة Network Address " Translator والتي تمنع ظهور عناوين IP الداخلية .أمام المستخدمين من خارج الشبكة الموثقة.

تكمن إحدي السلبيات الرئيسية في تقنية بوابات التطبيقات في انخفاض مستوي الأداء بسبب المعالجة المضاعفة التي تتطلبها وظيفة التوكيل proxy function وهناك سلبية أخري تكمن في انه قد يتوجب عليك أن تنتظر عدة أشهر حتى تزودك الشركة الصانعة لبرنامج جدران النار بتوكيل التطبيق application proxy لأي خدمة جديدة من خدمات انترنت مثل استخدام خدمات RealAudio.

وإذا كنت تنوي استخدام جدران النار دفاع محيطي خارجي فقط وراء توصيلات T1 الي مزود خدمة انترنت فلا داعي للقلق علي الأداء، لان عرض الحزمة المنخفض لهذه التوصيلات سيصل إلي حد الإشباع قبل وصول جدران النار الي ذلك الحد. قد تجد الكثير من المؤسسات ضرورة في استخدام جدران النار إضافية علي مستوي شبكاتها الداخلية لفرض حزام امني علي مزودات أقسامها المختلفة مثل مزود المورد البشرية الذي يحتوي عادة علي معلومات حساسة، ويصبح الأداء في هذه الحالة عاملا مهما نظرا لان الربط سيعتمد علي شبكة ايثرنت بسرعة10 ميجابت/ثانية

أو شبكة ايثرنت السريع 100 ميجابت/ثانية .وإذا كنت تنوي استخدام توكيلات التطبيقات داخليا فعليك أن تعتمد علي حل مبني علي عتاد سريع مثل pix firewall من شركة Cisco أو firebox من شركة Seattle software أو قد تلجا الي تركيب برمجيات جدران النار علي نظام يتضمن عدة معالجات .

أما النوع الثالث من تكنولوجيا جدران النار والذي أسمته شركة check point software باسم تفقد الحالة الكاملة state full inspection فهو موجود في برنامج firewall-1 من شركة نفسها وبرنامج pix firewall من شركة سيسكو وبرنامج On Guard من شركة On technology وبرنامج firewall/plus من

شركة network-1 وكما هو الحال في تقنية ترشيح الرزم فان هذه التقنية تستقبل أولا الرزم علي مستوي طبقة الشبكة Network layer ثم تقوم بتفحص جميع الرزم ومقارنتها مع نماذج معروفة من الرزم الصديقة وفيما تعطي طريقة تفقد الحالة الكاملة أداء اعلي بقليل من أداء توكيلات التطبيقات إلا أن الجدل يبقي قائمافيما إذا كانت آمنة مثلها أم اقل أمنا منها[198].

3- الوظائف الأساسية للجدران النارية: تتلخص أهم الوظائف التي تؤديها الجدران النارية في 199:

- منع دخول المستعملين غير المصرح لهم بالدخول إلى الشبكة.
- حماية استخدام الخدمات الهامة عند الدخول إلى الشبكة ومغادرتها.
- حماية عامة من جميع الهجمات.

وبذلك يمكن لأي شركة أو بنك أو مؤسسة حكومية حماية وتامين المعلومات الخاصة بها من أي مستعمل غير مصرح له بالدخول وهذا يعني أن برمجيات جدران النار تحتو يعلى مجموعة من السياسات التي تجعلها بمثابة مصفاة لمنع الطلبات المشبوهة من الوصول إلى الجهاز الخادم ؛ كما يمكن إعدادها بحث يتم إسقاط ووقف أية طلبات واردة تحاول النفاذ إلى الخادم من منفذ لم يحدد ضمن سياسات هذه البرمجيات , ويمكن لبرنامج الجدار الناري أن يقوم بحماية الشبكة من الفيروسات والحماية من البرمجيات الدخيلة بحسب ما سطر داخل البرمجة.

3- مزايا وعيوب الجدران النارية:

يمكن القول وكما في أية تقنية جديدة أن الجدران النارية لها عيوب ومزايا نلخصها في ما يلي[200]:

1- فيما يخص المزايا:

- توفير الحماية اللازمة للشبكة والمعلومات.
- توفير خدمات تشفير عالية القوة.
- الجدار الناري يتوافق مع جميع الشبكات المفتوحة.
- تخرين المعلومات والعمليات التي تمر من خلاله.

---

[198]- **أمن الشبكات..**[على الخط المباشر]. زيارة يوم: 2006/03/18 متوفر على الموقع: http://www.jubailnet.com/vb/forumdisplay.php

[199]- حجازي.عبد الفتاح البيومي. الحكومة الإلكترونية.المرجع السابق.ص. 60.

[200]- حجازي.عبد الفتاح البيومي. الحكومة الإلكترونية.المرجع نفسه.ص. 63.

- متابعة المستخدمين للشبكة وكل من يحاول العبث بها.

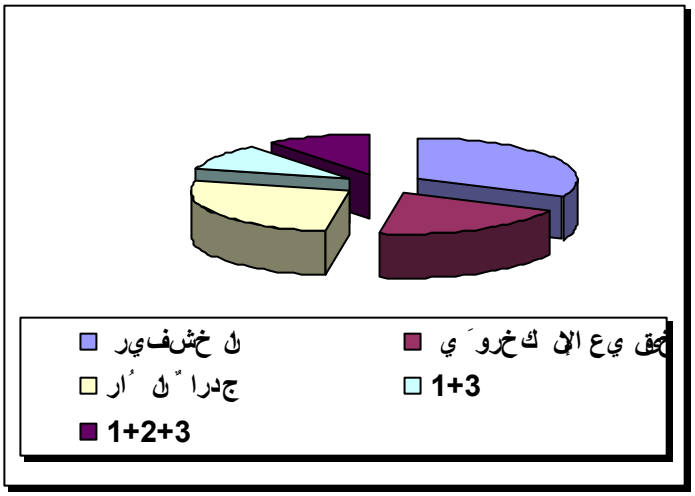
أما فيما يخص العيوب:

- لا يتعامل الجدار الناري مع البرامج الداخلية التي تهاجم النظام.

- لا يقدم الحماية للنقل الإذاعي والتلفزيوني.

التشفير ،التوقيع الإلكتروني، جدران النار أهم الطرق المعتمدة لحماية المعلومات وضمان سلامتها أثناء مسارها وعند سؤال الطلبة عن أهم وأنجع الطرق لحمايتها كانت الإجابة كما هي موضحة في الجدول رقم 20 من الصفحة 146

إذن فإن أنجع طرق الحماية حسب الطلبة هو عملية التشفير(31,5 %) والتشفير هو إعادة كتابة البيانات باستعمال أحد مفاتيح التشفير، ثم تليها جدران النار بنسبة (26,3 %) وهو محاولة تصفية البيانات الداخلة إلى الداخلية لمؤسسة ما عن طريق مصفاة يطلق عليها جدران النار، ومع تطور معاملات التجارية وظهور الإقتصاد الشبكي كالتجارة الإلكترونية والتسوق الإلكتروني أدى إلى ظهور وسيلة جديدة هي التوقيع الإلكتروني والذي يعد وسيلة لا غنى عنها في مثل هذه المعاملات كما بمكن الجمع بين وسيلتين آو أكثر من الوسائل السالفة الذكر وذلك لضمان حماية أكبر وهذا ما نوضحه في الشكل البياني التالي :



الشكل رقم:15 وسائل حماية المعلومات

2-5. أمن المعلومات: الأخلاق (أخلاق التعامل في مجتمع المعلومات)

إن الأخلاق تعد قوة ردعية في المجتمعات لا يستهان بها غي إرشاد وتوجيه سلوكيا ت الناس فما هو الدور الذي تلعبه الأخلاق في مجتمع المعلومات؟

5-2-1. مجتمع المعلومات.

أن مجتمع ما بعد الصناعة هو مجتمع المعلومات وفي مايلي نتطرق إلى اهم عناصر هذا المجتمع الجديد

5-2-1-1. مفهوم مجتمع المعلومات.

لابد في البداية إلى الإشارة أن هناك العديد من التعريفات لمجتمع المعلومات وأن تعريف مجتمع المعلومات لا غير واضح المعالم بشكل عام

إنه مفهوم يرى التحول من مجتمع صناعي إلى مجتمع حيث المعلومات هي القوة الدافعة والمسيطرة وهناك من يرى أنه المجتمع الذي ينشغل معظم أفراده بإنتاج المعلومات أو جمعها أو اختزانها أو معالجتها أو توزيعها [201]. كما يرى البعض بأن مجتمع المعلومات هو المجتمع الذي تستخدم فيه المعلومات بكثافة كوحي للحياة الاقتصادية والاجتماعية والثقافية والسياسية، ويرى الدكتور ناريمان متولي أن مجتمع المعلومات هو المجتمع الذي يعتمد في تطوره بصفة رئيسية على المعلومات الحاسبات الآلية وشبكات الإتصال أي أنه يعتمد على التكنلولوجيا الفكرية التي تضم سلع وخدمات جديدة مع التزايد المستمر للقوة العاملة المعلوماتية التي تقوم بإنتاج وتجهيز ومعالجة ونشر وتوزيع وتسويق هذه السلع والخدمات

وقد أدى عدم الاتفاق على مجتمع المعلومات إلى اختلاف الرؤى حوله فقد أشارت دراسة حديثة عن الموضوع إلى ثلاث رؤى لمجتمع المعلومات

الرؤية الأولى: وهي رؤية أوربية يمثلها العالم الاجتماعي(إيان مايلز**Ian miles**) وترتكز على الإنتشار الواسع لتكنولوجيا المعلومات والإتصالات ومالها تأثيرات هي التي تشكل مجتمع المعلومات

الرؤية الثانية: هي رؤية يابانية ويمثلها العالم الاتصالات اليابانية جوهوكا شاكاي **johoka shakia** وهي يرتكز على تدفق أو انسياب المعلومات بكميات هائلة عبر كل الوسائل في المجتمع وترتكز.

---

[201]– عبد الهادي ,محمد فتحي.**المعلومات وتكنولوجيا المعلومات على أعتاب قرن جديدة**. القاهرة:الدار العربية للكتاب ,2000.ص.18.

الرؤية الثالثة: وهي رؤية أمرقية ويمثلها عالم الإقصاد (فريتز ماكلون) على أن نسبة متزايدة من الناتج القومي الكلي للدولة تجيء من إنتاج المعلومات، ومن ثم أضافت الإقصاديات الحديثة قطاعا جديدا إلى القطاعات المعروفة[202].

ومن وجهة نظرنا أن كلى هذه الرؤى روافد تصب في نهر واحد ,وان كل واحدة من الرؤى الثلاثة السابقة إما أن تكون سببا لأخرى أو أن تكون حتمية لسابقتها .

إن عصر ما بعد الصناعي أو مجتمع المعلومات كما يطلق عليه هو حصيلة لتراكمات إحتماعية وعلمية وثقافية طيلة سنوات، وقد ساهم غب دخول هذا العصر التطورات التقنية والتكنولوجية التي عرفها العالم المعاصر؛ وتعد الولايات المتحدة الأمريكية وكندا ودول أوروبا من بين الدول السباقة للإنخراط في مجتمع المعلومات الكوني؛ أما دول العالم الثالث بصفة عامة والدول العربية خصوصا فقد خطت خطوت محتشمة للإنضمام لهذا الركب وعند سؤال الطلبة عن ضرورة آو حتمية الإنخراط في مجتمع المعلومات كانت الإجابة كما هي موضحة في الجدول رقم21 من الصفحة 146
إذن وحسب نتائج الجدول فإن الأغلبية الساحقة لعينة الدراسة (97,3 %) ترى أن دخول عالم المعلومات هو ضرورة ملحة تفرضها الظروف المعاشة وهذا من أجل اللحاق بركب الحضارة وعدم الاضمحلال في بوتقة العولمة .

5-2-1-2. خصائص مجتمع المعلومات:

يقدر علماء الاقتصاد أن حجم التعاملات المالية التي تتم يوميا عبر الأجهزة والشبكات الإلكترونية للمؤسسات المالية يصل إلى 25بليون دولار , ولعل هذا الرقم العالي يظهر اعتماد المجتمعات في هذا العصر على التجهيزات المنية على تقنيات الحاسب [203] ؛ويمكن تلخيص أهم خصائص التي تطبع مجتمع المعلومات[204]:

1- **انفجار المعرفة:** يرى العديد من لباحثين أن المعلومات المنتجة في الحقبة المعاصرة أكثر أهمية مما أنتج في كل تاريخ البشرية ,كما أنها تتزايد بمعدلات كبيرة نتيجة التطورات التي يشهدها العالم ونتيجة بروز تخصصات جديدة.

2- **زيادة أهمية المعلومات:** في مجتمع المعلومات ازدادت أهمية المعلومات وأصبحت المعلومة تدخل في كل الأنشطة والصناعات، كما تمثل المادة الخام لقطاعات كثيرة من قطاعات المجتمع المعاصر مشكِلة ما يمكن أن يطلق عليه" صناعة المعلومات " وأصبح ينظر إلى المعلومات كمورد أساسي وإستراتيجي يمكن أن يباع ويشترى.

---

[202]- عبد الهادي ,محمد فتحي. المرجع السابق.ص.18.
[203]- عباس , طاهر محمود.**المكتبات الرقمية وشبكة الأنترنت**.القاهرة: المركز الأصيل ,2003.ص.45.
[204]- لغقاب، محمد. مجتمع **الإعلام والمعلومات:ماهيته وخصائصه**.الجزائر:در هومة ،2003.ص.88.

3- **نمو المجتمعات والمنظمات المعتمدة على المعلومات** :يتميز مجتمع المعلومات كذلك بظهور منظمات تعتمد كلية ً على المعلومات مثل مؤسسات الجرائد والأخبار والإستعلامات والبنوك وشركات التأمين....

ويلاحظ أن انفجار أو تضخم هذه المنظمات قد بدأ في الظهور في نفس الوقت الذي شهد بدايات ثورة المعلومات المعاصرة.

4- **تعدد فئات المتعاملين مع المعلومات** : أوجد مجتمع المعلومات فئات كثيرة تتعامل مع البيانات والمعطيات والمعلومات وتشتغل بها منها:

- العلماء والفنانون والمصممين وغيرهم ممن يقدرون على إنتاج وإيجاد معلومة جديدة أو يعيدون تشكيل نماذج معرفية جديدة من واقع المعلومات الحالية.

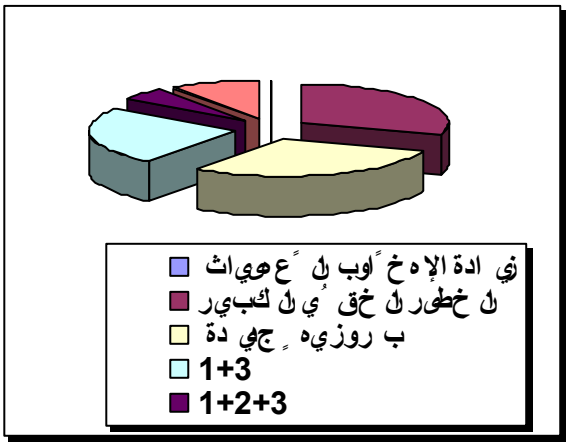
- العاملون في نقل وتوصيل المعلومة.

- العاملون في تخزين المعلومات كأخصائي المعلومات وأمناء المكتبات ومبرمجي الحاسب.

5- قلة الاعتماد على الورق: حيث تزايدت بصفة مطردة كميات المعلومات المنتجة على وسائط غير ورقية وفي المقابل فإن استعمال الورق أخد يتقلص.

إن العصر الذي نعيشه بكل حيثياته هو مجتمع المعلومات هو مجتمع المعلومات بحق؛ فقد غدت المعلومات العصب المحرك لكل مناحي الحياة الاجتماعية والسياسية والثقافية والعلمية، وقد تزايد الاهتمام بالمعلومات مند أن أصبحت تمثل مصدرا أساسيا للدخل القومي للدول المنتجة للمعلومات، وقد ظهرت قطاعات تُعنى بالمعلومات عي كل مراحلها أي مند إنتاجها وإلى غاية نشرها وتوزيعها؛ وقد اتسم مجتمع المعلومات بعدة خصائص نوجزها في الجدول22 من الصفحة 146

إذن فحسب عينة مجتمع الدراسة فإن الخاصيتين اللتان تطبعان مجتمع المعلومات هي زيادة الاهتمام بالمعلومات وكذا التطور التقني المذهل (31,5 %) وهذا ما يؤكده حشد ميزانيات ضخمة والتي تخصصها الدول المتقدمة من أجل تنمية البحوث العلمية وكذلك إنشائها لأكبر مراكز البحوث العلمية والتكنولوجية، إن هذا الاهتمام الكبير بالمعلومات أدى إلى ظهور مهن جديدة كصناعة المعلومات وهذا ما عبرت عنه (26,3 %) من عينة الدراسة، أما باقي الطلبة فيرون أن كل هذه الخصائص السالفة الذكر لها نفس الأهمية في مجتمع المعلومات ،ويمكنا أن نوضح ذلك بشكل أفضل كما يلي:



الشكل رقم:16 خصائص مجتمع المعلومات

5-2-1-3. أبعاد مجتمع المعلومات: :

يصوغ بيل (Bell, 1973) فكرة الأركان الإحداثية التي تفسر الأطر الاجتماعية وتدرس تماسك المجتمع من خلال وضع مفهوم يوضح تنظيم المجتمع، فيصنف المجتمع ما بعد الصناعي (مجتمع المعلومات) إلى ثلاثة كيانات: اجتماعية، سياسية، ثقافية. و يشتمل الكيان الاجتماعي على النواحي الاقتصادية والتكنولوجية ونظم العمل، أما الكيان السياسي فهو المعنى بتوزيع السلطات والكيان الثقافي يهتم بالمعاني والرموز.

وفى ضوء هذه الكيانات يرى بيل Bell أن في مجتمع المعلومات يحدث التالي:

1- تتغير أدوار الأفراد في المجتمع لبلوغ غايات محددة، ويعتمد على ذلك ظهور أنماط جديدة في السلوك على الأفراد مراعاتها لمواءمة حالة المجتمع الجديد ومثال ذلك انتشار النواحي التخصصية والعوامل المعرفية والتي تتطلب نشاطا مماثلا من الأفراد.

2- تنشأ علاقة تنافسية بين البناء الاجتماعي والكيان السياسي وذلك لأن مجتمع المعلومات قائم على تطور البناء الاجتماعي وظهور الجوانب المعرفية والأهمية المعلوماتية مما يسحب البساط من تحت أرجل النخبة السياسية الحاكمة.

3- يعتمد ظهور أنماط جديدة في حياة أفراد المجتمع على درجة المعرفة النظرية والإدراكية Cognitive Theoretical knowledge التي ترتبط بجوانب الثقافة المجتمعية، مما قد يؤدى إلى ظهور النزعة الفردية .

وينظر بيل Bell إلى مجتمع المعلومات على أن محوره الرئيسي ولب تكوينه يتمثل في عملية المعرفة ويعلل ذلك بالقول أن المعرفة هي الضابط الاجتماعي والموجه لعمليات الإبداع والتجديد والتغيير التي تعمل على نشأة علاقات وهياكل مجتمعية جديدة. ويتمركز مفهوم هذا المجتمع الجديد حول القطاع الاقتصادي والمعنى بالإنتاج والخدمات وتقسيم فئات العمل.

---

[205]- عبد الباري ,**وائل إسماعيل حسن.أسس مجتمع المعلومات العربي قراءة للأبعاد المعرفية والتقنية في المجتمع العصري**.[على الخط المباشر]. زيارة يوم: 2006/03/18 متوفر على الموقع:
http://www.arabcin.net/arabic/5nadwhauthors albari.htm.

أما الأبعاد المعرفية والتكنولوجية فى مجتمع المعلومات فيرى بيل **Bell** المجتمع ما بعد الصناعي بأنه مجتمع معرفي من خلال بعدين:

أ- تنامي مصادر التجديد والاختراعات القائمة على البحث والتطوير وازدياد العلاقة الوثيقة بين العلم والتكنولوجيا وذلك بسبب مركزية المعرفة النظرية.

ب- كون مؤشرات معدل الناتج القومي ونوع العمل قائمة بصفة كبيرة على الحقل المعرفي، ويتجلى ذلك بوضوح فى طبيعة تقسيم المهن التي تركز على الخدمات المعلوماتية.

5-2-2. أخلاق مجتمع المعلومات.

5-2-2-1. تعريف أخلاق مجتمع المعلومات.

إن مصطلح الأخلاق يتناول المبادئ التي توجه السلوك البشري وهو يتعلق بقضايا الصواب والخطأ ,العدل والظلم ,الصحيح وغير الصحيح وذلك بالنسبة لمجتمع ما أو جماعة معينة[206].

وإذا كانت دراسة الأخلاقيات في مهن المعلومات تعتبر فرعية لدراسة الأخلاقيات بصفة عامة ، فليس هناك اتفاق على تعريف محدد لمصطلح الأخلاقيات فالبعض يستخدم المصطلح بطريقة عامة للدالة على[207]:

- طريقة الحياة التي يرتضيها مجتمع معين.

- مجموعة من القواعد السلوكية التي تضمن تسيير المجتمع نحو الخير والصواب في مواجهة الشر والخطأ.

وكلمة الأخلاق **Ethics** مستخلصة من الجذر اليوناني **Ethos** والذي يعني خَلق؛ وتكون الأخلاق طقما من المعتقدات أو النمطيات أو المثاليات الموجِهة للأفراد.

ويذهب (كلايد كنغ **Clyde king**) إلي أنه يمكن تعريف الأخلاق بأنه نظام من المبادئ الأخلاقية التي تحدد السلوك الصواب والسلوك الخطأ وذلك بالنسبة لمجتمع أو أمة أو جماعة معينة.

وتزداد أهمية الأخلاق في الوقت الحالي أي في مجتمع المعلومات مع تزايد المشكلات الأخلاقية التي يواجهها العالم المعاصر ؛وعندما يذهب الباحثون في الغرب بعيدا في البحث عن أخلاق مجتمع المعلومات فإنهم يبحثون ويدرسون انطلاقا من مجتمعاتهم ومفاهيمهم وتوجهاتهم

---

[206]- عبد الهادي ، فتحي. **المعلومات وتكنولوجيا المعلومات على أعتاب قرن جديد.القاهر**ة: مكتبة الدار العربية للكتاب.،2000.ص.37.

[207] -الهوش ،أبو بكرمحمود. **التقنية الحديثة في المعلومات والمكتبات:نحو إستراتيجية عربية لمستقبل مجتمع الملومات**.القاهرة: دار الفجر،2002ص.244.

؛ وهم يحاولون بذلك ان يحددوا إالأخلاق بما ينفع هذه المجتمعات ويحافظ على تماسكها ؛وأخلاق مجتمع المعلومات لاتختلف عن الأخلاق بصفة عامة وفي الواقع يمكن إيجازها بأنها أخلاق رجل المعلومات وهي مجموعة من المبادئ والقيم التي يجب أن يتخلق بها الشخص في خضم هذا المجتمع وهي تختلف عن القانون لأنها تحدد تصرفات الناس دون إجبار أوإلزام قانوني.

5-2-2-2. أهم المبادئ الأخلاقية في مجتمع المعلومات:

إن الإنسان المعاصر ينظر إلى مجتمع المعلومات على أنه نموذج أخلاقي علمي واجتماعي متقدم ،سيتيح لمجتمعاتنا المخالفة إمكانات أكبر في تبادل المعلومات وتحقيق حرية إنسيابها ،وتحقيق فوائد متوازنة لمختلف المجتمعات وخاصة تلك الاضعف ثقافيا وإقتصاديا وتقنيا ،إلا أن الوقائع تختلف تماما عن النمودج الاخلاقي ويمكن ان نلخص أهم المبادئ والقيم الأخلاقية التي يجب ان تتوفر في مجتمع المعلومات في[208]:

– يشكل تعدد اللغات والثقافات في دائرة المعلومات العالمية ميزة أخلاقية وعلمية وثقافية هامة لابد من المحافظة عليها ضمانا لتنوع وتكامل دائرة المعلومات الدولية وللحفاظ على التراث الثقافي للبشرية ,وحرصا على تطور المشهد الثقافي العالمي.

– تشكل الفجوة الرقمية إحدى اهم المشكلات الأخلاقية التي يواجهه العالم وتتفرع عنها مشكلات أخلاقية وإقتصادية وإجتماعية وعلمية لايمكن للعالم ان يشيح نظره عنها ؛ وإن حل هذه المشكلات يعد الخطوة الأولى الضرورية لبناء مجتمع المعلومات.

– دعم التعاون العالمي في في مجال تبادل المعلومات ليس مسألة نظرية تطرح في المنتديات والمؤتمرات العالمية بل هي مسؤولية أخلاقية جماعية يتوجب على البلدان المتقدمة دعمها من خلال إتاحت المعلومات العلمية وعدم حجبها عن الدول النامية.

– إن مقهوم القرية الكونية يفرض أساسا نشوء مسؤولية إجتماعية جماعية إخلاقية لحل المشكلات التي يعاني منها سكان هذه القرية وأهم المسائل التي يجب الإنتباه لها في مجتنع المعلومات هي:

* الحق في الملكية الفكرية وإحترام أعمال الغير وعدم التعرض لها بأي نوع من أنواع الإعتداد والإستحواد.

---

[208]– **مشروع ميثا الشرف العربي لأخلاق مجتمع المعلومات**.[على الخط المباشر].زيارة يوم:2006/02/16. متوفر على الموقع:
http://www.arabcin.net/arabia3000/arabia1htm.

* الحق في حماية خصوصية الأفراد والمؤسسات وإحترام الحياة الخاصة بهم.

* حرية إكتساب المعلومة.

* مصادقة المعلومة وكيفية التعامل معها في ظل الإنفجار المعرفي.

* كيف يمكن حماية الشبكة من التلوث ومن التخريب فهي شيئ مشترك في مجتمع المعلومات.

5-2-2-3. الإفرازات الأخلاقية الجديدة في مجتمع المعلومات:

من الواضح أن التقنية المتقدمة والوصول إلى المعلومات المتنوعة أو حتى التمكن من هذه المعلومات وإمتلاكها كل هذا لا يجعل من الإنسان المستفيد معلوماتيا أكمل او أكثر صفاء وثراء روحيا ؛ إذا المهم هو مضمون المعلومات وأهدافها الإجتماعية ونوع علاقات الإنسان بها والموشور الذي يتعامل معها من خلاله وهذا ما يحدد الغالم الروحي للإنسان ، بل وغالبا ماتطرح التكنولوجيا المتقدمة ضروريات جديدة تلزم مالكها بالتمتع بأخلاقيات منظبطة إذ أن هناك فرق بين التعامل مع الحواسيب كهدف والتعامل معها كمجرد وسيلة.

لا شك ان إنتسار الحواسيب الشخصية والوسائل الحديثة يمكن أن يقوي الفردية لذى الناس ويضعف الروح الجماعية وكثلفة الإختلاط قي مابينهم لأن تكنولوجيا المعلومات مبنية أساسا على الإستخدام الفري وتحد من الإختلاطات المباشرة ؛ فالرفيق والزميل والصديق يصبح غالبا الآلة أو التجهيزات في حين يصعب التخلي عن معاشرة الناس كقيمة روحية عالية تَلزم الإنسان وترافقه مند الأزمة الغابرة.

إن موجة التكنولوجيا الجديدة تبرز على السطح ضروبا من الإغتراب أو الإستلاب ، ولا سيما ما يسمى بالإغتراب المعرفي ،وأحد جوانب هذا الإغتراب شعور الشخص بالدونية أو النقص إتجاه إمكانيات الآلة المتنامية بإستمرار ؛ ويرى بعض علام النفس أن منطق الآلة الصارم وتعامل الإنسان معه قد يؤدي مع الزمن من الوجهة النفسية على الأقل إلى فقدان حس الإبداع كما أن مايدعم هذه العولة الإجتماعية أو تشارك في وضع واقع تخيلي بديلا للواقع الفعلي هو ألعاب الكمبيوتر والموديلات والنمادج[209].

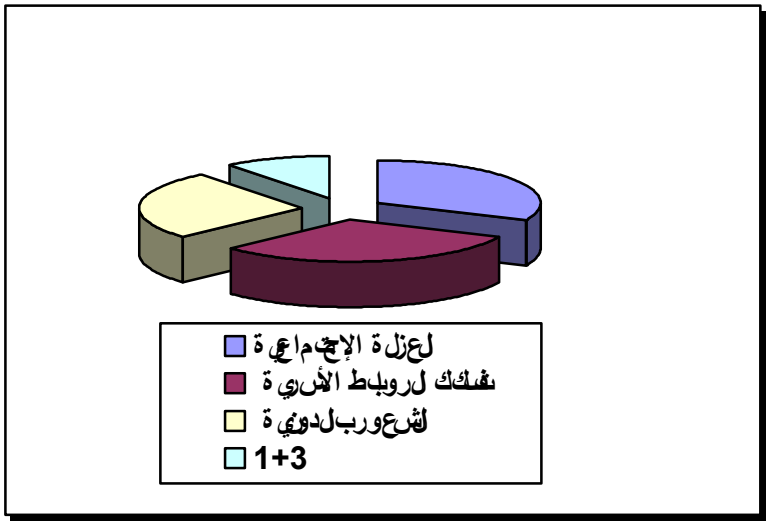
إن كل هذه الإفرازات السالفة الذكر والتي يتركها الإنخراط في مجتمع المعلومات على السلوكيات البشرية تعد من بين سلبيات هذا المجتمع الجديد وعند الإستفسار عن رأي الطلبة حول الموضوع كانت الإجابة بالإجماع على أنه لمجتمع المعلومات إفرازات سلوكية على الأفراد والنتائج كما هو موضح في الجدول رقم23 في الصفحة 147

---

[209]– النقري،معن.**المعلوماتية والمجتمع / مجتمع ما بعد الصناعة ومجتمع المعلومات**.المغرب؛ لبنان:المردز الثقفي العربي،2001.ص.20.

أما عن أهم هذه الإفرازات على السلوك البشري فإنه يمكن أن يتسبب فيخلق عزلة اجتماعية لدى الأفراد كما يمكن أن تساعد في تفكك الروابط الأسرية والاجتماعية داخل المجتمع كما تساهم في خلق نوع من الشعور بالدونية والإنهزامية داخل الفرد هذا أمام إمكانا ت الآلة اللامحدودة والجدول 24 في الصفحة 147 يوضح ذلك

إذن فإن الطلبة يرون أن خلق العزلة الإجتماعية لدى الفرد أهم مشكل يخلقه مجتمع المعلومات بنسبة (31.5 %) وهذه العزلة تنتج من بقاء الفرد لمدة ساعات أمام الآلة مما يجعله يبتعد تدريجيا عن محيطه، إضافة على الطرق المستحدثة غب التعليم كالتعليم عن بعد والذي يفقد الفرد الصديق والأستاذ والزميل وكل هذه العناصر تصبح متوفرة بطريقة إفتراضية؛ كما يؤدي الإنخراط في مجتمع المعلومات إلى تفكك الروابط الأسرية والإجتماعية (31,5 %) وهذا لنفس السبب وهو بقاء الفرد لأرقات طويلة أمام شاشة الحاسب مما يؤدي إلى القضاء على الروابط داخل الأسرة ؛إن هذه الإمكانيات الهائلة للآلة تجعل الإنسان يقف أمامها عاجزا مما يخلق لديه نوع من الإنهزامية والشعور بالدونية أمامها ويمكننا تمثيل هذه النتائج كما يلي:



الشكل رقم 17 الإفرازات الأخلاقية لمجتمع المعلومات

5-2-3. أخلاق الحاسب والانترنت.

لقد أدت الانترنت إلى خلق إفرازات جديدة في العالم منها ما هو سلبي ومنها ما هو إيجابي .

5-2-3-1. الأنترنت: الماهية والخدمات.

1- تعريف الأنترنت:

إن الأصل اللغوي لكلمة شبكة هو الفعل الثلاثي شبك بمعنى تداخل يقال تشبيك الشيء تداخل بعضه في بعض.

في حين تتكون كلمة الأنترنت الإنجليزية الأصل من قسمين **Inter** وهو إختصار لكلمة الدولية **International** والقسم الثاني وهو **net** وهو إختصار **Network** وهذا التعريف اللغوي يقودنا لبيان التعريف العلمي لهذه الشبكة إذا وردت تعاريف متعددة أهما أنه:" إرتباط لأف من الكمبيوترات في الإتصال مع بعضها البعض وهي شبكة الشبكات تشمل ملايين من المستخدمين يوميا "[210].

وقد مرت شبكة الأنترنت بعدت مراحل إلى أن وصلت إلا ما هي عليه الآن [211]: – بدأت فكرة الأنترنت كفكرة عام 1964 عندما تمكن الباحثون في مؤسسة **Rand comporation** من تقديم مفهوم الشبكة وتحويل مجموع البيانات.

– بدأ التنفيد المادي عام 1969 بإعتبارها بمثابة شبكة من 4 نقاط معتمدة على تحويل مجموع البيانات يطلق عليها **ARPANET**.

– أثناء الثمانينات إلتحقت عدة شبكات منها **BIRNET- CSNET** بالأنترنت

– عام 1984 تم ربط مايزيد عن 1000كمبيوتر بشبكة **ARPANET**.

– 1983 كانت **MILNET** جزء من الأنترنت وكانت تربط بين منظمات عسكرية ومنظمات بحثية وجامعات في المجال العسكري.

– عام 1984 تك إغلاق **ARPANET** رسميا مع إستمرار نقاط الوصل والشبكات الفرعية في آداء عملها.

– عام 1986 قانت مؤسسة العلوم القومية **national science fondation(NSF)** يربط خمسة من شبكاتها المعتمدة على الحاسبات فائقة السرعة والتي أصبحت فيما بعد تعرف بالأنترنت

– عام 1987 تحملت **NSf** المسؤولة عن إدارة هذه الشبكة.

– عام 1989 بلغ عدد المستخدمين 80.000 مستخدم.

– عام 1991 رفعت **Nsfnetr** مقيودها على الأنترنت لأغراض تجارية.

– 1992 ظهرت لأول مرة تطبيقات الإقتصاد الإلكتروني المعتمدة على الانترنت.

---

[210]– مومني.بشار طلال.مشكلات التعاقد عبر الأنترنت:دراسة مقارنة.الأردن:دار العالم الكتب ,2004.ص.10.

[211]– مرسى, نبيل محمد.التقنيات الحديثة للمعلومات.الإسكندرية:دار الجامعة الجديدة، 2005.ص.181.

– 1997 كان هناك حوالي 16 مليةن مستخدم في كافة أنحاء العالم.

– ومن ذلك الوقت وعدد المستخدمين يتزايد يوما بعد يوم والخدمات المقدمة في تطور وأصبحت الأنترنت شبكة عامة محققة للمشاركة ومستقلة.

الانترنت ذلك الفضاء المترامي الأطراف والذي غير مجرى الحياة، وجعل من الحياة أكثر سهولة ويسرًا، فقد فرضت نفسها كمصدر للمعلومات وأداة للاتصال حتى غدت الأداة الأكثر شعبية مند بدأ تواجدها؛ وقد نمت حتى غدت أهم مظاهر التكنولوجيا العالمية، وعند الإستفسار عن استعمال الطلبة لانترنت كانت الإجابة كما هي موضحة في الجدول رقم 25 من الصفحة147

إذن فقد أجاب اغلب الطلبة (94,8 %) على أنهم من مستعملي الأنترنت وذلك لأن عينة الدراسة تشمل طلبة الدراسات العليا،وهذه الفئة لا غنى لها عن الانترنت باعتبارها مصدر هام للمعلومات خصوصا وأغلب الطلبة في إطار تحصير مذكرات تخرجهم مما يجعلهم على إرتيادها.

2– خدمات الانترنت[212]:

1– البريد الإلكتروني: لإرسال وإستقبال الرسائل بسرعة كبيرة.

2– القوايم البريدية:إنشاء وتحديث قوائم العناوين البريدية الخاصة بمجموعلات الأشخاص.

3– خدمة مجموعة الأخبار: وهي شبيهة بخدمة القوائم البريدية إلا إنها تختلف في أن كل عضو يستطيع التحكم في نوع المقالات التي يريدإستلامها.

4– خدمة الأستلام الشخصي:حيث يمكن من خلال هذه الخدمة للإستعلام عن العناوين البريدية لأي شخص أو جهة تستخدم الأنترنت والمسجلين لديها.

5– خدمة المحادثات الشخصية: حيث يمكن التحدث مع الآخر بالصوت والصورة والكتابة.

6– خدمة الدردشة الجماعية:تشبه الخدمة السابقة إلا إنها في الغالب مكن لأي شخص أن يدخل في المحادثة أو يستمع عليها دون إختيار الآخرين.

7– خدمة نقل الملفات: لنقل الملفات من حاسب إلى آخر.

---

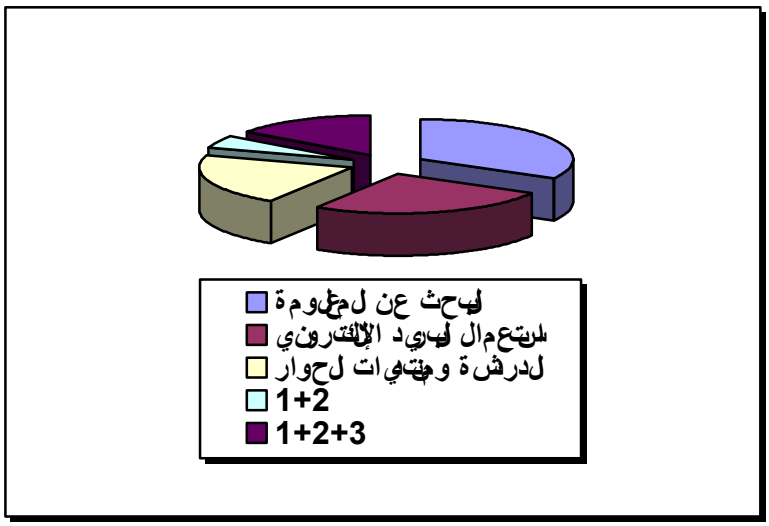
[212]– الجنبهي، منير محمد.الجنبهي، ممدوح ،منير محمد.الطبيعة القانونية للعقد الإلكتروني.الإسكندرية:دار الفكر الجامعي ،[د.ت.].ص.16–17.

8- خدمة شبكة الإستعلامات الشاملة **Gopher** تفيد في خدمات كثيرة كنقل الملفات والمشاركة في القوائم البريدية.

إضافة إلى خدات أخرى كخدمة الدخول عن بعد والصفحة الإعلامية العالمية...إلخ.

إذن فقد وفرت الانترنت العديد من الخدمات التي ت قدمها لمرتاديها بدأبالبريد الإلكتروني والذي حل العديد من مشاكل وعقبات البريد التقليدي حيث أصبح أكثر سرعة وسهولة، إضافة إلى منتديات الحوار والدردشة ومواقع التسلية،هذا إلى جانب أهم خدمة تقدمها الانترنت على الإطلاق وهي البحث الحر عن المعلومات وعند الإستفسار عن أهم الخدمات المحبذة لدى الطلبة كانت الإجابة كما هي مبينة في الجدول رقم 26 من الصفحة 147

ومن تحليل نتائج الجدول نلاحظ أن أكبر استعمال للانترنت هو لغرض البحث العلمي أي البحث الحر عن المعلومة (31,5%)، وهذا باعتبار الطلبة في الدراسات العليا وهم بصدد الإعداد لمذكرات التخرج،وبالتالي تزداد حاجتهم للمعلومات؛ ثم يليها استعمال البريد الإلكتروني(26,6%)وهي الخدمة الأكثر شعبية لدي جميع الناس وبمختلف الفئات والأعمار وها للمميزات التي تتصف بها هذه الخدمة إضافة إلى مجانية الإرسال؛ ثم تأتي إغراض التسلية والترفيه في المرتبة الموالية (21%)؛ لكن استعمال الأنترنت يشمل عادة جميع هذه الخدمات وهذا حسب الحاجة، والرسم البياني التالي يوضح توزيع هذه الخدمات:



الشكل رقم 18 خدمات الأنترنت

5-2-3-2. مخاطر الأنترنت:

ينتج عن استعمال شبكة الأنترنت مخاطر لا يمكن تداركها فالجرائم التي ترتكب عن طريق الشبكة تسمح للمجرمين بالإقدام على جرائمهم وهم على يقين بأنهم لا يمكن كشفهم وتبقى السرية مضمونة فهي لا تعطي أي دليل حسي وأهم هذه المخاطر[213]:

1-الصور اللاأخلاقية: إن إرسال صور لا أخلاقية عبر الانترنت غير مكلف بحيث يمكن إرسالها بالبريد الإلكتروني من شبكة سرية تتلقى هذه المراكز الرسالة فتلقي عنوان المرسل ثم تقوم بنشرها مرة ثانية وبالتالي يصبح من المستحيل معرفة المصدر الأصاي للرسالة او الصورة.

2-الإحتيال: يتم الإحتيال بعدة طرق مثلا يتم عرض بضاعة او صورة إباحية أو غيرها فيطابها أحد المشتركين بالبريد الإلكتروني حيث يطلب منه تحويل ثمنها إلى حساب مصرفي يحدد رقمه في أي مصرف موجود فيقدم طالب البضاعة على إرسال المبلغ حيث يتم سحبها ولا ترسل في المقابل البضاعة أو ترسلة خاطئة أو غير مطلوبة.

التعدي على الحقوق الأدبية والفكرية يمكن بواسطة شبكة الأنترنت بث الأعمال الأدبية والفكرية والأفلام السنمائية للجمهور ويستطيع أي منهم الحصول على نسخة من هذه الأعمال وهذا يشكل تزويرا وتعديا على حقوق المؤلف ، كما يمكن إستعمال شبكة الأنترنت لممارية ألعاب القمار ونشر المعلوملت التي تشكل خطرا كالمعلومات التي تحرض على ارتكاب الجرائم كالتسلح الغير شرعي أو العصيان أو الثورة او الإنتحار وكذاك يمكن إستعمال طالب البضاعة وإستعمال إسمه للقيام بنشطات إجرامية وإستعمال بطاقات الإئتمان بطرق غير فانونية مثل الهبات الخيرية والأرباح الوهمية والإستثمار في الشركات الخاسرة.

5-2-3-3. أخلاقيات الأنترنت[214]:

لقد فتحت الأنترنت أفاقا كبيرة غير مسبةقة في المجالات المختلفة وعلى الأخص في مجالات التعليم والبحث العلمي ونشر الوعي الثقافي وكذا النواحي السياسية والإجتماعية , ولكن ثم إستغلالها في الوقت نفسه من جانب الجماعلت الإجرامية عبر العالم في أغراض أخرى من بينها بث المعلومات المنافية للآداب والمساعدة على العمليات الغرهابية المختلفة.

إن طبيعة الأنترنت التفاعلية واللامركزية على مستوى العالم بالإضافة إلى أهميتها في توفير كم هائل من المحتوى المتاح من وإلى مكان أي مكان قد يؤدي إلى عدد كبير من القضايا القانونية والأخلاقية من بين بينها المحتوى الغير القانوني في الأنترنت.

---

[213]- مغبغب ،نعيم.**مخاطر المعلوماتية والأنترنت**.لبنان:[د.ن.] 1998.ص.213.

[214]- الهوش ،أبو بكر محمود.المرجع السابق.ص.256.

وتضع معضم دول العالم بعض القيود على نوع المحتوى الذي يعالج ويوزع في نطاق حدودها السياسية الوطنية ، وتعكس هذه القيود المفروضة في أي دولة التقاليد والأعراف الثقافية والقانونية ,بالإضافة إلى القيم الدينية والأخلاقية السائدة فيها وقد تختلف من دولة إلى أخرى.

ويمكن أن نخلص أهم عمليات التعامل مع الأنترنت في:

- إتخاد كافة التدابير الوقائية لحماية أفراد المجتمع وحمايته من البيانات الضارة.
- كفالة أمن البيانات والمعلومات وسريتها ومراعات الخصوصية وإحترامها.
- ضمان أن تكون المعلومات التي تقدمها لرفع مستوى المجتمع الإقتصادي والسياسي والإجتماعي.
- ضمان حماية حقوق الملكية الفكرية وقوانين الفضاء الإلكتروني.
- تحرى الضدق والموثوقية والامان في طلب البيانات.
- عدم إشتغلال الحوار عن بعد لغرض التمويه والتنكر وتأجيج نيران الكراهية.

5-3. أمن المعلومات والتشريعات.

إن التشريع بصفة عامة هو مجموع القواعد المكتوبة التي تنضم العلاقات القائمة بين الأطراف المعنية والداخلة فيه ولهذه القواعد القوى الجبرية اللازمة لتنفيده والتقيد به والعقاب في حالة المخالفة ولكي تكون القواعد تشريعا لابد ان تكون مكتوبة حيث يعتبر الدستور في الدول الحديثة هوأعلى مستويات التشريع[215].

---

[215]– قنديل ,يوسف. **نحو إستراتجية لدخول النتاج الفكري باللغة العربية**. تونس ؛ الرياض: مكتبة عبد العزيز العامة , 2001.ص. 535.

بصفة عامة كل مناحي الحياة الإقتصادية و الإجتماعية و السياسية ولحاول المشرع تطوير هذه القواعد من حين لأخر حتى تتماشى مع التطورات الحاصلة في المجتمع وبما أن الجرائم المعلوماتية هي مكن أهم الجرائم التي أفرزتها الثورة المعلوماتية الحالية فإن المشرعين في كافة أنحاء العالم عكفوا على إيجاد تشريعات تهتم بهذه الفئة من الجرائم نظرا للخصوصية التي تكتسيها سواء من حيث طبيعة الفعل أو من حيث مرتكب الجريمة.

5-3-1 تعريف التشريعات الخاصة بالجريمة المعلوماتية:

أطلقت العديد من التسميات على هذه التشريعات منها قوانين جرائم الكمبيوتر, تشريعات الجرائم المعلوماتية وهي توصف بشكل عام بأنها تشريعات حماية أنظمة المعلومات والحماية من استخدامتها الإجرامية وجاءت هذه التشريعات للتصدي لأنشطة إساءة استخدام الكمبيوتر وأنظمة تبادل المعلومات وكذا لمواجهة التحديات في ميدان استخدام الكمبيوتر كوسيلة لإرتكاب الجرائم ؛ وهذه التشريعات هي عبارةعن نصوص قانونية تحدد صور الجرائم والعقوبات إضافة إلى نصوص متعلقة بالمسؤولية الجزائية عند الشروع[216].

ويرجع مبرر هذه التشريعات إلى ماظهر من عجز قوانين العقوبات القائمة عن التطبيق على جرائم الكمبيوتر لأن محل جرائم الكمبيوتر ذو طبيعة معنوية تتمثل في المعلومات في حين أن النصوص القائمة في ميدان السرقة والتدمير والإتلاف تتطلب أن يكون محل الجريمة

ماديا ؛وفي الوقت الحالي تهدف هذه التشريعات إلى تحقيق ثقة عالية قي استخدام شبكات المعلومات في ميدلن أنشطة التجارة والإستمرار الإلكتروني ووصف غرضها العام بتحقيق أمن وحماية المعلومات

5-3-1. التشريعات الخاصة بأمن المعلومات:

إن المعلومات كما يرى العلم البريطاني **John naisbitt** هي مورد الإستراتيجي في مجتمع اليوم لا رأس مال فحسب ؛ وإنتاج المعرفة قد أصبح مفتاح الإنتاجية والمنافسة والإنجاز الإقتصادي وعليه كان لابد من وضع التشريعات اللازمة للحفاظ عليها وحمايتها وأهم هذه التشريعات [217]:

1- **التشريعات الخصوصية:** هناك ثلاث نمادج تشريعية لتدابير حماية الخصوصية المعلوماتية وهذه التدابير تعتمد في تطبيقها على إذا ما كان منطق النظام القانوني مجرد الإعتراف بالخصوصية معتمدا على إباحة كل ما يدخل في نطاق الحق ,وتستخدم وسائل لمواجهة الأنشطة التي تمثل الإعتداء على الخصوصية.

---

[216] – بهاء ,شهين **الأنترنيت والعولنة القاهرة**:عالم الكتب ,1999.ص. 73.

[217]– الجنبيهي ,منير محمد.أمن المعلومات الإلكترونية.المرجع السابق.ص. ص.77-79.

2- **القوانين الشاملة** compréhensive laws: في العديد من دول العالم تمة قوانين عامة تحكم عمليات جمع وإدارة ومعالجة البيانات الشخصية في القطاعين العام و الخاص مع وجود جهة لضمان التواؤم بين القوانين وتطبيقها وهذا هو النمودج الشائع في الدول التي تتبنى حماية البيانات كما هو الحال في دول الإتحاد الأروبي وفي الدول المتعين عليها التوافق مع دليا حماية البيانات الإرشادي الصادر عن الإتحاد الأروبي ولقد وضعت العديد من مثل هذه القوانين في دول خارج الإتحاد الأروبي كما هو الحال في كندا وأسترليا.

3- **القوانين المتخصصة:** وهي التي تتعلق بقطاع معين إذ أن بعض الدول كالولايات المتحدة الامريكية تجنبت سنتشريغ عام للخصوصية وفضلت إصدار قوانين معينة تحكم قطاعات بعينها كما هو الحال بتسجيلات الفيديو والخصوصية المالية وغيرها ؛وفي مثل هذه الحالة فإن إتخاد القواغد القانونية يتحقق من خلال آليات مختلفة وليس كما هو الحال بالنسبة للقانون الشامل والتي تنشأ جهة رقابة عامة , ويأخذ على هذا النموذج أنه يتطلب جهة أمنية تسن تشريعات جديدة كلما نشأت تقنيات جديدة ولهذا فإن الحماية تظل متخلفة عن تقنيات الاعتداد.

4- **لوائح التنظيم الذاتي:**

إن مصطلح التنظيم الذاتي **Autoregulation** يعني إنشاء واحترام إرادي للقواعد المتفق عليها في مجال معين دون رقابة.

وموضوع التنظيم الذاتي للتشريعات هو موقف شأن تقنيات المعلومات عموما , وقد ظهرت الحاجة إلى هذا النموذج في حقول التجارة الإلكترونية ومعايير الخدمات الفنية وحماية البيانات وأمن المعلومات وغيرها , وتضمن لوائح التنظيم الذاتي عموما لوائح تنظيم محتوى الأنترنت وكذلك تنظيم التقنيات وأخلاقيات التعامل مع الأنترنت.

5-3-2قوانين الملكية الفكرية[218]:

وأهم هذه القوانين:

1- **تشريعات حماية برامج الكمبيوتر:**

قوانين الملكية الفكرية في حقل حماية البرمجيات طورت حتى شملت بقية المصنفات الرقمية وقد عكس تطورها الاتجاهات العالمية في إدراج

الملكية الفكرية من تنظيمات التجارة الدولية للتوجه الحاصل نحو الاقتصاد الرقمي والاقتصاد المؤسس على المعرفة ونحو رأس المال الفكري.

---

[218]– [218]– الجنبيهي ,منير محمد.أمن المعلومات الإلكترونية. المرجع السابق ص.81.

2- تشريعات الأصول الإجرائية الجزائية:

هي تشريعات الإثبات المتفقة مع عصر الكمبيوتر والمعلومات التي هي في الحقيقة تطوير لقواعد الإجراءات والإثبات التقليدية واكنها أيضا تتصل عضزيا بالحقوق الجديدة المعترف بها ميدان تقنيات المعلومات

3- تشريعات المحتوى الضار:

ثمة إتجاهين متباينين بين توجه لدمجها مع تشريعات إمكانية المعلومات كما هو في أوروبا أو فصلها عنها كماهو في أمريكا.

4- **تشريعات معايير الأمن المعلومات:**

وهي تعتير إمتداد لتطور تشريعات المواصفات القياسية لتبادل البيانات والتشفير.

5-3-3. **تشريعات الملكية الفكرية**[219]:

1- **تشريعات الإستثمار** : والتجارة والضرائب والجمارك والإتصالات والأظمة الحكومية المتأثرة بتقنية المعلومات.

2- **تشريعات التجارة الإلكترونية**: وتتضمن التوقيع الإلكيروني والتعاقد الإلكتروني والتسوق الإلكتروني.

3- **تشريعات الإختصاص والقانون المطبق على المنازعات القضائية في بيئة المعلومات:**

بشكل خاص منازعات الملكية الفكرية ومنازعات التجارة والأعمال والبنوك الإلكترونية.

إذن وبعد إستعراض أهم القانونية العالمية الصادرة في ما يخص حماية المعلومات ارتأيت أن نستطلع مدى علم طلبة الحقوق في جامعة منتوري قسنطينة على هذه القوانين فكانت النتائج موضحة في الجدول رقم 27 في الصفحة ؟؟؟؟؟؟؟؟؟؟؟

من تحليل نتائج الجدول يتضح لنا أن (60%) من طلبة الحقوق على دراية بالقوانين والتشريعات الدولية المستحدثة لحماية المعلومات، حيث تعتبر الدول الغربية الدول الرائدة في مجال استحداث هذه القوانين والتشريعات وهذا لما شهده هذا العصر من جرائم لا تحصى والتي يكون هدفها المعلومات؛ بينما(40 %) من الطلبة ليسوا على دراية بهذه المستجدات

---

[219]-- الجنبيهي ,منير محمد.أمن المعلومات الإلكترونية. المرجع السابق ص.82.

وهذا قد يكون راجع إلى عدم الاهتمام بمثل هذه المواضيع لحداثتها وعدم انتشارها في الدول العربية عمامة والجزائر خاصة.

5-3. الحماية القانونية للمصنفات الرقمية:

إن تدفق المعلومات وتداولها هي الغاية الجوهرية من وراء شبكة الأنترنت حيث يتم نقل وإرسال المعلومات من مكان إلى آخر وهذه المعلومات هي ملك لأشخاص ونتاج فكرٍ إنساني الذي يجب إحترامه وقد بدأت حماية هذه الأفكارتأخد طابعها القانوني مند القرن الثامن عشر تحت ما يسمى بحقوق الملكية الفكرية ؛والتي تعرف بأنها حقوق دهنية أو حق الملكية الفكرية لتأليف ما.

ونظرا لتطور أوعية المعلومات التي أصبحت تعتمد الوسائل الرقمية كان لزاما على المشرعين والمهتمين بحقوق التأليف تطوير حقوق التأليف لتشمل الأعمال الرقمية قصد مسايرة العصر والوسائل المستجدة وهي قضية تثير جدلا واسعا في اوساط القانونيين والوالناشرين والمكتبيين والمستفيدين.

وب ع ميلاد شبكة المعلومات الدولية المعروفة بالأنترنت ظهرت بعض المشاكل تتعلق بيطبيق حقوق الملكية الفكرية والعلامات الصناعية والتجارية على هذه الشبكة للأسباب التالية :[220]

– تغيير شكل وأسلوب إخراج وعرض المصنفات حيث أصبح الأمر يتعلق الأمر بمنظومة بيانات يتم نشرها علىالأنترنت يتم نشرها ويمكن نسخها وتحويلها بسرعة وسهولة فائقة , ويستطيع ملايين الأشخاص الحصول على نسخة كاملة من المصنف في الحال.

– إن شبكة الأنترنت مفتوحة ومترامية الأطراف تتمتع بحرية إنسياب المعلومات دون ان تحكمها أي سلطة مركزية ومن ثم لا توجد جهة محددة لتفصي عمليات التقليد والنسخ الذي يشكل مساسا بحق المولف , فقد إنتشرت يلك الممارسات وإنتشرت وباتت تشكل خطورة كبيرة خصوصا على الموديلات والماركات.

– أن قانون الملكية الفكرية لايصلح لمواجهة التحديات الجديدة.

المصنفات التي تتمتع بالحماية على الأنترنت:

---

[220]– منصور ,محمد حسين. **المسؤولية الإلكترونية..الإسكندرية**:دار الجامعة الجديدة ,2003.ص..313.

إن تشريعات حماية حق المؤلف تسري على كل المبتكرات أيا كان موقعها وصورتها , وأيا كانت الاداة التي يتم التعبير عتها من خلالها , ومن تم فهي تحمي كافة صور التعبير عن الأفكار والمعلومات بما في ذلك برامج الحاسبات الآلية وبنوك المعلومات ومن محل الحماية :[221]

– المصنف المكتوب:حيث تتمتع كافة المصنفات المكتوبة بحماية حق المؤلف على الأنترنت , ويدخل في ذلك الكتب والكتيبات والمقالات والنشرات وغيرها من المصنفات المكتوب مثل البريد الإلكتروني وملحقاته.

– المصنفات الموسيقية المسوموعة والمرئية المقترنة بالألفاظ وغير المقترنة والمصنفات السمعية البصرية كالأفلام والمقطوعات الموسيقية المارة بالأنترنت والمودعة عليه.

– الصور التي تمر عبر الأنترنت ومن ثم فإن نشر الصورة إلكترونيا يمثل تعديا على حق المؤلف ويدخل في ذلك الرسم بالخطوط أو الألوان والنحت والطباعةعلى الحجر وعلى الأقمشة ولأية مصنفات مماثلة في مجال الفنون الجميلة والمواصفات الفوتوغرافية ومواصفات الفن التشكيلي والتركيبي

– الصور التوضيحية والخرائط الجغرافية والرسومات التخطيطية والمصنفات الثلاثية الأبعاد المتعلقة بالجغرافيا أو الطبوغرافيا أو التصميمات المعمارية

– المصنفات المشتقة وذلك دون الإخلال بالحماية المقرونة للمصنفات التي شتقت منها والمصنف المشتق هو الذي يستمد أصله من مصنف سابق الوجود كالترجمات والتجميعات بما في ذلك قواعد البيانات وساء في الحاسب أو غيره

– مصنفات العمارة وذلك ببرنامج الحاسب الآلي

– قواعد البيانات وساء كانت مقروءة من الحاسب الآلي أو من غيره ويكون الكثير من هذه القواعد منشورا على الأنترنت.

المعاهدات والقوانين الخاصة بحماية حق الملكية الفكرية:

تعتبر حماية الملكية الفكرية من أكبر الحقوق التي يتم إنتهاكها يوميا على شبكة الأنترنت وعليه فوجود معاهدات دولية تمنع تلك الإنتهاكات وإصدار كل دولة قوانين خاصة بها أمر ضروري وقد عقدت عدة معاهدات تنص على حماية الملكية نحاول إيجازها فيما يلي:[222]

---

[221]– منصور ,محمد حسين. المسؤولية الإلكترونية.المرجع السابق.ص.318.

[222]الجنبيهي منير محمد. جرائم الأنترنت والحاسب الآلي. المرجع السابق. ص 116

1- **معاهدة برن:**

تعتبر هذه المعاهدة والتي تم التوقيع عليها عام 1971 في سويسرا حجر الأساس في مجال الحماية الدولية لحق المؤلف وقد وقعت الإتفاقية 120 دولة ونصت على منح أصحاب المؤلف حق إستشاري في التصريح بعمل نسخ بأي طريقة

2- **معاهدة تربس** :وتعتبر هذه المعاهدة كذلك من بين المعاهدات التي تم عقدها في مجال حماية الملكية الفكرية من السطو عليها خصوصا بعد إنشار عمليات السطو الإلكتروني وقد تم التوقيع عليها سنة 1994 وقد إهتمت الإتفاقية بالجوانب التجارية التي لها علاقة بالملكية الفكرية

3- معاهدات الوبيو:

وقد ضمت هذه المعاهدات ثلاث مجموعات [223]:

- معاهدة الوبيو بشأن حق المؤلف , معاهدة الوبيو بشأن الآداء والتسجيل الصوتي , معاهدة الوبيو بشأن الحماية الدولية لحق المؤلف والحقوق المجاورة.

- معاهدة الوبيو بشأن حق المؤلف: وقد وقعت هه المعاهدة في ديسمبر 1996 وتتكون من ثمانية عشر مادة , تبدأ بالديباجة ثم تتنارل علاقة تلك المعاهدة بمعاهدة برن ثم تتعرض لنطاق تطبيق الحماية حق المؤلف كحق التوزيع أو الأجير ونقل المصنف والإلتزامات المتعلقة بالتكنولوجيا ومدة الحماية والإستثناءات.

- معاهدة الوبيو بشأن بشأن الآدىء والتسجيل الصوتي: ثم التوقيع غليها في ديسمير 1996 وتقع في أربعة فصول يتناول الفصل الأول علاقة المعاهدة بالمعاهدات الأخرى أما الفصل الثاني فيتناول حقوق فنانوا الآداء معنويا وماديا وحقةق الإستنساخ والتوزيع والتأجير.

- معاهدة الوبيو بشأن حقوق المألف والحقوق المجاورة يبدأ بمقدمة ثم تناول الطابع القانوني للمعاهدة وعلاقتها بمعاهدات أخرى ثم إتفاقية جدول الأعمال الرقمي.

3 – لالمكافحة القانونية للجرائم الإلكترونية:

3-1 لالمعاهدات والمؤتمرات الدولية لمكافحة الجرائم الإلكترونية:

تعد المعاهدات الدولية هي الأساس الذي يرتكز عليه التعاون الدولي في مجال مكافحة الجرائم الإلكترونية وقد تم عقد العديد من المعاهدات التي تعمل على تنسيق التعاون في ما يخص مكافحة الجرائم الإلكترونية ومن تلك المعاهدات:

---

[223] المرجع نفسه. ص 119.118.

* معاهدة بودابستBUODAPESTلمكافحت جرائم الأنترنت:

شهدت العاصمة المجرية بودابست في أوخر عام 2001 ميلاد أول المعاهدة الدولية التي تكافح جرائم الأنترنت , وتبلورت التعاون الدولي في محابتها ومحاولة الحد منها خاصة

للمعاهدات والمؤتمرات الدولية

تعد المعاهدات الدولية هي الأساس الذي يتركز عليه التعاون الدولي في مجال مكافحة الجرائم الإلكترونية وقد تم عقد العديد من المعاهدات التي تعمل على التعاون الدولي في مجال مكافحة الجرائم الإلكترونية ومن تلك المعاهدات:

- معاهدة بودابست لمكافحة جرائم الأنترنت **Budapest:**

شهدت العاصمة المجرية بودابست في أواخر عام 2001 م أول المعاهدات الدولية التي تكافح جرائم الأنترنت وتبلور التعاون الدولي في محاربتها ومحاولة الحد منها خاصة بعد أن وصلت تلك الجرائم إلى حد خطير حيث أصبحت تهدد الأشخاص والممتلكات وبعد التوقيع على تلك الإتفاقية من مسؤولين في الدول الأروبية إضافة إلى أمريكا واليابان وكندا وجنوب أفريقيا هو نتاج مباثات ومفاوضات إستغرقت ما يزيد عن أربعة أعوام حتى يتم التوصل إلى الصيغة النهائية المناسبة لتلك الإتفاقيات حتى يتم التوقيع عليها من طرف جميع الأطراف دون إعتراض وقد كان الخلاف الوحيد هو مجال محاربة العنصرية ومن المعروف أن هذه الجريمة يعاقب عليها القانون الدولي ولابد من النص في الإتفاقية على لزوم العمل على إزالة تلك المواقع التي على التحريض على الكراهية ومن ضمن الجوانب العديدة التي تناولت تلك الإتفاقيات الإرهاب الإلكتروني وعمليات تزوير بطاقات الإئتمان ودعارة الأطفال وتلك الجرائم تعتبر من أكثر الجرائم إنشارا على المستوى العالمي بصة عامة وأروبا بصفة خاصة وتحدد الإتفاقية أفضل الطرق الواجب إتباعها في التخفيف من جرائم الأنترنت [224]

- المعاهدة الأروبية لمكافحة جرائم الأنترنت:

وقعت اللجنة الخاصة المعنية بقضابا الجريمة بتكليف من المجلس الأروبي علىالمسودة النهائية لمعاهدة شاملة تهدف إلى مساعدة البلدان في مكافحة الجرائم وسط إنقادات من دعاة حماية الحرية الشخصية وبعد أن يتم المصادقة المصادقة عليها من قبل رئاسة المجلس وتوقيعها من البلدان المعنية تستلزم الإتفاقية الدول الموقعة عليها بين الحد الأدنى من القوانين الضرورية للتعامل نع جرائم التقنيةالعالية بما في التحول غير المصرح به ألى الشبكة [225].

---

[224]- الجنبيهي منير محمد. جرائم الأنترنت والحاسب الآلي ووسائل مكافحتها المرجع السابق. ص.9796.

[225]المرجع نفسه ص 104 -

3-الجهود الدولية لمواجهة جرائم المعلوماتية

إتجهت كافة الدول المتقدمة تكنولوجيا إلى إستحدات نصوص قانونية جديدة تجرم الجرائم الإلكترونية[226]:

*** على المستوى العالمي:**

تعتبر دولة السويد من أوائل الدول التي إتجهت إلى سن تشريعات قانونية جديدة خاصة بجرائم الأنترنت والحاسب الآلي لتستطيع ان تعاقب المهتتمين بإرتكاب مثل هذه الجرائم ؛ حيث صدر أول قانون خاص ويسمى بقانون البيانات وقد صدر هذا القانون عام 1973 وقد عالج هذا القانون قضايا الإحتلال عن طريق الأنترنت؛ وفي عام 1989 صدر قانون آخريحمل رقم 1213 عرف كافة المصطلحات الضرورية لتطبيق القانون على الجرائم المعلوماتية.

وقد خولت وزارة العدل الأمريكية عام2000 خمس جهات حكومية للتعامل مع جرائم الأنترنت منها مكتب التحقيقات الفدرالية **FBI** .

أما بريطانيا فهي ثالث دولة تسن قانون خاص بها لجرائم الأنترنت والحاسب وهذا عام 1981.

أما فرنسا فقد طورت قولنينها الجنائية للتوافق مع المستجدات الإجرامية حيث أصدرت قانون خاص بها سنة1988 ؛ وقد سارت العديد الطرق على نفس النهج حيث عدلت كل من هولندا وألمانيا وبولندا قوانينها لتتماشى مع هذه الجرائم.

*** على المستوى العربي** [227]:

أما الحال في الدول العربية فإنه وللأسف لا توجد أي دولة عربية قامت بسن قوانين جديدة أو قامت بتحديث قوانينها الخاصة لتستوعب تلك المستجدات الإجرامية فالدول العربية مازالت بعيدة كل البعد عن عن ذلك التطور القانوني الذي يحاول اللحاق بالتطورالإجرامي ؛ أما الأمر في المملكة العربية السعودية فلا توجد نفس المشاكل على أساس أن كافة التشريعات تنطلق من الشريعة الإسلامية وبالتالي فهي لاتحتاج إلى تحديث , فالشريعة الإسلامية صالحة لكل زمان ومكان, وقد إتخدت مدينة الملك عبد العزيز للعلوم والتقنية من خلال وحدة الأنترنت المشرفة على عمل مقدمي خدمة الأنترنت عددا من الإجراءات الفنية التي تهدف إلى محاصرة أعمال المخربين والميسللين ومن بين هذه الإجراءات:

- منع إنتحال أرقام الأنترنت.

---

[226]– الجنبيهي منير محمد. جرائم الأنترنت والحاسب الآلي ووسائل مكافحتها المرجع السابق.ص. 102.

[227]– الجنبيهي منير محمد. المرجع نفسه. ص.107.

- العمل على منع إستءة استخدام البريد الإلكتروني.

3-3 الجهود العربية لمكافحة الجريمة الإلكترونية [228]:

لعل من أبرز ما يمكن أن يقال عن الجهود العربية المبدولة من أجل الحماية من جرائم الحاسب إعتماد مجلس وزراء العدل العرب للقانون العربي الموحد كقانون نمودجي بموجب القرار رقم 229 وبالرجوع إلى المذكرة الإيضاحية لهذا القانون نجد أن الباب السابع الخاص بالجرائم ضد الإشخاص الناتج عن المعالجات المعلوماتية حيث على وجوب حماية الحياة الخاصة الأسرار من أخطار المعالجة الإلكترونية ؛أما المادة 464 فقد نصت على عقابمن يقوم بفعل الدخول بطريقة الغش إلى نظام أوجزء من نظام المعالجة الألية وتعد هذه المحاولة بالرغم من تواضعها من أبرز ما ثم على صعيد تعزيز التعاون على المستوى العربي من الناحية التشريعية

وتكللت الجهود العربية في إطار الحماية الفكرية وحق المؤلف خصوصا في إبرام الإتفاقية العربية لحماية حقوق المؤلف التي أوصى بها مؤتمر الوزراء المسؤولين عن الشؤون الثقافية المنعقد في بغداد عام 1981 ؛ كذلك فإن الجمعية المصرية للقانون الجنائي لها إتجاه محمود في هذا الموضوع وتمثل ذلك في مؤتمرها السادس في القاهرة من 25-28 أكتوبر عام 1993 حول جرائم الكمبيوتر والجرائم الأخرى التي أكد المؤتمرون على عالميتها ووجوب تكاثف الجهود لمكافحتها لأنها تمثل وجها سلبيا للتقدم الحضاري ؛ وقد خرجج المؤتمرون بصور السلوك الإجرامي وتوصيات بضرورة التعاون الدولي في مجال أنظمة المعلومات.

إلى جانب هذه الجهود هناك جهود أخرى تتض ح معالمها في الجهود المتعلقة بالملكية الفكرية كالمؤتمر الدولي الأول للملكية الفكرية سنة 1995 ؛ كما عقد في بغداد مؤتمرين لمستجدات الملكية الفكرية سنة 1997 ومن توصيات المؤتمر إنشاء محاكم خاصة للبث في النزاعات المتعلقة بالحماية ؛وبعدها عقد المؤتمر الثاني للملكية الفكرية عام 1998.

وكما سبق الإشارة إليه فإن الجرائم المعلوماتية الحديثة طرحت مشاكل كبيرة من الناحية القضائية وذلك لعدم تناسب القوانين القديمة مع هذه المستجدات ومحاولة لمعرفة إذا ما كان المشرع الجزائري يعاني من مشاكل عند عرض هذا النوع من القضايا على المحاكم وكانت الإجابة كما يوضحه الجدول 28 في الصفحة 148

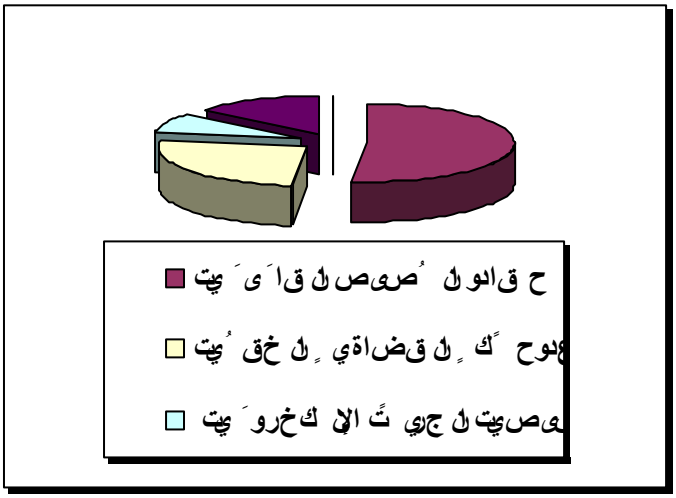
إذن وحسب نتائج الجدول فإن اغلب الطلبة (66,6%) ليسوا على دراية إن كان المشرع الجزائري يتعرض لمشاكل عند طرح القضايا المعلوماتية على المحاكم ، وهذا راجع إلى قلة هذه القضايا في الجزائر من جهة وعدم محاولة الطلبة التعرف على المستجدات الحاصلة في مصرح

---

[228]- عبابنة , محمود محمد.**جرائم الحاسب وأبعادها الدولية**.عمان:دار الثقافة,2005.ص.180.

الجريمة والتشريعات من جهة أخرى؛ أما (33,3%) يرون أن المشرع الجزائري تعترضه العديد من المشاكل والعراقيل عند الفصل في مثل هذه القضايا أما عن أسباب هذه المشاكل فيرجعها الطلبة إلى الأسباب الموضحة في الجدول رقم 27 (أنظر الصفحة 148)

إذن فإن الطلبة يرون بأن القاضي معرض للمشاكل وعراقيل عند الفصل في قضايا المعلوماتية أما عن مرد هذه المشاكل فهي تقادم النصوص القانونية (60%)، ذلك لأن القوانين والتشريعات الجزائرية تعد قديمة ولا تتماشى مع التطورات الحاصلة على ساحة الجريمة وبالتالي خلق صعوبة تطبيق هذه القوانين على الجرائم التي استحدثتها البيئة الإلكترونية؛ كما يرى (60%) من الطلبة ان سبب هذه المشاكل يرجع إلى عدم تمكن القضاة من التقنيات الحديثة،وهذا راجع إلى حداثة دخول الانترنت إلى الجزائر،ومنه فإن أغلب القضاة لدينا تنقصهم الخبرة والتجربة في ما يتعلق بمثل هذه التقنيات وبالتالي يصعب عليهم الفصل فيها كما أن خصوصية هذه الجرائم تؤدي على خلق عراقيل للقضاة؛والشكل البياني التالي يوضح هذه النسب:



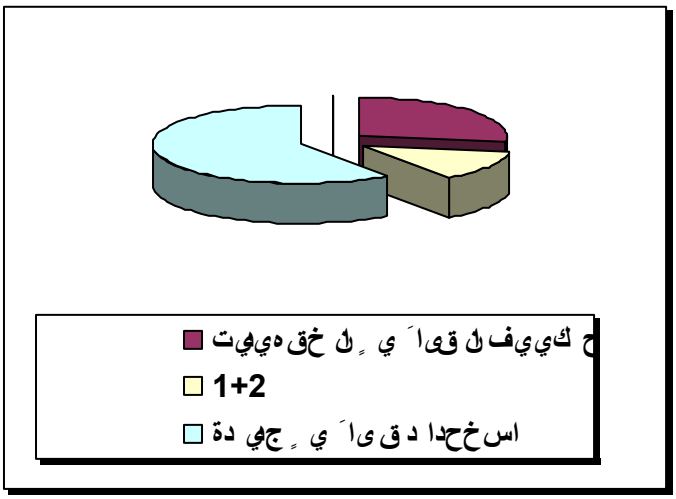
الشكل رقم: 19 أسباب المشاكل التي تعترض القضاة في الفصل في القضايا المعلوماتي

ومن اجل تدارك النقص في التشريعات الجزائرية فيما يخص تشريعات حماية المعلومات ،حاولنا معرفة إذا كانت هناك مساعي لاحتواء مثل هذه الجرائم من خلال سؤال الطلبة وكانت الإجابة كما هي موضحة في الجدول رقم30 الصفحة 149

ومن تحليل نتائج الجدول السابق نلاحظ أن أغلب الطلبة (66,6%) ليسوا على دراية إن كانت هناك مساعي أو مشاريع لاستحداث أو تطوير القوانين أو المراسيم من أجل احتواء ظاهرة الإجرام المعلوماتي، والتي أصبحت بحق جرائم العصر التي تهدد المجتمع الكوني ككل ؛ أما (20%) من عينة الدراسة فقد نفوا وجود أي مساعي لإحداث تغييرات على القوانين في الوقت الراهن إلا أن الغد كفيل بأن تتغير هذه النظرة خصوصا وأن هذه الجرائم في توسع

رهيب ولم يسلم منها أحد غي العالم، أما عند محاولة معرفة اقتراحات الطلبة من أجل حل هذه المشكلة كانت الإجابة كما هو موضح غي الجدول رقم 31 الصفحة149

إذن فإن أغلب الطلبة (60%) يرون أن أحسن حل لاحتواء ظاهرة الإجرام المعلوماتي هو استحداث قوانين جديدة وهذا باعتبار أنه الاختيار الأنجع؛ لأن هذه الطاهرة جديدة وتحتاج إلى حلول جذرية تستطيع الإلمام بكل جوانبها ولا تحتاج إلى حلول مؤقتة أو هامشية؛ أما (26%) من الطلبة فيرون أن تكييف القوانين التقليدية يعتبر كافيا لاحتواء الجرائم الحديثة؛ أما باقي الطلبة فإن الحل بالنسبة لهم هو تعديل وتكييف فالقوانين التقليدية في مواضع معينة واستحداث أخرى في مواضع حيث لا مجال للتعديل وهذا الحل هو الأقرب للصواب والشكل البياني التالي يوضح ذلك:



الشكل رقم:20 اقتراحات الطلبة حول احتواء ظاهرة الإجرام المعلوماتي

الجامعات. لهذا فالشبكة ليست آمنة في تصميمها وبناءها. لكن مع توسع إستخدام الشبكة ودخول جميع فئات المجتمع إلى قائمة المستخدمين بدأت تظهر جرائم على الشبكة إزدادت مع الوقت وتعددت صورها وأشكالها. وفيما يلي إستعراض لعدد من جرائم الإنترنت:

أولا: صناعة ونشر الفيروسات: وهي أكثر جرائم الإنترنت إنتشارا وتأثيرا. إن الفيروسات كما هو معلوم ليست وليدة الإنترنت فقد أشار إلى مفهوم فيروس الحاسب العالم الرياضي المعروف "فون نيومن"في منتصف الأربعينات الميلادية. لم تكن الإنترنت الوسيلة الأكثر استخداما في نشر وتوزيع الفيروسات إلا في السنوات الخمس الأخيرة، حيث أصبحت الإنترنت وسيلة فعالة وسريعة في نشر الفيروسات. ولا يخفى على الكثير سرعة توغل ما يسمى بـ "الدودة الحمراء" حيث استطاعت خلال أقل من تسع ساعات اقتحام ما يقرب من ربع مليون جهاز في 19 نوفمبر2001 م. إن الهدف المباشر للفيروسات هي المعلومات المخزنة على الأجهزة المقتحمة حيث تقوم بتغييرها أو حذفها أو سرقتها و نقلها إلى أجهزة أخرى.

ثانيا: الإختراقات : تتمثل في الدخول غير المصرح به إلى أجهزة أو شبكات حاسب آلي ؛ وجل عمليات الإختراقات (أو محاولات الإختراقات) تتم من خلال برامج متوفرة على الإنترنت يمكن لمن له خبرات تقنية متواضعة أن يستخدمها لشن هجماته على أجهزة الغير، وهنا تكمن الخطورة؛ تختلف الأهداف المباشرة للإختراقات، فقد تكون المعلومات هي الهدف المباشر حيث يسعى المخترق لتغيير أو سرقة أو إزالة معلومات معينة؛ وقد يكون الجهاز هو الهدف المباشر بغض النظر عن المعلومات المخزنة عليه، كأن يقوم المخترق بعمليته بقصد إبراز قدراته "الإختراقيه" أو لإثبات وجود ثغرات في الجهاز المخترق ؛ من أكثر الأجهزة المستهدفة في هذا النوع من الجرائم هي تلك التي تستضيف المواقع على الإنترنت، حيث يتم تحريف المعلومات الموجودة على الموقع أو ما يسمى بتغيير وجه الموقع(Defacing) ؛ إن استهداف هذا النوع من الأجهزة يعود إلى عدة أسباب من أهمها كثرة وجود هذه الأجهزة على الشبكة، وسرعة إنتشار الخبر حول اختراق ذلك الجهاز خاصة إذا كان يضم مواقع معروفة.

ثالثا: تعطيل الأجهزة: كثر مؤخراً إرتكاب مثل هذه العمليات، حيث يقوم مرتكبوها بتعطيل أجهزة أو شبكات عن تأدية عملها بدون أن تتم عملية إختراق فعلية لتلك الأجهزة , تتم عملية التعطيل بإرسال عدد هائل من الرسائل بطرق فنية معينة إلى الأجهزة أو الشبكات المراد تعطيلها الأمر الذي يعيقها عن تأدية عملها, من أشهر الأمثلة على هذا النوع من الجرائم تلك التي تقوم بتعطيل الأجهزة المستضيفة للمواقع على الشبكة ؛ إن الأسباب وراء إستهداف هذا النوع من الأجهزة تماثل أسباب استهدافها في جرائم الاختراقات والتي سبق ذكرها جميع الجرائم التي ذكرناها تستهدف بشكل مباشر معلومات أو أجهزة وشبكات حاسبات.

أما جرائم الإنترنت التي تستهدف جهات سواء كانوا أفراداً أو مؤسسات، ففيما يلي عرض لبعضها :

رابعاً: انتحال الشخصية: هي جريمة الألفية الجديدة كما سماها بعض المختصين في أمن المعلومات وذلك نظراً لسرعة إنتشار إرتكابها خاصة في الأوساط التجارية. تتمثل هذه الجريمة في استخدام هوية شخصية أخرى بطريقة غير شرعية، وتهدف إما لغرض الاستفادة من مكانة تلك الهوية (أي هوية الضحية) أو لإخفاء هوية

شخصية المجرم لتسهيل ارتكابه جرائم أخرى, إن إرتكاب هذه الجريمة على شبكة الإنترنت أمر سهل وهذه من أكبر سلبيات الإنترنت الأمنية، وللتغلب على هذه المشكلة، فقد بدأت كثير من المعاملات الحساسة على شبكة الإنترنت كالتجارية في الاعتماد على وسائل متينة لتوثيق الهوية كالتوقيع الرقمي والتي تجعل من الصعب إرتكاب هذه الجريمة.

خامساً: المضايقة والملاحقة: تتم جرائم الملاحقة على شبكة الإنترنت غالباً باستخدام البريد الإلكتروني أو وسائل الحوارات الآنية المختلفة على الشبكة , تشمل الملاحقة رسائل تهديد وتخويف ومضايق ؛ تتفق جرائم الملاحقة على شبكة الإنترنت مع مثيلاتها خارج الشبكة في الأهداف والتي تتمثل في الرغبة في التحكم في الضحية، تتميز جرائم المضايقة والملاحقة على الإنترنت بسهولة إمكانية المجرم في إخفاء هويته علاوة على تعدد وسهولة وسائل الاتصال عبر الشبكة، الأمر الذي ساعد في تفشي هذه الجريمة ؛ من المهم الإشارة إلى أن كون طبيعة جريمة الملاحقة على شبكة الإنترنت لا تتطلب اتصال مادي بين المجرم والضحية لا يعني بأي حال من الأحوال قلة خطورتها فقدرة المجرم على إخفاء هويته تساعده على التمادي في جريمته والتي قد تفضي به إلى تصرفات عنف مادية علاوة على الآثار السلبية النفسية على الضحية.

سادساً: التغرير والاستدراج: غالب ضحايا هذا النوع من الجرائم هم صغار السن من مستخدمي الشبكة ؛ حيث يوهم المجرمون ضحاياهم برغبتهم في تكوين علاقة صداقة على الإنترنت والتي قد تتطور إلى التقاء مادي بين الطرفين, إن مجرمي التغرير والاستدراج على شبكة الإنترنت يمكن لهم أن يتجاوزوا الحدود السياسية فقد يكون المجرم في بلد والضحية في بلد آخر وكون معظم الضحايا هم من صغار السن، فإن كثير من الحوادث لا يتم الإبلاغ عنها حيث لا يدرك كثير من الضحايا أنهم قد ُغرر بهم.

سابعاً: التشهير وتشويه السمعة: يقوم المجرم بنشر معلومات قد تكون سرية أو مضللة أو مغلوطة عن ضحيته، والذي قد يكون فرداً أو مجتمع أو دين أو مؤسسة تجارية أو سياسية. تتعدد الوسائل المستخدمة في هذا النوع من الجرائم، لكن في مقدمة قائمة هذه الوسائل إنشاء موقع على الشبكة يحوي المعلومات المطلوب نشرها أو إرسال هذه المعلومات عبر القوائم البريدية إلى أعداد كبيرة من المستخدمين.

ثامناً: صناعة ونشر الإباحية: لقد وفرت شبكة الإنترنت أكثر الوسائل فعالية وجاذبية لصناعة ونشر الإباحية؛ إن الإنترنت جعلت الإباحية بشتى وسائل عرضها من صور وفيديو وحوارات في متناول الجميع، ولعل هذا يعد أكبر الجوانب السلبية للإنترنت خاصة في مجتمع محافظ على دينه وتقاليده ؛ إن صناعة ونشر الإباحية تعد جريمة في كثير من دول العالم خاصة تلك التي تستهدف أو تستخدم الأطفال ؛ لقد تمت إدانة مجرمين في أكثر من مائتي جريمة في الولايات المتحدة الأمريكية خلال فترة أربع سنوات والتي انتهت في ديسمبر 1998م، تتعلق هذه الجرائم بتغرير الأطفال في أعمال إباحية أو نشر مواقع تعرض مشاهد إباحية لأطفال.

تاسعاً: النصب والاحتيال :أصبحت الإنترنت مجالاً رحباً لمن له سلع أو خدمات تجارية يريد أن يقدمها، وبوسائل غير مسبوقة كاستخدام البريد الإلكتروني أو عرضها على موقع على الشبكة أو عن طريق ساحات الحوار؛ ومن الطبيعي أن ُيساء استخدام هذه الوسائل في عمليات نصب واحتيال ؛ ولعل الذي يستخدم البريد

الإلكتروني بشكل مستمر تصله رسائل بريدية من هذا النوع. إن كثيراً من صور النصب والاحتيال التي يتعرض لها الناس في حياتهم اليومية لها مثيل على شبكة الإنترنت مثل بيع سلع أو خدمات وهمية، أو المساهمة في مشاريع استثمارية وهمية أو سرقة معلومات البطاقات الائتمانية واستخدامها ؛ وتتصدر المزادات العامة على البضائع عمليات النصب والاحتيال على الإنترنت ؛ إن ما يميز عمليات النصب والاحتيال على الإنترنت عن مثيلاتها في الحياة اليومية هي سرعة قدرة مرتكبها على الاختفاء والتلاشي. بعد هذا العرض لعدد من أنواع جرائم الإنترنت.

1-3-4. الفيروســــــــــــــــــــــات[229]:

أصبح الحديث عن الفيروسات من الأمور الطبيعية بل أن الكثير ممن لديهم حاسبات شخصية ربما يكونون قد تعرضوا لأذى تلك الفيروسات إذا ما علمنا أن هناك أكثر من20 ألف فيروس معروف في الوقت الحاضر. ونحاول من خلال هذا العنصر تسليط الضوء على الفيروسات بأنواعها المختلفة وكيفية الوقاية منها عن طريق أشهر برامج الحماية"Antivirus Programs " المجاني منها والتجاري علما بأن الدراسات تقول: أن 40% فقط ممن يستخدمون الحاسبات الشخصية في المكاتب أو المنازل لديهم برامج حماية من الفيروسات، ويأتي حديثنا هذا متصلا لكون الكثير من المستخدمين بدؤوا يلحظون انتشار الفيروسات في الوقت الحاضر خاصة أثناء عملية جلب البرامج DownLoad مثل الألعاب والبرامج المجانية، كما أن الفيروسات يمكن أن تصيب جهازك أثناء قراءتك أو من خلال مرفقات بريدك الالكتروني .

و الفيروس الحاسوبي Computer Virus عبارة عن برنامج Software مخفي لا يمكن رؤيته من خلال برامج الاستعراض كتب بعناية ليكون قادرا على الدخول إلى نظامك الحاسوبي بشكل سري Surreptitiously وقد يُصيبُ بعض ملفاتكَ بالأذى والتخريب أو قد يكتفي بعرض رسالة ما تلبث أن تذهب؛ عموما يمكن القول أن أي برنامج يهدف إلى إلحاق الأذى بأنظمة وملفات الغير يسمى فيروسا، عادة ما يقوم الفيروس بإعادة نفسه (تكرار نفسه Replicate Itself) وإصابة اكبر قدر من الملفات وهنا تكمن الخطورة، وكثيراً ما توصف الفيروسات على أنها سريعة الانتشار أي أنها تنتقل من نظام أو وسط تخزيني لآخر بسرعة كبيرة. على سبيل المثال لنفترض أن حاسبا شخصيا مصاباً بفيروس من الفيروسات ثم قمت بحفظ بعض الملفات من ذلك الجهاز إلى قرص مرن أو قرص CD أو أرسلت منه ملفاً عبر البريد الالكتروني أو عبر برامج الاتصال مثل ICQ فإن الجهاز المستقبل سيصاب بذلك الفيروس وهكذا تتسع دائرة الإصابة إلا إذا تم القضاء على ذلك الفيروس بواسطة أحد برامج الحماية القوية.

أنواع الفيروسات

تظل حرب الفيروسات مستعرة ودائما ما توصف بأنها الحرب التي لا يمكن أن تقف بل أن إتهامات

---

[229]– **فيروسات الحاسب أنماطها وأعراضها وطرق الوقاية منها**. [على الخط المباشر].زيارة يوم :2006/02/12.متوفر على الموقع:**http://www.al-jazirah.com.sa/services**

تقول أن الشركات المنتجة للبرامج وحفاظا على حقوقها تقوم بصنع فيروسات تظهر فور استخدام نسخ غير أصلية من تلك البرامج، وهذا الكلام لا يستطيع أحد أن يثبت صحته من عدمها لكن الفيروسات موجودة ويجب علينا كمستخدمين للحاسبات أن نقي أنفسنا من شرورها وأضرارها وحتى نفعل ذلك يجب أن نعرف أنواعها حيث إشتهرت منها أربعة أنواع هي على النحو التالي :

- فيروسات قطاع إعادة التحميل Boot sector viruses
- فيروسات البرامج أو الملفات Program Or File Viruses
- فيروسات الماكرو Macro Viruses
- فيروسات متعددة الأطراف Multipartite Viruses

وتسبب الفيروسات في عدة أعراض تتراوح من كونها مجرد رسالة أو عدة رسائل تظهر فجأة ثم سرعان ما تختفي أو أن تقوم بحذف بعض البرامج أو حذف قطاع التحميل أو تدمير كامل القرص الصلب وبالتالي تخسر كل المعلومات والبرامج التي به.

- ظهور رسائل غريبة على شاشة حاسوب، آو أصوات غريبة أو موسيقى صاخبة تنبعث من الجهاز في أوقات متفرقة .
- كثرة ظهور رسائل انتهاء الذاكرة Run Out of Memory أو المساحة التخزينة.
- تغيير إسم الجهاز .
- عدم وجود تطبيقات كانت في السابق تعمل بالجهاز.
- بطء الحاسب الآلي عن السرعة المعتادة .
- بطء الحاسب في أداء بعض المهمات البسيطة كان يأخذ وقتا طويلا في عملية حفظ وثيقة عبارة عن سطرين أو ثلاثة.

1-3-4. أمن المعلومـــــــــات:

إن شبكة الإنترنت كشبكة معلوماتية ينطبق عليها النموذج المعروف لأمن المعلومات ذو الأبعاد الثلاثة وهي:

1. سرية المعلومات: وذلك يعني ضمان حفظ المعلومات المخزنة في أجهزة الحاسبات أو المنقولة عبر الشبكة وعدم الإطلاع عليها إلا من قبل الأشخاص المخولين بذلك.

2. سلامة المعلومات: يتمثل ذلك في ضمان عدم تغيير المعلومات المخزنة على أجهزة الحاسب أو المنقولة عبر الشبكة إلا من قبل الأشخاص المخولين بذلك.

3 .وجود المعلومات: وذلك يتمثل في عدم حذف المعلومات المخزنة على أجهزة الحاسب إلا من قبل الأشخاص المخولين بذلك.

إن جرائم الإنترنت ليست محصورة في هذا النموذج، بل ظهرت جرائم لها صور أخرى متعددة تختلف باختلاف الهدف المباشر في الجريمة. إن أهم الأهداف المقصودة في تلك الجرائم هي كالتالي:

1. المعلومات: يشمل ذلك سرقة أو تغيير أو حذف المعلومات، ويرتبط هذا الهدف بشكل مباشر بالنموذج الذي سبق ذكره.

2 .الأجهزة: ويشمل ذلك تعطيلها أو تخريبها.

3. الأشخاص أو الجهات: تهدف فئة كبيرة من الجرائم على شبكة الإنترنت أشخاص أو جهات بشكل مباشر كالتهديد أو الابتزاز؛ علماً بأن الجرائم التي تكون أهدافها المباشرة هي المعلومات أو الأجهزة تهدف بشكل غير مباشر إلى الأشخاص المعنيين أو الجهات المعنية بتلك المعلومات أو الأجهزة. بقي أن نذكر أن هناك جرائم متعلقة بالإنترنت تشترك في طبيعتها مع جرائم التخريب أو السرقة التقليدية، كأن يقوم المجرمون بسرقة أجهزة الحاسب المرتبطة بالإنترنت أو تدميرها مباشرة أو تدمير وسائل الاتصال كالأسلاك والأطباق الفضائية وغيرها. حيث يستخدم المجرمون أسلحة تقليدية إبتداء من المشارط والسكاكين وحتى عبوات متفجرة، وكمثال لهذا الصنف من الجرائم قام مشغل أجهزة في إحدى الشركات الأمريكية بصب بترين على أجهزة شركة منافسة وذلك لإحراقها حيث دمر مركز الحاسب الآلي الخاص بتلك الشركة المنافسة برمتها[230].

أصبحت قضية الأمن، التي تؤرق العالم؛ شرقه وغربه، الهم الأكبر والشغل الشاغل للمتعاملين مع الشبكة العنكبوتية العالمية " الإنترنت "، سواء أكانوا أفرادا أم مؤسسات أم مجموعات ــ groups. وبات المتعاملون مع الشبكة العنكبوتية يخشون عمليات القرصنة على معلوماتهم وتعاملاتهم وحساباتهم المصرفية، وكل ما يرسلونه أو يستقبلونه على هذه الشبكة العنكبوتية. حتى أن عمليات القرصنة هذه، التي تقوم بها مجموعات "الهاكرز"، جزءا من الأمن القومي في معظم دول العالم، وخصوصاً تلك الدول الكبرى التي تستضيف خوادم الإنترنت ــ servers ــ حتى إن رئيس الوزراء البريطاني "توني بلير" اعتبرها من أكثر الجرائم التي تهدد الأمن القومي البريطاني؛ نظراً لصعوبة تعقّب مرتكبيها.

وأصبحت الحقيقة المؤكدة التي لاشك فيها في هذا المجال، هي: أن القراصنة أو " الهاكرز "، قد لجأوا إلى اختراع برامج وطرق جديدة معقدة جداً، من شأنها تمكينهم من اختراق الشبكات والأجهزة مهما تكون حمايتها، ومهما تكون تعقيدات الاحتياطات الأمنية التي تقوم بها الشركات الكبرى؛ لحماية معلوماتها وقواعد البيانات الخاصة بها. وتختلف برامج التجسس في المميزات وطرق الاستخدام، ولكن الطرق التقليدية التي يستعملها "الهاكرز" المبتدئون جميعاً، تعتمد على فكرة واحدة، وهي ما سُمي بـــ"الملف اللاصق" " file patch"، الذي يرسله المتجسس إلى جهاز الضحية، عن طريق البريد الإلكتروني، أو برامج المحادثة، فيقوم

---

[230]– الهاجري, إياس. **جرائم الإنترنت**. [على الخط المباشر].زيارة يوم :2006/02/12.متوفر على الموقع: http://www.egovs.com/egovs_webo2/news

الضحية المستخدم بفتحه بحسن نية، دون دراية منه أنه قام في الوقت نفسه بفتح الباب على مصراعيه للمتجسس؛ ليفعل ما يريد بجهازه [231]

إذن فإن الطلبة يرون بأن القاضي معرض للمشاكل وعراقيل عند الفصل في قضايا المعلوماتية أما عن مرد هذه المشاكل فهي تقادم النصوص القانونية (60%)، ذلك لأن القوانين والتشريعات الجزائرية تعد قديمة ولا تتماشى مع التطورات الحاصلة على ساحة الجريمة وبالتالي خلق صعوبة تطبيق هذه القوانين على الجرائم التي استحدثتها البيئة الإلكترونية؛ كما يرى (60%) من الطلبة ان سبب هذه المشاكل يرجع إلى عدم تمكن القضاة من التقنيات الحديثة،وهذا راجع إلى حداثة دخول الانترنت إلى الجزائر،ومنه فإن أغلب القضاة لدينا تنقصهم الخبرة والتجربة في ما يتعلق بمثل هذه التقنيات وبالتالي يصعب عليهم الفصل فيها كما أن خصوصية هذه الجرائم تؤدي على خلق عراقيل للقضاة؛والشكل البياني التالي يوضح هذه النسب:

الشكل رقم: 19 أسباب المشاكل التي تعترض القضاة في الفصل في القضايا المعلوماتي

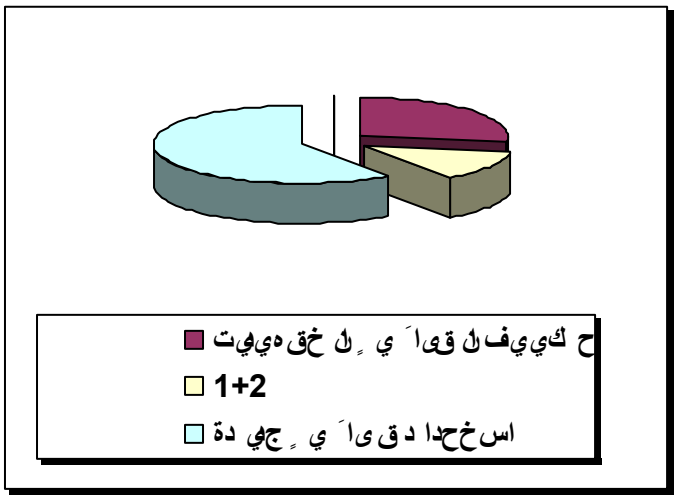
ومن اجل تدارك النقص في التشريعات الجزائرية فيما يخص تشريعات حماية المعلومات ،حاولنا معرفة إذا كانت هناك مساعي لاحتواء مثل هذه الجرائم من خلال سؤال الطلبة وكانت الإجابة كما هي موضحة في الجدول رقم30 الصفحة 149

ومن تحليل نتائج الجدول السابق نلاحظ أن أغلب الطلبة (66,6%) ليسوا على دراية إن كانت هناك مساعي أو مشاريع لاستحداث أو تطوير القوانين أو المراسيم من أجل احتواء ظاهرة الإجرام المعلوماتي، والتي أصبحت بحق جرائم العصر التي تهدد المجتمع الكوني ككل ؛ أما (20%) من عينة الدراسة فقد نفوا وجود أي مساعي لإحداث تغييرات على القوانين في الوقت الراهن إلا أن الغد كفيل بأن تتغير هذه النظرة خصوصا وأن هذه الجرائم في توسع رهيب و لم يسلم منها أحد غي العالم، أما عند محاولة معرفة اقتراحات الطلبة من أجل حل هذه المشكلة كانت الإجابة كما هو موضح غي الجدول رقم 31 الصفحة149

---

[231] –عبد الله، إسلام. **الحماية من فيروسات الإنترنت ضرب من الخيال**. [على الخط المباشر]. زيارة يوم 2006/02/12:. متوفر على الموقع: http://www.aljesr.nl/map.htm

إذن فإن أغلب الطلبة (60%) يرون أن أحسن حل لاحتواء ظاهرة الإجرام المعلوماتي هو استحداث قوانين جديدة وهذا باعتبار أنه الاختيار الأنجع؛ لأن هذه الطاهرة جديدة وتحتاج إلى حلول جذرية تستطيع الإلمام بكل جوانبها ولا تحتاج إلى حلول مؤقتة أو هامشية؛ أما (26%) من الطلبة فيرون أن تكييف القوانين التقليدية يعتبر كافيا لاحتواء الجرائم الحديثة؛ أما باقي الطلبة فإن الحل بالنسبة لهم هو تعديل وتكييف فالقوانين التقليدية في مواضع معينة واستحداث أخرى في مواضع حيث لا مجال للتعديل وهذا الحل هو الأقرب للصواب والشكل البياني التالي يوضح ذلك:



الشكل رقم:20 اقتراحات الطلبة حول احتواء ظاهرة الإجرام المعلوماتي

مر التشفير بعدة تطورات إلى أن وصل إلى ما هو عليه الآن[232]:

- 50- 58 سنة قبل الميلاد: يستخدم الإمبراطور يوليوس قيصر **Jules césar** الرموز المشفرة في رسالته على حاكمه سيسرون **ciceron** في حروبه ضد بلاد الغال وكان يستخدم في ذلك طريقة إستبدال الحروف الأصلية بالحروف التي تليها مباشرة أو تنفيذ عمليات تجعل النص المكتوب غير مفهوم.
- 1499: نشر الراهب الألماني جون ترتيمام **Jean Tritheme** أول كتاب خاص بالتشفير يعرض فيه كيفية التشفير.

[232]– عبد الحق, ط.**مدخل إلى المعوماتية: برمجيات الحاسب الشخصي. = Logiciel de PC** .البليدة: فصر الكتاب ,2005.ص.327.

- 1914- 1918: تطور علم التشفير خلال الحرب العالمية الأولى بشكل كبير وهذا باستخدام تقنيات جديدة تهدف على سرعة الاتصالات العسكرية.

- 1977: تصميم نظام التشفير **RSA** .

- 1997: استخدام مفتاح تشفير بطول 40 بت ثم فك تشفيره من طرف طالب جامعي في عدد من الدقائق.

- 1999: استخدام مفتاح تشفير بطول 512 بت والذي تم فك شفرته من طرف مجموعة من الباحثين بعدة أربعة أشهر.

- 2001الإستخدام الواسع لنظام التشفير **open pgp** من طرف الكثير من العاملين على شبكة الأنترنت بقصد تأمين سرية المعلومات.

3- أنواع التشقير:

التشفير نوعان[233]:

7 -**التشفير المتماثل:** يستخدم فيه المفتاح نفسه للتشفير وكذا لفك الشفرة, وبذلك فإن المفتاح يكون معروفا من طرف كل من مرسل الرسالة ومستقبلها ولا يرسل المفتاح مع الرسالة ولكن يرسل بطرق أخرى حرصا على حماية سرية المفتاح وعدم إطلاع الغير عليه؛ وقد استعملت كتب للأكود **sécure code book** وتتضمن قائمة بمفاتيح التسفير التي يجب أن تستخدم بطرق محددة ؛فعلى سبيل المثال فإن الرسالة التي ترسل يوم الأربعاء يتم استخدام المفتاح **A** يفك شفرتها ,وتفقد كتب الأكواد فيمتها إذا ما تمت سرقتها لأن ذلك يعني كشف المفتاح من قبل الغير.

8 -التشفير غير المتماثل: ويستخدم فيه مفتاحان لكل مستخدم , أحدهما +مفتاح عام معروف من قبل الآخرين حيث يسجله الشخص عادة مع توقيعه على البريد الإلكتروني , في حالة الرغبة في إرسال رسالة مشفرة إلى ذلك الشخص يتم استخدام ذلك المفتاح العام لكتابة الرسالة أما لفكها فيستخدم مفتاح خاص لا يعرفه إلا المستقبل نفسه ؛وغلى الرغم من ارتباط كل نمن المفتاح العام والخاص ببعضهما إلا أن أي منهما لا يدل على الآخر.

وهناك طرق متعددة للتشفير تتراوح في درجة تعقيدها فقد تكون سهلة للغاية لا تتعدى فكرة الاستبدال كما هو الحال في شيفرة قيصر التي تمثل في أبسط صورها إستبدال كل حرف في الأبجدية بحرف آخر وفقا لمفتاح الشيفرة المحدد ,وقد تم تطوير فكرة الاستبدال حتى تصبح أكثر تعقيدا وبالتالي يصبح كسرها أمرا في غاية الصعوبة.

---

[233]- بومفلاح, فاتن.المرجع السابق.ص.561.

4- أهمية التشفير:

إن أهم الأخطار التي يمكن أن نتغلب عليها بواسطة التشقير هي[234]:

- الإطلاع على المعلومات المحضورة.
- محاولات تعديل البيانات إلى وجهة إخرى
- تأخير محتويات الرسائل المتبادلة.
- تغيير كلمات السر الخاصة بالمستفدين.
- إنتحال شخصية المستخدم الحقيقي.
- تعديل البيانات المخزنة على الحاسب.

5-1-3-3. الجدران النارية:

1- تعريف الجدران النارية:

يخطر في بال معظم الناس عند الحديث عن أمن شبكة الأنترنت برامج جدران النار وعلي الرغم من أن برامج جدران النار لا تعتبر علاجا لجميع مشاكل أمن المعلومات علي شبكة الانترنت، إلا إنها ضرورية لأي إستراتيجية متعبة، في مجال أمن انترنت، تعتبر برمجيات جدران النار ببساطة حاجزا بين شبكتين وهما في اغلب الأحيان شبكة داخلية وتسمي الشبكة الموثقة **trusted network** شبكة خارجية تسمي **entrusted network**وهي شبكة انترنت في هذه الحالة وتقوم برمجيات جدران النار بفحص رزم البيانات القادمة والخارجة اعتمادا علي مجموعة قواعد التي يضعها المشرف علي الشبكة، للسماح لهذه الرزم بالمرور أو يقوم بحجبها ومنعها من الوصول إلي الشبكة الداخلية.

في الأيام الغابرة كانت تقام أسوار حجرية تفصل بين الأبنية والبيوت الخشبية , فتمع في حالة إندلاع حريق امتداد اللهب من بيت لآخر وكانت تسمى بجدران النار , وفي الشبكات الحديثة مثل الأنترنت يمكن اعتماد الطريقة نفسها لحماية مصادر الشبكات الداخلية من الأخطار الناتجة عن ضياع المعلومات الحيوية[235].

ويمكن تعريف الجدار على أنه برنامج **software** أو عتاد **hardware** لحماية موارد الشبكة الداخلية من مستخدمي الشبكات الأخرى , وتستخدم في حالة ارتباط الشبكة بشبكات واسعة وتعمل على منع المستخدمين الخارجيين من الوصول إلى مولد الشبكة وبياناتها الخاصة [236].

---

[234]- داود ,حسن الطاهر.الحاسب وأمن المعلومات.المرجع السابق.ص.178.

[235]- المسفر ,**يوسف.الشبكات المعلوماتية والجدران النارية**.من مجلة علوم وتكنولوجيا.ع53. اتلسنة الخامسة 1996.ص.48.

إذن فالجدران النارية عبارة عن نظام أو مجموعة أنظمة تفيد تعزيز ضبط الوصول إلى المعلومات بين شبكتين أما الوسائل المعتمدة فمختلفة إنما من حيث المبدأ يمكن تعريفه بأنه عبارة عن آليتين , واحدة تعيق الحركة والأخرى تسمح بها [237].

2- أنواع الجدران النارية:

تستخدم معظم برمجيات جدران النار اليوم طريقة واحدة أو أكثر من الطرق الثلاث المتبعة في فحص الرزم وتستخدم العديد من الموجهات تقنية جدران النار المسماة بترشيح الرزم **packet filtering** والتي تفحص عناوين وبوابات المصدر **Source** والوجهة النهائية **destination** لرزم **TCP** ورزم **UDP** القادمة ثم ترفض أو تسمح للرزم بالمرور وفقا لمجموعة من القواعد مسبقة التحضير وتعتبر تقنية ترشيح الرزم طريقة رخيصة نسبيا وشفافة بالنسبة للمستخدم ولها تأثير طفيف غير ذي بال علي أداء الشبكة ولكن تجهيز تقنية ترشيح الرزم يعتبر عملية معقدة نسبيا ويتطلب معرفة دقيقة بالشبكة وبرتوكولات النقل بل يتطلب في بعض الأحيان معرفة ببروتوكولات التطبيق.

تكمن المشكلة الأخرى في تقنية مرشحات الرزم في أنها عرضة لما يسمي خداع بروتوكول انترنت **IP Spoofing**وهي طريقة يستخدمها الهاكرز ليتمكنوا من الوصول إلى شبكة شركة عن طريق تغيير عناوين بروتوكولات انترنت في ترويسة الرزم إلى عناوين أخرى مقبولة من قبل شركة أخرى

أما النوع الأكثر تقدما وأمنا من أنواع جدران النار فهي برامج بوابات التطبيقات **application gateways**، تستخدم معظم منتجات جدران النار العاملة بتقنيات بوابات التطبيقات بما فيها برامج **eagle**الشهيرة من شركة **Raptor** ما يسمي توكيلات التطبيقات **application proxies** وهي عبارة عن برامج مكتوبة لخدمات معينة من خدمات انترنت (مثل خدمات **HTTP** ، **FTP**وخدمة **telnet**وتعمل علي مزود مرتبط بشبكتين كمزود **Server** لزبون تطبيقات **application client** وكزبون لمزود التطبيقات **application server**

ونظرا لان برامج توكيلات التطبيق تقوم بتقييم رزم الشبكة لتحديد شرعية البيانات المتعلقة بتطبيق معين فإنها تعتبر شكل عام أكثر أمنا من مرشحات الرزم. وتمتاز معظم جدران النار لبوابات التطبيقات باحتوائها علي ميزة تدعي "ترجمة العناوين الشبكة **Network Address Translator** "والتي تمنع ظهور عناوين **IP**الداخلية .أمام المستخدمين من خارج الشبكة الموثقة. تكمن إحدي السلبيات الرئيسية في تقنية بوابات التطبيقات في انخفاض مستوي الأداء بسبب المعالجة المضاعفة التي تتطلبها وظيفة التوكيل **proxy function**وهناك سلبية أخري تكمن في انه قد يتوجب عليك أن تنتظر عدة أشهر حتى تزودك الشركة الصانعة لبرنامج جدران النار بتوكيل التطبيق **application proxy** لأي خدمة جديدة من خدمات انترنت مثل استخدام خدمات **RealAudio.** وإذا كنت تنوي استخدام جدران النار دفاع محيطي

---

[236]- بومفلاج , فاتن.**حماية المعلومات في شبكة ام القرى**.مقتطف من كتلب الوقائع.مج 2.الشلرقة 2001,.ص.562.

[237]- المسفر ,يوسف. المرجع السابق.ص.48.

خارجي فقط وراء توصيلات **T1** الي مزود خدمة انترنت فلا داعي للقلق علي الأداء، لان عرض الحزمة المنخفض لهذه التوصيلات سيصل إلي حد الإشباع قبل وصول جدران النار الي ذلك الحد. قد تجد الكثير من المؤسسات ضرورة في استخدام جدران النار إضافية علي مستوي شبكاتها الداخلية لفرض حزام امني علي مزودات أقسامها المختلفة مثل مزود المورد البشرية الذي يحتوي عادة علي معلومات حساسة، ويصبح الأداء في هذه الحالة عاملا مهما نظرا لان الربط سيعتمد علي شبكة ايثرنت بسرعة 10 ميجابت/ثانية أو شبكة ايثرنت السريع 100 ميجابت/ثانية .وإذا كنت تنوي استخدام توكيلات التطبيقات داخليا فعليك أن تعتمد علي حل مبني علي عتاد سريع مثل **pix firewall** من شركة **Cisco** أو **firebox** من شركة **Seattle software** أو قد تلجا الي تركيب برمجيات جدران النار علي نظام يتضمن عدة معالجات .

أما النوع الثالث من تكنولوجيا جدران النار والذي أسمته شركة **check point software** باسم تفقد الحالة الكاملة **state full inspection** فهو موجود في برنامج **firewall-1** من شركة نفسها وبرنامج **pix firewall** من شركة سيسكو وبرنامج **On Guard** من شركة **On technology** وبرنامج **firewall/plus** من شركة **network-1** وكما هو الحال في تقنية ترشيح الرزم فان هذه التقنية تستقبل أولا الرزم علي مستوي طبقة الشبكة **Network layer** ثم تقوم بتفحص جميع الرزم ومقارنتها مع نماذج معروفة من الرزم الصديقة وفيما تعطي طريقة تفقد الحالة الكاملة أداء اعلي بقليل من أداء توكيلات التطبيقات إلا أن الجدل يبقي قائما فيما إذا كانت آمنة مثلها أم اقل أمنا منها[238].

3- الوظائف الأساسية للجدران النارية: تتلخص أهم الوظائف التي تؤديها الجدران النارية في 239:

- منع دخول المستعملين غير المصرح لهم بالدخول إلى الشبكة.
- حماية استخدام الخدمات الهامة عند الدخول إلى الشبكة ومغادرتها.
- حماية عامة من جميع الهجمات.

وبذلك يمكن لأي شركة أو بنك أو مؤسسة حكومية حماية وتامين المعلومات الخاصة بها من أي مستعمل غير مصرح له بالدخول وهذا يعني أن برمجيات جدران النار تحتو يعلى مجموعة من السياسات التي تجعلها بمثابة مصفاة لمنع الطلبات المشبوهة من الوصول إلى الجهاز الخادم ؛ كما يمكن إعدادها بحث يتم إسقاط ووقف أية طلبات واردة تحاول النفاذ إلى الخادم من منفذ لم يحدد ضمن سياسات هذه البرمجيات , ويمكن لبرنامج الجدار الناري أن يقوم بحماية الشبكة من الفيروسات والحماية من البرمجيات الدخيلة بحسب ما سطر داخل البرمجة.

3- مزايا وعيوب الجدران النارية:

---

[238]- **أمن الشبكات..**[على الخط المباشر]. زيارة يوم: 2006/03/18 متوفر على الموقع: http://www.jubailnet.com/vb/forumdisplay.php

[239]- حجازي.عبد الفتاح البيومي. الحكومة الإلكترونية.المرجع السابق.ص. 60.

يمكن القول وكما في أية تقنية جديدة أن الجدران النارية لها عيوب ومزايا نلخصها في ما يلي[240]:

1- فيما يخص المزايا:

- توفير الحماية اللازمة للشبكة والمعلومات.

- توفير خدمات تشفير عالية القوة.

- الجدار الناري يتوافق مع جميع الشبكات المفتوحة.

- تخزين المعلومات والعمليات التي تمر من خلاله.

- متابعة المستخدمين للشبكة وكل من يحاول العبث بها.

أما فيما يخص العيوب:

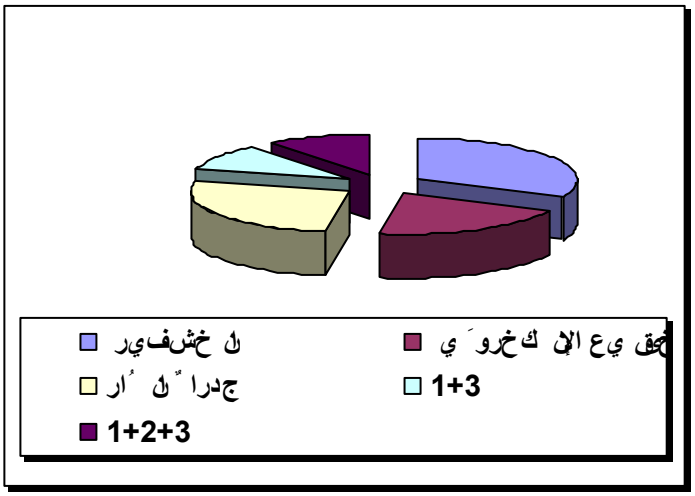
- لا يتعامل الجدار الناري مع البرامج الداخلية التي تهاجم النظام.

- لا يقدم الحماية للنقل الإذاعي والتلفزيوني.

التشفير ،التوقيع الإلكتروني، جدران النار أهم الطرق المعتمدة لحماية المعلومات وضمان سلامتها أثناء مسارها وعند سؤال الطلبة عن أهم وأنجع الطرق لحمايتها كانت الإجابة كما هي موضحة في الجدول رقم 20 من الصفحة 146

إذن فإن أنجع طرق الحماية حسب الطلبة هو عملية التشفير(31,5 %) والتشفير هو إعادة كتابة البيانات باستعمال أحد مفاتيح التشفير، ثم تليها جدران النار بنسبة (26,3 %) وهو محاولة تصفية البيانات الداخلة إلى الداخلية لمؤسسة ما عن طريق مصفاة يطلق عليها جدران النار، ومع تطور معاملات التجارية وظهور الإقتصاد الشبكي كالتجارة الإلكترونية والتسوق الإلكتروني أدى إلى ظهور وسيلة جديدة هي التوقيع الإلكتروني والذي يعد وسيلة لا غنى عنها في مثل هذه المعاملات كما يمكن الجمع بين وسيلتين آو أكثر من الوسائل السالفة الذكر وذلك لضمان حماية أكبر وهذا ما نوضحه في الشكل البياني التالي :

[240]- حجازي.عبد الفتاح البيومي. الحكومة الإلكترونية.المرجع نفسه.ص. 63.



الشكل رقم:15 وسائل حماية المعلومات

5-2. أمن المعلومات: الأخلاق (أخلاق التعامل في مجتمع المعلومات)

إن الأخلاق تعد قوة ردعية في المجتمعات لا يستهان بها غي إرشاد وتوجيه سلوكيا ت الناس فما هو الدور الذي تلعبه الأخلاق في مجتمع المعلومات؟

5-2-1. مجتمع المعلومات.

أن مجتمع ما بعد الصناعة هو مجتمع المعلومات وفي مايلي نتطرق إلى اهم عناصر هذا المجتمع الجديد

5-2-1-1. مفهوم مجتمع المعلومات.

لابد في البداية إلى الإشارة أن هناك العديد من التعريفات لمجتمع المعلومات وأن تعريف مجتمع المعلومات لا غير واضح المعالم بشكل عام

إنه مفهوم يرى التحول من مجتمع صناعي إلى مجتمع حيث المعلومات هي القوة الدافعة والمسيطرة وهناك من يرى أنه المجتمع الذي ينشغل معظم أفراده بإنتاج المعلومات أو جمعها أو اختزانها أو معالجتها أو توزيعها [241].
كما يرى البعض بأن مجتمع المعلومات هو المجتمع الذي تستخدم فيه المعلومات بكثافة كوحي للحياة الاقتصادية والاجتماعية والثقافية والسياسية، ويرى الدكتور ناريمان متولي أن مجتمع المعلومات هو المجتمع الذي يعتمد في تطوره بصفة رئيسية على المعلومات الحاسبات الآلية وشبكات الإتصال أي أنه يعتمد على

[241]– عبد الهادي ,محمد فتحي.**المعلومات وتكنولوجيا المعلومات على أعتاب قرن جديدة**. القاهرة:الدار العربية للكتاب ,2000.ص.18.

التكنولوجيا الفكرية التي تضم سلع وخدمات جديدة مع التزايد المستمر للقوة العاملة المعلوماتية التي تقوم بإنتاج وتجهيز ومعالجة ونشر وتوزيع وتسويق هذه السلع والخدمات

وقد أدى عدم الاتفاق على مجتمع المعلومات إلى اختلاف الرؤى حوله فقد أشارت دراسة حديثة عن الموضوع إلى ثلاث رؤى لمجتمع المعلومات

الرؤية الأولى: وهي رؤية أوربية يمثلها العالم الاجتماعي(إيان مايلز**Ian miles**) وترتكز على الإنتشار الواسع لتكنولوجيا المعلومات والإتصالات ومالها تأثيرات هي التي تشكل مجتمع المعلومات

الرؤية الثانية: هي رؤية يابانية ويمثلها العالم الاتصالات اليابانية جوهوكا شاكاي **johoka shakia** وهي يرتكر على تدفق أو انسياب المعلومات بكميات هائلة عبر كل الوسائل في المجتمع وترتكز.

الرؤية الثالثة: وهي رؤية أمرقية ويمثلها عالم الإقصاد (فريتز ماكلون) على أن نسبة متزايدة من الناتج القومي الكلي للدولة تجيء من إنتاج المعلومات ، ومن ثم أضافت الإقصاديات الحديثة قطاعا جديدا إلى القطاعات المعروفق[242].

ومن وجهة نظرنا أن لكل هذه الرؤى روافد تصب في نهر واحد ,وان كل واحدة من الرؤى الثلاثة السابقة إما أن تكون سببا لأخرى أو أن تكون حتمية لسابقتها .

إن عصر ما بعد الصناعي أو مجتمع المعلومات كما يطلق عليه هو حصيلة لتراكمات إحتماعية وعلمية وثقافية طيلة سنوات، وقد ساهم غب دخول هذا العصر التطورات التقنية والتكنولوجية التي عرفها العالم المعاصر؛ وتعد الولايات المتحدة الأمريكية وكندا ودول أوروبا من بين الدول السباقة للإنخراط في مجتمع المعلومات الكوني؛ أما دول العالم الثالث بصفة عامة والدول العربية خصوصا فقد خطت خطوت محتشمة للإنضمام لهذا الركب وعند سؤال الطلبة عن ضرورة آو حتمية الإنخراط في مجتمع المعلومات كانت الإجابة كما هي موضحة في الجدول رقم21 من الصفحة 146
إذن وحسب نتائج الجدول فإن الأغلبية الساحقة لعينة الدراسة (97,3 %) ترى أن دخول عالم المعلومات هو ضرورة ملحة تفرضها الظروف المعاشة وهذا من أجل اللحاق بركب الحضارة وعدم الاضمحلال في بوتقة العولمة .

5-2-1-2. خصائص مجتمع المعلومات:

يقدر علماء الاقتصاد أن حجم التعاملات المالية التي تتم يوميا عبر الأجهزة والشبكات الإلكترونية للمؤسسات المالية يصل إلى 25بليون دولار , ولعل هذا الرقم العالي يظهر اعتماد المجتمعات في هذا العصر على التجهيزات المنية على تقنيات الحاسب [243] ؛ويمكن تلخيص أهم خصائص التي تطبع مجتمع المعلومات[244]:

---

[242]– عبد الهادي ,محمد فتحي. المرجع السابق.ص.18.

[243]– عباس , طاهر محمود.**المكتبات الرقمية وشبكة الأنترنت**.القاهرة: المركز الأصيل ,2003.ص.45.

1- **انفجار المعرفة:** يرى العديد من لباحثين أن المعلومات المنتجة في الحقبة المعاصرة أكثر أهمية مما أنتج في كل تاريخ البشرية ,كما أنها تتزايد بمعدلات كبيرة نتيجة التطورات التي يشهدها العالم ونتيج ة بروز تخصصات جديدة.

2- **زيادة أهمية المعلومات:** في مجتمع المعلومات ازدادت أهمية المعلومات وأصبحت المعلومة تدخل في كل الأنشطة والصناعات، كما تمثل المادة الخام لقطاعات كثيرة من قطاعات المجتمع المعاصر مشكِلة ما يمكن أن يطلق عليه" صناعة المعلومات " وأصبح ينظر إلى المعلومات كمورد أساسي وإستراتيجي يمكن أن يباع ويشترى.

3- **نمو المجتمعات والمنظمات المعتمدة على المعلومات** :يتميز مجتمع المعلومات كذلك بظهور منظمات تعتمد كليةً على المعلومات مثل مؤسسات الجرائد والأخبار والإستعلامات والبنوك وشركات التأمين....

ويلاحظ أن انفجار أو تضخم هذه المنظمات قد بدأ في الظهور في نفس الوقت الذي شهد بدايات ثورة المعلومات المعاصرة.

4- **تعدد فئات المتعاملين مع المعلومات** : أوجد مجتمع المعلومات فئات كثيرة تتعامل مع البيانات والمعطيات والمعلومات وتشتعل بها منها:

- العلماء والفنانون والمصممين وغيرهم ممن يقدرون على إنتاج وإيجاد معلومة جديدة أو يعيدون تشكيل نماذج معرفية جديدة من واقع المعلومات الحالية.

- العاملون في نقل وتوصيل المعلومة.

- العاملون في تخزين المعلومات كأخصائي المعلومات وأمناء المكتبات ومبرمجي الحاسب.

5- قلة الاعتماد على الورق: حيث تزايدت بصفة مطردة كميات المعلومات المنتجة على وسائط غير ورقية وفي المقابل فإن استعمال الورق أخد يتقلص.

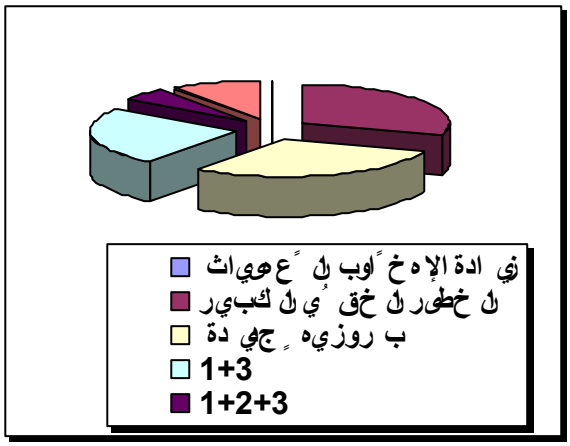
إن العصر الذي نعيشه بكل حيثيات ه هو مجتمع المعلومات هو مجتمع المعلومات بحق؛ فقد غدت المعلومات العصب المحرك لكل مناحي الحياة الاجتماعية والسياسية والثقافية والعلمية، وقد تزايد الاهتمام بالمعلومات مند أن أصبحت تمثل مصدرا أساسيا للدخل القومي للدول المنتجة للمعلومات، وقد ظهرت قطاعات تُعنى بالمعلومات عي كل مراحلها أي مند إنتاجها وإلى غاية نشرها وتوزيعها؛ وقد اتسم مجتمع المعلومات بعدة خصائص نوجزها في الجدول22 من الصفحة 146

إذن فحسب عينة مجتمع الدراسة فإن الخاصيتين اللتان تطبعان مجتمع المعلومات هي زيادة الاهتمام بالمعلومات وكذا التطور التقني المذهل (31,5 %) وهذا ما يؤكده حشد ميزانيات ضخمة والتي تخصصها

---

[244]- لغقاب، محمد. مجتمع **الإعلام والمعلومات:ماهيته وخصائصه**.الجزائر:در هومة ،2003.ص.88.

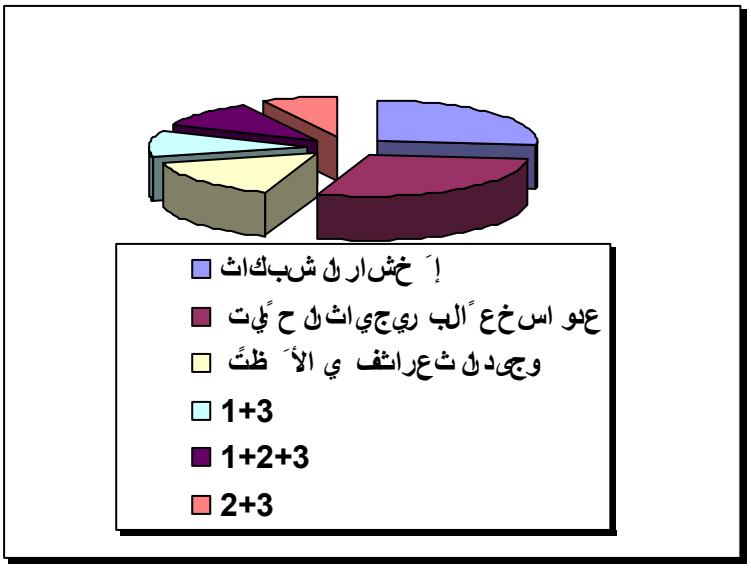
الدول المتقدمة من أجل تنمية البحوث العلمية وكذلك إنشائها لأكبر مراكز البحوث العلمية والتكنولوجية، إن هذا الاهتمام الكبير بالمعلومات أدى إلى ظهور مهن جديدة كصناعة المعلومات وهذا ما عبرت عنه (26,3 %) من عينة الدراسة، أما باقي الطلبة فيرون أن كل هذه الخصائص السالفة الذكر لها نفس الأهمية في مجتمع المعلومات ،ويمكنا أن نوضح ذلك بشكل أفضل كما يلي:



الشكل رقم:16 خصائص مجتمع المعلومات

إذن وكما سبق الإشارة إليه فإن البيئة الإلكترونية أدت إلى قلب العديد من الأمور؛ حيث ظهرت العديد من الإفرازات منها ما هو سلبي ومنها ما هو إيجابي، وتعد الفيروسات واحدة من أبرز الإفرازات السلبية وقد ساهم في انتشاره هذه الأوبئة عدة أمور موضحة في الجدول رقم **15** الصفحة 144

وفقد أعرب الطلبة على أنه ومهما اختلفت الأسباب التي تؤدي إلى إنتشار الفيروسات بشكل رهيب فإن أهمها على الإطلاق هو عدم استعمال برمجيات الحماية بنسبة (28,9 %) وذلك على الرغم كمن الأهمية التي تكتسيها هذه البرمجيات، ثم يليها إنتشار الشبكات بنسبة (26,3 %)، حيث أن الشبكات اكتسحت العالم المعاصر مما جعلها تشكل مناخا ملائما لنمو وتطور الفيروسات، كما أدى ظهور الشبكة العنكبوتية إلى استعمالها كناقل ممتاز لنشر هذه الفيروسات؛ ومن أهم أسباب انتشارها كذلك وجود ثغرات كثيرة في الحاسب وأنظمة التشغيل وهذا ما عبر عنه (17,7 %) من العينة، كما تشكل هذه الأسباب إذا توفرت جميعها لأكبر وأحسن بيئة لالتهاب الشبكة بهذه الفيروسات وهذا ما يوضحه الشكل البياني التالي:



الشكل رقم :11 أسباب إنتشار الشبكات

4-1-3-3. وسائل إنتقال الفيروس[245]:

يمكن لفيروس الحاسب الإنتقال داخل شبكة الإنترنيت أو أي شبكة محلية عن طريق وسائل أربعة:

1- البريد الإلكتروني:

ينتقل الفيروس عبر برنامج أوت لوك وأوت لوك اكيبريس وذلك عن طريق ملف يلصق بالرسالة التي ترد عبر البريد الإلكتروني ويحمل ملف إسم **REACLM EXE** وتظهر له أيقونة بقوته **ATML** وذلك في محاولة لخداع المستخدم ويكفي قيام المستخدم بالنقر على الملف حتى ينسخ الفيروس نفسه و بمد رسالة تلقائية ترسل إلى جميع العناوين الخاصة بالبريد الإلكتروني التي توجد في دفتر عناوين المستخدم.

2- مزود ويب ISS

يضع الفيروس عناوين عديدة بشكل ؟؟؟؟؟ لما يفعله فيروس **CODERED** بحثا عن مزودات **ISS**والتي تتضمن ثغرات أمنية يستفيد منها في عملية الإنشار ويحاول الفيروس كذلك الاستفادة من دودة فيروس**CODERED2** التي تنتشر عبر مزود **ISS** حيث كانت الدودة تترك برنامج باب خلفي في هذه المزودات كي تسمح للمخترق بالدخول إليها والسيطرة عليها فيما بعد

3- متصفح الأنترنت:

[245]- حجارى , عبد الفتاح بيومي. النظام القانوني لحماية الحكومة الإلكتورنية. الكتاب الثاني و الجنائية المعلوماتية لنظام الحكومة الإلكترونية. الإسكندرية:دار الفكر الجامعي 2003 ص ص 74 - 78

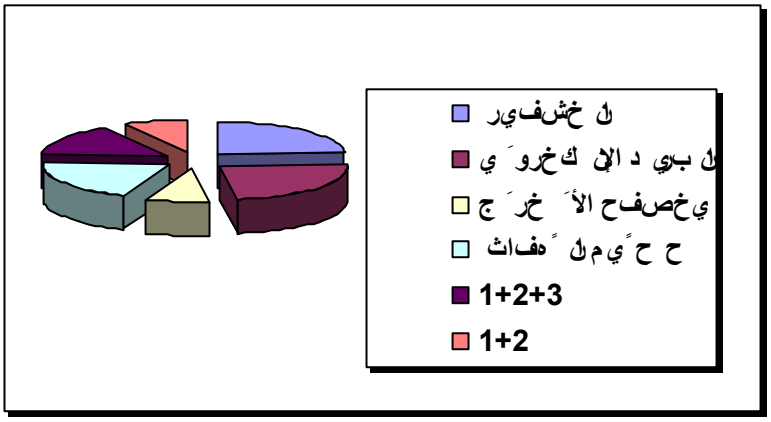
بعد أن يصيب الفيروس أحد المزودات – شبكة الأنترنيت – بالطريقتين السابقتين بنسخ شفرة معينة إلى كل صفحات (**asp- htmail- htm**) التي توجد في المواقع التي يستضيفها مزود -الأنترنيت – وعند زيارة الموقع المصاب من طرف أحد المستخدمين ويبد أفي تنزيل ملف منه يشتعل الفيروس تلقائيا ويصيب جهاز المستخدم

4- المشاركة على الملفات:

تسمح هذه الطريقة للفيروس أن ينتشر عبر الشبكات المحلية التي وجدت ملفات أو مجلدات مشتركة عبر شبكة ميكروسوفت .

وكما سبق الإشارة إليه فإن الفيروسات تنتشر بعدة طرق أهمها البريد الإلكتروني وكذا تحميل الملفات من الأنترنت والجدول 16 الصفحة 144 بوضح ذلك

ترى عينة الدراسة أن أهم طرق انتشار الفيروسات هي البريد الإلكتروني (31,5 %)،فمع إنتشار شبكة الانترنت أصبح البريد الإلكتروني الخدمة الأكثر شعبية والتي أدت إلى زيادة استخدام الشبكة وقد استغل صناع الفيروسات هذه الخدمة من أجل نشر سمومهم على الشبكة، كما يمكن أن يؤدي تحميل الملفات من الأنترنت خصوصا من المواقع المشبوهة إلى المساهمة في إنتشار هذه الأوبئة وهذا ما عبرت عنه (26,5 %) من عينة الدراسة إضافة على العديد من الطرق الأخرى كمتصفح الأنترنت ونوضح ما سبق ذكره بشكل أفضل بالرسم البياني التالي:



الشكل رقم: 12 طرق نشر الفيروسات

4-2. أنواع الفيروسات وأشكالها:

4-2-1. أنواع الفيروسات

إن الفيروسات مهما أختلف شكلها أو نوعها خاصة واحدة هي إلحاق الأدى والضرر بالبرامج إلي برمجت لإلحاق الأذى بها ويمكن أن نميز العديد من أنواع الفيروسات:

4-2-1-1. قطاع التشغيل bootseetor :

وتعتبر من أقدم الفيروسات وأكثرها إنتشار إذ تستطيع أن تصيب المقطع التشغيلي في الأقراص المرنة أو مقطع نظام تشغيل الدوس **dos** حيث أن كل الأقراص سواء كانت صلبة أو مرنة تملك قطاع تشغيل ويتكون من المعلومات الخاصة بشكل القرص (نوع البنية , نوع المعطيات) وتكمن خطورة هذه الفيروسات في قدرتها على إتلاف هذا الجزء ثم يقوم بأحد مكان قطاع تشغيل القرص المصاب بنسخة منه ثم ينقل المقطع الأصلي إلى مكان آخر في القرص [246] .

4-2-1-2. فيروسات الملفات:

وهي الفيروسات التي تلصق نفسها مع ملفات البرامج التنفيدية ذات الإمتداد **com exe** وقد يمتد أثرها ليصيب الملفات ذات الإمتداد **ouc , dry ,sys**.....ومع هذا النوع من الفيروسات فإن البرامج تصاب بمجرد بدأ تشغيل هذه الرمج[247] ويمكن تقسيم هذه الفيروسات إلى أربغة أنواع[248]:

أ- الفيروسات المتطفلة:

التي تلصق نفسها بالملفات لكي تتكاثر وتبقي الملف الأصلي بحالة سليمة

ب- الفيروسات المرافقة:

التي تعتمد على قاعدة الأسبقية في التنفيد للملفات ذات الإمتداد **com** وتتمكن من نقل العدوى عن طريق إنشاء ملف جديد بدون ؟؟؟؟؟ الملف

ج- الفيروسات الرابطة:

وهي التي تصيب البرامج بتغيير المعلومات في جدول مواقع الملفات

د- الفيروسات المستبدلة:

التي تقوم بالكتابة فوق جزء من برنامج دون تغيير حجم الملف مما يؤدي إلى فشل الملف عند تنفيذه.

4-2-1-2. الفيروسات متعددة القدرة التحويلية:

---

246 -**types des virus informatique.(**en ligne) (23/02/2006)
fr escpotting.com/ seardr/ riduchon.html www.affiliate

2 - المرجع السابق

3 - شوقي , حسام المرجع السابق ص10

وهذه الفيروسات لها القدرة الديناميكية على وتنفيذ الشفرات عند الإنتقال من ملف إلى آخر لكي يصعب اكتشافها [249].

4-2-1-4. فيروس الماكرو:

هذا النوع أيضا سريع الإنتشار بين المستخدمين خاصة أنه قادر على كل الطرق كالأقراص الصلبة والبريد الإلكتروني والبرامج المجانية ويعتبر من أحد أنواع الفيروسات والجدير بالذكر وهذا الفيروس لا يصيب إلا البرنامج التطبيقي الذي صمم لإتلافه فمثلا لو إن فيروس صمم ليصيب برنامج تحرير الكلمات والنصوص فإنها لا يستطيع إلحاق الأذى بأي برنامج آخر [250].

4-2-1-5. **الفيروسات قطاع الإقلاع:**

تستقر هذه النوعية من الفيروسات في الأماكن التي يقرأها الكمبيوتر بالقرص الصلب وينفد التعليمات المخزنة ضمنها عند الإقلاع ثم تصيب قطاع الإقلاع الخاصة بنظام الدوس بينما تصيب فيروسات الفئة الفرعية المسماة **MBR virus** قطاع الإقلاع الرئيسي للكومبيوتر كما يمكن أن يصيب الفيروس قطاع الإقلاع ةالملفات في وقت واحد ويطلق عليه - الفيروس المتعدد الأجزاء - [251].

4-2-2. أشكال الفيروسات:

بعد تطرفنا بشيء من الإنجاز إلى أهم أنواع الفيروسات والتي من الممكن أن تصيب جهاز الحاسب وإلحاق الخراب والدمار به يجدر بنا الإشارة إلى أنه هناك عدة أشكال للفيروسات حيث أنها لا تتخذ نمطا واحدا ويمكن أن نلخص أهم أشكالها كما يلي [252]:

4-2-2-1.المتخفي: وهو الذي يختبئ في الذاكرة الرئيسية ويسيطر على القطاعات.

4-2-2-2. البطيء: كلما كان إنتشار الفيروس بطيئا كلما صعب إكتشافه والتخلص منه سريعا وأسلوب عما هذا الفيروس هو إصابة الملفات التي كان المستخدم ينوي تعديلها.

4-2-2-3. السريع: يصيب هذا الفيروس كل الملفات الحالية بمجرد دخوله إلى الحاسب وهو ليس خطيرا بشكل كبير.

4-2-2-4. المتعدد الأشكال: هي الفيروسات التي لو تتم مقارنة نسختين من الفيروس نفسه لا يتطابقان مما يصعب مهمة برنامج الحماية ويتطلب منها القيام بأمور كثيرة ومعقدة لاكتشاف هذا النوع.

---

[249]- شوقي ,حسام.المرجع السابق.ص. 10

2- **أروع كتاب في الهاكينغ**: الفيروسات.JOUAHARA2.CD.ROM

[251]- شوقي ,حسام.المرجع السابق.ص. 10

[252]- - شوقي ,حسام.المرجع السابق.ص.14.

4-2-2. أشهر الفيروسات:

4-2-2-1. أشهر فيروسات الحاسب

الفيروس الباكستاني: صمم هذا النوع من الفيروس من طرف باكستاني متخصص في المعلوماتية كان يبيع البرامج المعلوماتية بنصف دولار بينما سعرها في الولايات المتحدة الأمريكية 450 دولار.

الفيروس 13 أكتوبر: تعد نسبة الإصابة بهذا الفيروس قليلة أما سبب تسميته بهذا الإسم هو الشائعة التي ظهرت من أنه سوف يصيب أجهزة الحاسب جميعا في 13 أكتوبر 1989.

الفيروس العقل: وهو من فيروسات نظام التشغيل الدوس وتتمثل خطورته في أنه يكتب على قطاع التحميل للقرص مما يسبب تحميل الفيروس بمجرد تشغيل الجهاز وقبل تحميل أية برامج مضادة وهو ينقل العدوى إلى أي قرص بمجرد عرض الفهرس الخاص بهذا القرص ,ويتميز بقدرته على الإختفاء حيث يقوم بتخزين نفسه بالقطاعات التالفة من القرص[253].

فيروس الحب: ظهر هذا الفيروس في جميع أحاء العالم وبصفة خاصة بالولايات المتحدة الأمريكية وتقدر خسائر أمريكا منه نحو 10مليار دولار وقد اقتحم أنظمة الكمبيوتر العسكرية في وكالة الأمن القومي وقد انتشر هذا الفيروس عن طريق فتح البريد الإلكتروني للمستخدم تحت عنوان **LOVE** ثم لا يلبث أن ينتشر في كافة أنحاء الحاسب بمجرد فتحه.

فيروس مايكل أنجلو: أنطلق هذا الفيروس في 06 مارس 1992 بمناسبة الإحتفال بذكرى ميلاد الرسام الإيطالي مايكل أنجلو والذي توفي عام 1564 ولقد أصاب العديد من أنواع الحاسب [254].

4-2-2-2. أشباه الفيروسات:

1- الدودة:

برامج الدودة هي عبارة عن برامج مخصصة لاستغلال أية فجوات لكي تنتقل إلى الحاسبات الآلية عبر الوصلات التي تربط بينها وتجدر الإشارة إلى أن هده البرامج تتكاثر وتنتشر أثناء عملية انتقالها وتهدف إلى التقليل أو خفض كفاءة النظام ألمعلوماتي أو إتلاف نظم التشغيل والبيانات والملفات والبرامج [255].

ولقد ضربت نماذج كثيرة من هده الدودة شبكات الحاسب حول العالم نورد بعضا منها غي ما يلي [256]:

1-1 –الدودة مصاصة الدماء:

1-

2- العريان , على محمد. المرجع السابق.ص.90.

255- – العريان , محمد علي.المرجع السابق.ص.97.

256- داود , حسن الطاهر. **أمن الشبكات والمعلومات**. المرجع السابق. ص.

يعتبر بعض الدود خبيثا وبعضه حميدا وقد استخدمت شركة ّ زيدوكسّ

غي بداية الثمانينات دودة حميدة أسمتها الدودة مصاصة الدماء وكانت هده الدودة تظل خامدة طول النهار عندما يكون استخدام النظام الفي ساعات الذروة وفي الليل تستيقظ وتنشط وتستخدم المعالج بعد أن يكون قد تخفف عبء العمل لأداء بعض المهام المعقدة التي تحتاج إلى قدرات المعالج باستمرار.

1-2. دودة الأنترنت الهائلة:

لم يكن الاهتمام الموجه لهدا النوع من الفيروسات كبيرا حتى 3نوفمبر 1988 عندما أطلقت دودة الأنترنت الهائلة لتغزو الشبكة ففي أقل من ستة ساعات استطاع هدا البرنامج الذي لابتعد حجمه 99 سطرا أن يشل كل الأجهزة المرتبطة بالانترنت من نوع صن فاكس وعددها 6.000 جهاز ؛ وكانت هده الدودة عندما تصيب الجهاز تقوم بتشغيل برنامج صغير في خلفية الجهاز المصاب و لم يشعر أحد يهدا الأمر في البداية ؛ لولا خطأ بسيط من المبرمج وهو أن الدودة لا تقوم باختبار الجهاز إدا ما كان مصابا أم لا وكان من اثر دلك أن حدثت حالات كثيرة من تعدد الإصابة التي وصلت في بعض الحالات إلى المئات مما عرقل عمل الأجهزة ؛وتفاقم المشكل لاعتمادها على البريد الإلكتروني مما أدى ببعض المواقع إلى فصل نظمها عن الأنترنت.

2- القنابل:

تعد القنابل إحدى الطرق التي تتلف بها المعلومات وهي على غرار باقي الفيروسات صممت لإحداث الضرر بالأنظمة والمعلومات وأهم انواع القنابل:

4 القنبلة المنطقية:

القنبلة المنطقية هي عبارة عن برنامج أو جزء من برنامج ينغد في لحظة معينة أو كل فترة زمنية منظمة ويتم وضعه في شبكة الأنترنت بهدف تحديد ظروف أو حالة النظام لغرض تسهيل تنفيذ عمل غير مشروع ؛ومن دلك مثلا إدخال التعليمات في برنامج تشغيل وهو البرنامج الذي يقوم بتحميل ذاكرة الحاسب بالبرنامج المراد تنفيده ؛وهو الذي ينفد في مرة عمل جديد وينصب البحث على عمل معين يمكن أن يكون محل للاعتداء كأن تسعي القنبلة المنطقية مثلا بالبحث عن حرف معين وليكن الألف في السجلات وعند الأمر بالحذف تتحرك متتالية وتقوم بإزالة هدا الحرف أينما وجدته ومن الأمثلة الواقعية التي استخدمت فيها 2- **القنبلة المنطقية:**

- تمكن خبير في نظم المعلومات غي الدنمارك من صنع قنبلة منطقية في نظام الحاسبات أدى إلى محو أكثر من مئة برنامج وقد تم أيضا محو النسخ الاحتياطية عند تشغيلها نظرا لانتقال آثار القنبلة إليها ثم ضبط الفاعل وحكم عليه بالسجن لستة أشهر[257].

[257]- الرومي ,محمد أمبن.المرجع السابق.ص.57.

2- القنبلة الزمنية:

أما عن القنبلة الزمنية فهي تثيرا حدثا في لحظة زمنية معينة بالساعة واليوم والسنة ويتم إدخالها في البرنامج وتنفد في جزء من الميلي ثانية أو دقائق بتاريخ المحدد سلغا ؛ وبمعنى آخر لأي خبير في صناعة البرامج أن يقوم بصناعة الفيروس إذا كان يضمر شرا للمستهدف ومن اهم الأمثلة التي إستجدمت فيها الهذا الأسلوب :[258]

في فرنسا قام خبير في نظم المعلومات بدافع الإنتقام على اثر فصله من المنشأ الذي يعمل فيه بوةضع قنبلة في شبكة المعلومات الخاصة بالمنشأ بحيث تنفجر بعد مضي ستة أشهر من رحيله وترتب عن ذلك إتلاف كل البيانات المتعلقة بها[259].

---

[258]- العريان , محمد علي.المرجع السابق.ص.57.

[259]- الرومي ,محمد أمبن.المرجع السابق.ص.57.

*- حصان طروادة: تقول الأسطورة أن طروادة كانت مدينة عظيمة منيعة الأسوار والحصون ولم يتمكن مقاتلي إسبارطة من دخولها رغم صبرهم في حصار المدينة الذي دام عشر سنوات وفي الأخير لجأوا إلى حيلة إدعاء الإنسحاب مخلفين وراءهم حصانا خشبيا هدية للطروادبين وكان الحصان يحوي في داخله ثلث الجيش الإسبرطي ,ثم فتح الباب لباقي الجيش بعد إدخال الحصان إلى المدينة.

خاتمة

الخاتمة

على ضوء التطورات المتسارعة والحاصلة في العالم والتي تؤثر في الإمكانيات والتقنيات المتقدمة المتاحة والرامية إلى خرق منظومات الحواسيب بغية سرقة أو تخريب المعلومات أوتدمير أجهزة الحواسيب ومراكزها، إدى إلى التفكير الجدي لتجديد الأساليب والإجراءات الدفاعية والوقائية حسب الإمكانيات المتوفرة لحماية منظومات الحواسيب (أجهزة ومعلومات) منأي خرق أو تخريب.

فكلما تطورت البيئة الإلكترونية كلما فتح فيها مجال أكبر للهاكرز من أجل القيام بأعمالهم التخريبية خصوصا مع ضعف التشريعات والقوانين التي تهتم بحماية المعلومات, وبذلك أصبح امن المعلومات ضرورة حتمية للمؤسسات والأفراد على حد السواء .

ومن خلال إنجازنا لهذا البحث واجهتنا جملة من العراقيل والصعوبات نوجز أهمها فيما يلي :

- نقص المراجع التي تهتم بالموضوع من الناحيتين التقنية والتشريعية وهذا لحداثة موضوع الدراسة .
- عدم تجاوب عينة الدراسة مما شكل صعوبة في العمل .
- عدم فهم بعض المصطلحات المذكورة في إستمارة الإستبانة لطلبة الحقوق كونها مصطلحات تفنية
- وجود صعوبات في توزيع الإستبات وإسترجاعها.

وبالرغم من كل المشاكل التي إعترضتنا إلا أن البحث تم إنجازه بحمد الله وتوفيقه ,توصلنا من خلاله إلى بعض النتائج التي نسعى من خلالها إلى تطوير البحث العلمي .

وبهذا نكون قد وصلنا إلى آخر خطوة في هذا البحث وهذا من خلال تقديم أهم النتائج المتوصل إليها ومدى مطابقتها مع فرضيات الدراسة التي سبق ذكرها لتكون بمثابة حلول مسبقة للإشكالية المطروحة والمتمثلة في أهم التحولات التي طرأت على مصرح الجريمة وكيف يمكننا إحتوائها تقنيا وقانونيا وما هو الدور الذي تلعبه السلطة الاخلاقية في التقليل من وطأة الأزمة .

وفي الأخير نستخلص من خلال هذه الدراسة أن الفرضيات الموضوعة في بداية هذا البحث قد تحققت في مجملها مؤكدة بذلك على أهمية توفير الحماية التقنية والتشريعية من أجل ضمان تداول حر للمعلومات .

الفرضية الأولى:

الخاتمة

على ضوء التطورات المتسارعة والحاصلة في العالم والتي تؤثر في الإمكانيات والتقنيات المتقدمة المتاحة والرامية إلى خرق منظومات الحواسيب بغية سرقة أو تخريب المعلومات أوتدمير أجهزة الحواسيب ومراكزها، إدى إلى التفكير الجدي لتجديد الأساليب والإجراءات الدفاعية والوقائية حسب الإمكانيات المتوفرة لحماية منظومات الحواسيب (أجهزة ومعلومات) منأي خرق أو تخريب.

فكلما تطورت البيئة الإلكترونية كلما فتح فيها مجال أكبر للهاكرز من أجل القيام بأعمالهم التخريبية خصوصا مع ضعف التشريعات والقوانين التي تهتم بحماية المعلومات, وبذلك أصبح امن المعلومات ضرورة حتمية للمؤسسات والأفراد على حد السواء .

ومن خلال إنجازنا لهذا البحث واجهتنا جملة من العراقيل والصعوبات نوجز أهمها فيما يلي :

- نقص المراجع التي تهتم بالموضوع من الناحيتين التقنية والتشريعية وهذا لحداثة موضوع الدراسة .
- عدم تجاوب عينة الدراسة مما شكل صعوبة في العمل .
- عدم فهم بعض المصطلحات المذكورة في إستمارة الإستبانة لطلبة الحقوق كونها مصطلحات تفنية
- وجود صعوبات في توزيع الإستبات وإسترجاعها.

وبالرغم من كل المشاكل التي إعترضتنا إلا أن البحث تم إنجازه بحمد الله وتوفيقه ,توصلنا من خلاله إلى بعض النتائج التي نسعى من خلالها إلى تطوير البحث العلمي .

وبهذا نكون قد وصلنا إلى آخر خطوة في هذا البحث وهذا من خلال تقديم أهم النتائج المتوصل إليها ومدى مطابقتها مع فرضيات الدراسة التي سبق ذكرها لتكون بمثابة حلول مسبقة للإشكالية المطروحة والمتمثلة في أهم التحولات التي طرأت على مصرح الجريمة وكيف يمكننا إحتوائها تقنيا وقانونيا وما هو الدور الذي تلعبخه السلطة الاخلاقية في التقليل من وطأة الأزمة .

وفي الأخير نستخلص من خلال هذه الدراسة أن الفرضيات الموضوعة في بداية هذا البحث قد تحققت في مجملها مؤكدة بذلك على أهمية توفير الحماية التقنية والتشريعية من أجل ضمان تداول حر للمعلومات .

لعل من أبرز ما يمكن أن يقال عن الجهود العربية المبدولة من أجل الحماية من جرائم الحاسب إعتماد مجلس وزراء العدل العرب للقانون العربي الموحد كقانون نمودجي بموجب القرار رقم 229 وبالرجوع إلى المذكرة الإيضاحية لهذا القانون نجد أن الباب السابع الخاص بالجرائم ضد الإشخاص الناتج عن المعالجات المعلوماتية حيث على وجوب حماية الحياة الخاصة الأسرار من أخطار المعالجة الإلكترونية ؛أما المادة 464 فقد نصت على عقابمن يقوم بفعل الدخول بطريقة الغش إلى نظام أوجزء من نظام المعالجة الألية وتعد هذه المحاولة بالرغم من تواضعها من أبرز ما تم على صعيد تعزيز التعاون على المستوى العربي من الناحية التشريعية

وتكللت الجهود العربية في إطار الحماية الفكرية وحق المؤلف خصوصا في إبرام الإتفاقية العربية لحماية حقوق المؤلف التي أوصى بها مؤتمر الوزراء المسؤولين عن الشؤون الثقافية المنعقد في بغداد عام 1981 ؛ كذلك فإن الجمعية المصرية للقانون الجنائي لها إتجاه محمود في هذا الموضوع وتمثل ذلك في مؤتمرها السادس في القاهرة من 25-28 أكتوبر عام 1993 حول جرائم الكمبيوتر والجرائم الأخرى التي أكد المؤتمرون على عالميتها ووجوب تكاثف الجهود لمكافحتها لأنها تمثل وجها سلبيا للتقدم الحضاري ؛ وقد خرجج المؤتمرون بصور السلوك الإجرامي وتوصيات بضرورة التعاون الدولي في مجال أنظمة المعلومات.

إلى جانب هذه الجهود هناك جهود أخرى تتض ح معالمها في الجهود المتعلقة بالملكية الفكرية كالمؤتمر الدولي الأول للملكية الفكرية سنة 1995 ؛ كما عقد في بغداد مؤتمرين لمستجدات الملكية الفكرية سنة1997 ومن توصيات المؤتمر إنشاء محاكم خاصة للبث في النزاعات المتعلقة بالحماية ؛وبعدها عقد المؤتمر الثاني للملكية الفكرية عام 1998.

وكما سبق الإشارة إليه فإن الجرائم المعلوماتية الحديثة طرحت مشاكل كبيرة من الناحية القضائية وذلك لعدم تناسب القوانين القديمة مع هذه المستجدات ومحاولة لمعرفة إذا ما كان المشرع الجزائري يعاني من مشاكل عند عرض هذا النوع من القضايا على المحاكم وكانت الإجابة كما يوضحه الجدول 28 في الصفحة 148

إذن وحسب نتائج الجدول فإن اغلب الطلبة (66,6%) ليسوا على دراية إن كان المشرع الجزائري يتعرض لمشاكل عند طرح القضايا المعلوماتية على المحاكم ، وهذا راجع إلى قلة هذه القضايا في الجزائر من جهة وعدم محاولة الطلبة التعرف على المستجدات الحاصلة في مصرح الجريمة والتشريعات من جهة أخرى؛ أما (33,3%) يرون أن المشرع الجزائري تعترضه العديد من المشاكل والعراقيل عند الفصل في مثل هذه القضايا أما عن أسباب هذه المشاكل فيرجعها الطلبة إلى الأسباب الموضحة في الجدول رقم 27 (أنظر الصفحة 148)

الملحق الأول جداول تفريغ إستمارة الدراسة

لجدول رقم01: عدد طلبة كل قسم حسب السنوات الدراسية

عينة الدراسة	عدد طلبة السنة الأولى	عدد طلبة السنة الثانية	المجمـــوع
طلبة الحقـــــوق	45	105	150
طلبة الإعلام الآلي	20	18	38

الجدول 02: الإستسبانات الموزعة والمسترجعة

عينة الدراسة	عدد الإستمارات الموزعة	عدد الإستمارات المسترجعة	النسبة %
طلبـــة الحقوق	30	30	100
طلبة الإعلام الآلي	08	08	80
المجمـــوع	38	38	100

الجدول 03: عينة الدراسة موزعة حسب الأقسام بالنسبة للمجتمع الأصلي

عينة الدراسة	عدد الإستمارات الموزعة	النسبة المئوية
طلبـــــة الحقـــــوق	30	% 79
طلبة الإعلام الآلي	08	% 21
المجمـــــــوع	38	% 100

الجدول رقم04: وجود فرق بين المجرم المعلوماتي والمجرم التقليدي:

وجود الفرق بين المجرم المعلوماتي والتقليدي	التكرار	النسبة %
نعـــــــــم	33	86,8
لا	05	13,2
المجموع	38	100

الجدول رقم05:الفرق بين المجرم المعلوماتي والمجرم التقليدي

الفرق بين المجرم المعلوماتي والتقليدي	التكرار	النسبة %
1- نوع الجريمة	03	7,8
2- صفات المجرم	06	15,7
3- طريقة إرتكاب الجريمة	10	26,3
2+1	08	21
3+2+1	07	18,5
3+2	04	10,5
المجموع	38	100

الجدول رقم06: مميزات الهاكرز

مميزات الهاكرز	التكرارات		النسبة %
إنسان إجتماعي	03		7,8
إنسان ذكـــــي	30		78,9
مميزات أخرى	05	03)لا يقيم حدودا بين حقوقه وحقوق الآخرين	13,1
		02) انتهازي استغلالي	
المجموع	38		100

الجدول رقمّ07: أسباب الهاكرز للقرصنة

أسباب القرصنة	التكرار	النسبة %
1- مكاسب مالية	15	39,4
2- دوافع شخصية	04	10,5
3- الفضول وحب المغامرة	03	7,8
3+1	08	18,5
3+2+1	08	18,5
المجموع	38	100

الجدول رقم08: تمركز الهاكرز في العالم

سبب تمركز الهاكرز في أمريكا	التكرارات	النسبة%
1- انعدام الوازع الأخلاقي	04	10,5
2- التطور التكنولوجي المذهل	04	10,5
3- إنتشار الثقافة المعلوماتية	12	31,5
3+1	08	21
3+2	04	10,5
3+2+1	06	15,7
المجموع	38	100

الجدول رقم09: مميزات الجريمة الالكترونية

مميزات الجريمة الإلكتروني	التكرار	النسبة %
صعوبة إكتشافها	10	26,4
ذكاء الجاني	08	21
صعوبة تطبيق القانون	10	26,4
3+1	04	10,5
3+2+1	06	15,7
المجموع	38	100

الجدول رقم10: صور قرصنة البرامج

صور قرصنة البرامج	التكرار	النسبة %
تقليد البرنامج	06	15,5
سرقة البرنامج الأصلي	04	10,7
نسخ البرنامج	14	36,8
3+1	06	15,7
3+2+1	06	15,7
2+1	02	5,2
المجموع	38	100

الجدول رقم: 11جرائم الانترنت

جرائم الانترنت	التكرار	النسبة %
الإستدراج اللاأخلاقي	10	26,3
جرائم الإعتداء على المال	04	10,5
جرائم إنتهاك الخصوصية	10	26,3
2+1	04	10,5
3+1	06	15,7
3+2	04	10,5
المجموع	38	100

الجدول رقم:12 جرائم الإعتداء على الخصوصية:

جرائم الإعتداء على الخصوصية	التكرار	النسبة %
إنتحال الشخصية	10	26,4
تشويه السمعة	08	21
الإحتيال والإستلاء على المال	07	18,4
2+1	03	7,8
3+2+1	08	21
3+1	02	5,2
المجموع	38	100

الجدول رقم 13 أغراض الإختراق

أغراض الإختراق	التكرار	النسبة %
أغراض سياسية	06	15,7
أغراض عسكرية	06	15,7
أغراض تجارية	10	26,3
أعراض فردية	15	42,5
المجموع	38	100

الجدول رقم14: طرق الحماية

طرق الحماية	التكرار	النسبة %
عدم وصل الكمبيوتر بالشبكة	02	5,2
إستعمال برامج الحماية	36	94,8
المجموع	38	100

الجدول رقم:15 أسباب إنتشار الفيروسات

أسباب إنتشار الفيروسات	التكرار	النسبة
إنتشار الشبكات	10	% 26,3
عدم إستعمال برامج الحماية	11	% 28,9
وجود ثغرات	06	% 15,7
3+1	04	% 10,5
3+2+1	04	% 10,5
3+2	03	% 7,8
المجموع	38	% 100

الجدول رقم:16 طرق إنتشار الفيروسات

طرق إنتشار الفيروسات	التكرار	النسبة
البريد الإلكتروني	12	% 31,5
متصفح الأنترنت	04	% 10,5
تحميل الملفات	10	% 26,5
3+2+1	08	% 21
2+1	04	% 10,5
المجموع	38	% 100

الجدول رقم17 أعراض الإصابة بالفيروسات

أعراض الإصابة بالفيروسات	التكرار	النسبة
اكتظاظ ذاكرة الحاسب	10	% 26,3
فقدان الملفات	10	% 26,3
تحطيم الفهرس الرئيسي	06	% 15,7
3+1	02	% 5,2
3+2+1	04	% 10,5
3+1	06	% 5,2
المجموع	38	% 100

الجدول رقم: 18 أهمية امن المعلومات

أهمية أمن المعلومات	التكرارات	النسبة
ضرورة	36	%94,8
ترف	02	% 5,2
ليس له دور	00	% 00
المجموع	38	% 100

الجدول رقم:19 وقت حفظ المعلومات

وقت حفظ المعلومات	التكرارات	النسبة
أثناء حفظها	05	% 13,1
أثناء نقلها	03	% 7,8
إثناء الحفظ والنقل	30	% 78,9
المجموع	38	% 100

الجدول رقم:20 وسائل حماية المعلومات

وسائل الحماية	التكرار	النسبة
1- التشفير	12	% 31,5
2- التوقيع الإلكتروني	08	% 21
3- جدران النار	10	% 26,3
3+1	04	% 10,5
3+2+1	04	% 10,5
المجموع	38	% 100

الجدول رقم21 حتمية الإنخراط في مجتمع المعلومات

حتمية الإنخراط في مجتمع المعلومات	التكرارات	النسبة%
نعـــــــــم	37	97,3
لا	10	2,7
المجموع	38	100

الجدول رقم22 خصائص مجتمع المعلومات

خصائص مجتمع المعلومات	التكرارات	النسبة
1- زيادة الإهتمام بالمعلومات	12	% 31,5
2- التطور التقنـــي	12	% 31,5
3- خلق مهن جديدة	10	% 26,3
3+1	02	% 5,2
3+2+1	04	% 10,5
المجموع	38	% 100

الجدول رقم23 وجود إفرازات مجتمع المعلومات على الأخلاق

إفرازات مجتمع المعلومات على الأخلاق	التكرار	النسبة
نعم	36	%94,8
لا	02	% 5,2
المجموع	38	% 100

الجدول24 إفرازات مجتمع المعلومات على الأخلاق

الإفرازات الأخلاقية الجديدة	التكرار	النسبة
1- العزلة الإجتماعية	12	% 31,5
2- تفكك الروابط الأسرية	12	% 31,5
3- الشعور بالدونية	10	% 26,9
3+1	04	% 10,5
المجموع	38	% 100

الجدول رقم25 الإستعمال الانترنت

الإستعمال الأنترنت	التكرار	النسبة%
نعم	36	94,8
لا	02	5,2
المجموع	38	100

الجدول رقم 26 خدمات الانترنت

خدمات الانترنت	التكرار	النسبة %
1- البحث عن المعلومات	12	31,5
2- إستعمال البريد الإلكتروني	10	26,3
3- الدردشة ومنتديات الحوار	08	21
2+1	02	5,2
3+2+1	06	15,7
المجموع	38	100

الجدول رقم27 إطلاع الطلبة على تشريعات حماية المعلومات العالمية

الإطلاع على تشريعات حماية المعلومات	التكرار	النسبة %
نعم	18	60
لا	12	40
المجموع	38	100

الجدول رقم:**28 المشاكل التي تواجه المشرع الجزائري للفصل في القضايا المعلوماتية.**

لمشاكل التي تواجه المشرع الجزائري للفصل في القضايا المعلوماتية.	التكرار	النسبة %
نعم	10	33,3
لا	00	00
لا أدري	20	66,6
المجموع	30	100

الجدول رقم:29 أسباب المشاكل التي يتعرض لها القاضي عند عرض القضايا المعلوماتية

أسباب المشاكل التي يتعرض لها القاضي عند عرض القضايا المعلوماتية	التكرار	النسبة %
1- تقادم النصوص	06	60
2- عدم تمكن القضاة من التقنية	03	30
3-خصوصية الجريمة المعلوماتية	01	10
المجموع	10	100

الجدول رقم: 30 وجود مساعي جزائرية لاحتواء الجرائم المعلوماتية

وجود مساعي جزائرية لاحتواء الجرائم المعلوماتية	التكرارات	النسبة %
نعم	04	13,3
لا	06	20
لاأدرى	20	66,6
المجموع	30	100

الجدول رقم :31 اقتراحات الطلبة

اقتراحات الطلبة	التكرارات	النسبة %
1- استحداث قوانين جديدة	04	13,3
2- تكييف القوانين التقليدية	06	20
2+1	20	66,6
المجموع	30	100

قائمة المراجع

قائمة المراجع:

1. جعفر صادق الحسيني. تكنولوجيا شبكات الحاسب .ط2.عمان : دار وائل للنشر،2006.
2. شاكر، علي كمال . شبكات المعلومات لأخصائي المكتبات والمعلومات . القاهرة : الدار اللبنانية المصرية ،2005.
3. أديب،محمد. شبكات المعلومات :الحاضر والمستقبل القاهرة : المكتبة الاكاديمية،1998.
4. الهادي ،محمد محمد. دورة حياة عملية تطوير نظم المعلوماتية. القاهرة: المكتبة الأكاديمية ،2001.
5. درويش، محمدجمال الدين. التخطيط للمشروعات المعلوماتية . القاهرة : المكتبة الاكاديمية،2002.
6. عوض، نبيل. تكنولوجيا المعلومات ونطور العلم . القاهرة : المكتبة الأكاديمية ،2005.
7. شوقي ,حسام .حماية وأمن المعلومات على الأنترنت .القاهرة :دار الكتب العلمية ,2003 .
8. الغنيمي ,وائل إبراهيم .معجم الشبكات والحايبات : إنجليزي – عربي .بيروت :دار الراتب الجامعية , [د.ت.] .
9. البداينة .ذياب . الأمن وحرب المعلومات . عمان : دار الشروق ,2002.
10. العريان, محمد علي . الجرائم المعلوماتية الإسكندرية :دار الجامعة الجديدة ,2004.
11. محمود عبد الله حسين علي ,سرقة المعلومات المخزنة في الحاسب الآلي ,دار النهضةالعربية القاهرة 2002
12. موسى ،مصطفى محمد .أساليب إجرامية بالتقنية الرقمية :ماهيتها ومكافحتها .القاهرة : دار الوثائق القومية المصرية ،2001.
13. عفيفي. عفيفي كامل .جرائم الكمبيوتر وحقوق المؤلف والمصنفات الرقمية ودورالشرطة والقانون :دراسة مقارنة .ط.2.[د.م]: [د.ن],2000.
14. عفيفي. عفيفي كامل .جرائم الكمبيوتر وحقوق المؤلف والمصنفات الرقمية ودورالشرطة والقانون :دراسة مقارنة .ط.2.[د.م]: [د.ن],2000.
15. الجنبيهي ,منير محمد ؛ الجنبيهي ,ممدوح محمد .جرائم الأنترنت والحاسب الآلي ووسائل مكافحتها .دار الفكر الجامعي :الإسكندرية ,2004.
16. منصور, محمد حسين .المسؤولية الإلكترونية .الإسكندرية :دار الجامعة الجديدة ,2003
17. الجنبيهي ,منير محمد ؛ الجنبيهي ,ممدوح محمد .البنوك الإلكترونية .الإسكندرية :دار الفكر الجامعي ,2005.
18. الجنبيهي ,منير محمد ؛ الجنبيهي , ممدوح محمد . أمن المعلومات الإلكترونية .الإسكندرية :دار الفكر الجامعي , 2005
19. طلية.محمد فهمي .؛ غبد الوهاب ,مثطفى رضا ....وآخرون .فيروسات الحاسب وأمن البيانات ,1996
20. الربيعي ,محمد,شعبان أحمد أحمد ,وآخرون. المعجم الشامل لمصطلحات الحاسب الآلي ة الأنترنت .مكتبة السيكان الرياض 2001ص
21. حجارى , عبد الفتاح بيومي . النظام القانوني لحماية الحكومة الإلكتورنية. الكتاب الثاني و الجنائية المعلوماتية لنظام الحكومة الإلكترونية . الإسكندرية :دار الفكر الجامعي 2003 ص
22. عبير الرضا .الأنترنت :النشأة والأخطار . مؤخودة من مجلة عجمال للعلوم والتكنولوجيا .مج 6.ع.3 ,2001.
23. البياتي , هلال عبود الوسائل الفنية لحماية البرامج ودور التشريع في حمايةالمعلومات . مجلة أبحاث الحاسب .مج 1 ,1996.
24. داود ,حسن الطاهر. الحاسب وامن المعلومات .الرياض : معهد الإدارة العامة,2000.
25. سيد حسين ,فاروق الأنترنت وأحدث ما كتب عنها .بيروت:دار الراتب الجامعية,1999.
26. أبو هبة, نجوى التوقيع الإلكتروني = La signature électronique : تعريفه ,مدى حجيته في الإثبات .القاهرة :دار النهضة العربية ,2002.

27. قنديل , سعيد السيد . التوقيع الإلكتروني : ماهيته ,صوره, حجيته في الإثبات بين التدويل والإقتباس . الإسكندرية : دار الجامعة الجديدة ,2004.
28. حجازي , عبد الفتاح البيومي . التوقيع الإلكتروني في النظم القانونية المقارنة .الإسكندرية : دار الفكر الجامعي.
29. عبد الحق, ط .مدخل إلى المعوماتية : برمجيات الحاسب الشخصي. = Logiciel de PC .البليدة: فصر الكتاب ,2005.
30. عبد الهادي ,محمد فتحي .المعلومات وتكنولوجيا المعلومات على أعتاب قرن جديدة . القاهرة :الدار العربية للكتاب ,2000
31. عباس , طاهر محمود .المكتبات الرقمية وشبكة الأنترنت .القاهرة :المزكزالإصيل ,2003.
32. لعقاب ،محمد. مجتمع الإعلام والمعلومات :ماهيتهوخصائصه .الجزائر :در هومة ،2003.
33. عبد الهادي ، فتحي . المعلومات وتكنولوجيا المعلومات على أغتاب قرن جديد .القاهرة: مكتبة الدار العربية للكتاب .،2000.
34. الهوش ،أبو بكرمحمود. التقنية الحديثة في المغلومات والمكتبات :نحو إستراتيجية عربية لمستقيل مجتمع الملومات .القاهرة: دار الفجر،2002
35. النقري،معن .المعلوماتية والمجتمع / مجتمع ما بعد الصناعة ومجتمع المعلومات .المغرب؛ لبنان :المردز الثقفي العربي،2001.
36. مومني .بشار طلال .مشكلات التعاقد عبر الأنترنت:دراسة مقارنة .الأردن :دار العالم الكتب ,2004.
37. مرسى, نبيل محمد .التقنيات الحديثة للمعلومات .الإسكندرية :دار الجامعة الجديدة، 2005
38. الجنبهي ، منير محمد .الجنبهي ،ممدوح ،منير محمد .الطبيعة القانونية للعقد الإلكتروني .الإسكندرية :دار الفكر الجامعي ،[د.ت.]
39. مغبغب ،نعيم .مخاطر المعلوماتية والأنترنت .لبنان :[د.ن.] 1998.
40. قنديل ,يوسف. نحو إستراتجية لدخول النتاج الفكري باللغة العربية . تونس ؛ الرياض : مكتبة عبد العزيز العامة , 2001.
41. بهاء ,شهين الأنثرنيت والعولنة القاهرة :عالم الكتب ,1999.
42. منصور ,محمد حسين . المسؤولية الإلكترونية ..الإسكندرية :دار الجامعة الجديدة ,2003.
43. عبابنة , محمود محمد .جرائم الحاسب وأبعادها الدولية .عمان :دار الثقافة,2005.
44. نظم المعومات الإدارية
45. نظم المعلومات المفاهيم والتصميم .
46. جعفر صادق الحسيني. تكنولوجيا شبكات الحاسب .ط2.عمان : دار وائل للنشر،2006.
47. شاكر، علي كمال . شبكات المعلومات لأخصائي المكتبات والمعلومات . القاهرة : الدار اللبنانية المصرية ،2005.
48. أديب،محمد. شبكات المعلومات :الحاضر والمستقبل القاهرة : المكتبة الاكاديمية،1998.
49. الهادي ،محمد محمد. دورة حياة عملية تطوير نظم المعلوماتية. القاهرة: المكتبة الأكاديمية ،2001.
50. درويش، محمدجمال الدين. التخطيط للمشروعات المعلوماتية . القاهرة : المكتبة الاكاديمية،2002.
51. عوض، نبيل. تكنولوجيا المعلومات ونطور العلم . القاهرة : المكتبة الأكاديمية ،2005.
52. شوقي ,حسام .حماية وأمن المعلومات على الأنترنت .القاهرة :دار الكتب العلمية ,2003 .
53. الغنيمي ,وائل إبراهيم .معجم الشبكات والحايبات : إنجليزي – عربي .بيروت :دار الراتب الجامعية , [د.ت.] .
54. البداينة .ذياب . الأمن وحرب المعلومات . عمان : دار الشروق ,2002.
55. العريان, محمد علي . الجرائم المعلوماتية الإسكندرية :دار الجامعة الجديدة ,2004.
56. محمود عبد الله حسين علي ,سرقة المعلومات المخزنة في الحاسب الآلي ,دار النهضةالعربية القاهرة 2002
57. موسى ،مصطفى محمد .أساليب إجرامية بالتقنية الرقمية :ماهيتها ومكافحتها .القاهرة : دار الوثائق القومية المصرية ،2001.

58. عفيفي. عفيفي كامل .جرائم الكمبيوتر وحقوق المؤلف والمصنفات الرقمية ودورالشرطة والقانون :دراسة مقارنة .ط.2.[د.م]: [د.ن],2000.
59. عفيفي. عفيفي كامل .جرائم الكمبيوتر وحقوق المؤلف والمصنفات الرقمية ودورالشرطة والقانون :دراسة مقارنة .ط.2.[د.م]: [د.ن],2000.
60. الجنبيهي ,منير محمد ؛ الجنبيهي ,ممدوح محمد .جرائم الأنترنت والحاسب الآلي ووسائل مكافحتها .دار الفكر الجامعي :الإسكندرية ,2004.
61. منصور, محمد حسين .المسؤولية الإلكترونية .الإسكندرية :دار الجامعة الجديدة ,2003
62. الجنبيهي ,منير محمد ؛ الجنبيهي ,ممدوح محمد .البنوك الإلكترونية .الإسكندرية :دار الفكر الجامعي ,2005.
63. الجنبيهي ,منير محمد ؛ الجنبيهي , ممدوح محمد . أمن المعلومات الإلكترونية .الإسكندرية :دار الفكر الجامعي , 2005
64. طلية.محمد فهمي .؛ غبد الوهاب ,مثطفى رضا ....وآخرون .فيروسات الحاسب وأمن البيانات ,1996
65. الربيعي ,محمد,شعبان أحمد أحمد ,وآخرون. المعجم الشامل لمصطلحات الحاسب الآلي ة الأنترنت .مكتبة السيكان الرياض 2001ص
66. حجارى , عبد الفتاح بيومي . النظام القانوني لحماية الحكومة الإلكتورنية. الكتاب الثاني و الجنائية المعلوماتية لنظام الحكومة الإلكترونية . الإسكندرية :دار الفكر الجامعي 2003 ص
67. عبير الرضا .الأنترنت :النشأة والأخطار . مؤخودة من مجلة عجمال للعلوم والتكنولوجيا .مج 6.ع.3 ,2001.
68. البياتي , هلال عبود الوسائل الفنية لحماية البرامج ودور التشريع في حمايةالمعلومات . مجلة أبحاث الحاسب .مج 1 ,1996.
69. داود ,حسن الطاهر. الحاسب وامن المعلومات .الرياض : معهد الإدارة العامة,2000.
70. سيد حسين ,فاروق الأنترنت وأحدث ما كتب عنها .بيروت:دار الراتب الجامعية,1999.
71. أبو هبة, نجوى التوقيع الإلكتروني = La signature électronique : تعريفه ,مدى حجيته في الإثبات .القاهرة :دار النهضة العربية ,2002.
72. قنديل , سعيد السيد . التوقيع الإلكتروني : ماهيته ,صوره, حجيته في الإثبات بين التدويل والإقتباس . الإسكندرية : دار الجامعة الجديدة ,2004.
73. حجازي , عبد الفتاح البيومي . التوقيع الإلكتروني في النظم القانونية المقارنة .الإسكندرية : دار الفكر الجامعي.
74. عبد الحق, ط .مدخل إلى المعوماتية : برمجيات الحاسب الشخصي. = Logiciel de PC .البليدة: فصر الكتاب ,2005.
75. عبد الهادي ,محمد فتحي .المعلومات وتكنولوجيا المعلومات على أعتاب قرن جديدة . القاهرة :الدار العربية للكتاب ,2000
76. عباس , طاهر محمود .المكتبات الرفمية وشبكة الأنترنت .القاهرة :المزكزالإصيل ,2003.
77. لعقاب ،محمد. مجتمع الإعلام والمعلومات :ماهيتهوخصائصه .الجزائر :در هومة ،2003.
78. عبد الهادي ، فتحي . المعلومات وتكنولوجيا المعلومات على أغتاب قرن جديد .القاهرة: مكتبة الدار العربية للكتاب .،2000.
79. الهوش ،أبو بكرمحمود. التقنية الحديثة في المغلومات والمكتبات :نحو إستراتيجية عربية لمستقيل مجتمع الملومات .القاهرة: دار الفجر،2002
80. النقري،معن .المعلوماتية والمجتمع / مجتمع ما بعد الصناعة ومجتمع المعلومات .المغرب؛ لبنان :المردز الثقفي العربي،2001.
81. مومني .بشار طلال .مشكلات التعاقد عبر الأنترنت:دراسة مقارنة .الأردن :دار العالم الكتب ,2004.
82. مرسى, نبيل محمد .التقنيات الحديثة للمعلومات .الإسكندرية :دار الجامعة الجديدة، 2005

83. الجنبهي ، منير محمد .الجنبهي ،ممدوح ،منير محمد .الطبيعة القانونية للعقد الإلكتروني .الإسكندرية :دار الفكر الجامعي ،[د.ت.]
84. مغبغب ،نعيم .مخاطر المعلوماتية والأنترنت .لبنان :[د.ن.] 1998.
85. قنديل يوسف. نحو إستراتجية لدخول النتاج الفكري باللغة العربية . تونس ؛ الرياض : مكتبة عبد العزيز العامة , 2001.
86- Alin .f. le projet InterNet .paris : eyrolles ;1998
87- Alin .f. l'entreprise intranet guide de conduite de projet . paris : eyrolles ;2001
88- Gardarin g.I'internet/ Intranet&base de données .paris : eyrolles ;2000
89- Montagnier.j.pratique des reseaux d'entroprise. paris : eyrolles ;1998
90- Woodcock.joanne.formation aux réseaux .raris :micro application.2001
91- Woodcock.joanne.les réseaux formation de base .raris :micro application.2001