SOUTH VALLEY NATIONAL UNIVERSITY

FACULTY OF COMPUTING AND ARTIFICIAL INTELLIGENCE

الحاسبات والأخلاقيات

COMPUTERS AND ETHICS

© Can Stock Photo - csp11714765

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ (1)

الْحَمْدُ لِلَّهِ رَبِّ الْعَالَمِينَ (2) الرَّحْمَنِ الرَّحِيمِ (3) مَالِكِ يَوْمِ الدِّينِ (4) إِيَّاكَ نَعْبُدُ وَإِيَّاكَ نَسْتَعِينُ (5) اهدنا الصِّرَاطَ الْمُسْتَقِيمَ (6) صِرَاطَ الَّذِينَ أَنْعَمْتَ عَلَيْهِمْ غَيْرِ الْمَغْضُوبِ عَلَيْهِمْ وَلَا الضَّالِّينَ (7)

اللهم صل على سيدنا محمد وعلى أزواجه أمهات المؤمنين وعلى ذريته وآل بيته كما صليت على إبراهيم في العالمين إنك حميد مجيد.

تُعدّ أخلاقيات استخدام الحاسب نظاماً من المبادئ الأخلاقية التي يجب على المستخدم إتباعها أثناء استخدام الحاسب في المنزل، أو الجامعة، أو العمل، حيث قام معهد أخلاقيات الحاسوب (Computer Ethics Institute) بإطلاق عدة توجيهات لكيفية الالتزام بالأخلاق عند استخدام الحاسب، وهي: الحرص على استخدام الحاسب الآلي بما يحترم ويراعي الآخرين، وعدم استخدامه لإيذائهم. حرص المستخدم على عدم حدوث تداخل بين أعماله وأعمال الآخرين على جهاز الحاسب الآلي، وعدم حذف ملفات قد يحتاج إليها شخص آخر. عدم التطفل على عمل شخص آخر موجود على الحاسب الآلي. عدم استخدام الحاسب الآلي لأغراض السرقة. عدم نسخ أو استخدام برمجيات دون دفع ثمنها، وتجنب استخدام موارد حاسوبية خاصة بالآخرين دون إذن. الانتباه للعواقب الاجتماعية للبرنامج الذي يقوم مستخدم الحاسوب بكتابته أو النظام الذي يقوم بتصميمه.

آداب وأخلاقيات عامة يجب مراعاة بعض الأخلاقيات العامة أثناء استخدام الحاسب، فيما يأتي بعض منها: تجنب استعمال الحاسب بشكل خاطئ قد يخرّب قطعه وأجزاءه، خصوصاً الأجهزة العامة كأجهزة المدارس، والجامعات، والمكتبات العامة. الحرص على سلامة أجزاء الجهاز، وبرامجه، ومحتوياته سواء من تحميل برامج تثقل الحاسب أو تسبب تلفه. الالتزام بالقوانين التي وضعت لتنظيم عملية الاستفادة من الحاسب، كالحفاظ على اسم المستخدم وكلمة السر وعدم إعطائها للآخرين من غير المصرح لهم استخدام الأجهزة. الحرص على جودة وفاعلية البرامج التي يتم تطويرها على أن تكون متوافقة مع متطلبات التي طلبها المستخدم. الحرص على عدم استخدام أقراص مضغوطة أو أقراص فلاش تحتوي على فيروسات وبرامج تؤدي إلى تخريب الحاسب.

أعزائي طلاب الحاسبات والمعلومات والذكاء الاصطناعى

مرحبًا بكم في هذا المقرر الذي سيفتح أمامنا أبوابًا جديدة في فهم التكنولوجيا ليس فقط كأداة أو مهنة، ولكن كقوة تؤثر بشكل عميق في حياتنا اليومية وفي مجتمعنا بأسره. ربما اعتدنا على التفكير في البرمجة والشبكات والأنظمة كعالم تقني بحت، حيث الدقة والسرعة والكفاءة هي الملك، ولكن ماذا عن الأبعاد الإنسانية؟ ماذا عن القرارات التي نتخذها والتي قد تؤثر على خصوصية الأشخاص، أمنهم، وحتى حقوقهم؟

في هذا المقرر، "Computers and Ethics"، سنغوص في الأسئلة التي قد لا تبدو واضحة على السطح: كيف يمكن لخط برمجي أن ينتهك خصوصية شخص ما؟ ما هي المسؤولية التي نحملها عندما نصمم خوارزمية قد تؤثر على مستقبل الآلاف؟ وهل يمكن للتكنولوجيا أن تكون محايدة حقًا، أم أنها دائمًا ما تحمل في طياتها قيمًا وتأثيرات أخلاقية؟

أنتم على وشك الانطلاق في رحلة تفكير نقدي، حيث ستتجاوزون المعرفة التقنية التقليدية لتكتشفوا البعد الأخلاقي لكل قرار تقني تتخذونه. ستتعلمون كيف تكونون ليس فقط مبرمجين أو مهندسين مهرة، ولكن أيضًا مواطنين عالميين واعين بأثر التكنولوجيا على البشرية.

فلنبدأ هذه الرحلة معًا، ونفتح نقاشات مثيرة حول كيف يمكننا استخدام التكنولوجيا لصنع عالم أفضل، أكثر عدالةً، وأكثر احترامًا لحقوق الجميع.

سوف نتناول فى هذا الكتاب الموضوعات التالية:

1. الأخلاقيات Ethics.
2. أخلاقيات الحاسب Computer Ethics.
3. أخلاقيات عصر المعلومات The Ethics Of The Information.
4. الجرائم الإلكترونية Cybercrime.
5. الملكية الفكرية وحماية البرامج Intellectual Property and Software Protection.
6. أخلاقيات القوانين والانترنت Ethics Of Laws And The Internet.
7. حقوق المؤلف وحماية البرمجيات Copyright Protection for Software.

Contents

الفصل الأول 10
الأخلاقيات 10
ETHICS 10
أخلاقيات استخدام الحاسوب 11
الأخلاق والدين ..... **Error! Bookmark not defined.**
أخلاقيات محترفي الحاسب ..... **Error! Bookmark not defined.**
الفصل الثانى 21
أخلاقيات الحاسب 21
COMPUTER ETHICS 21
أخلاقيات الحاسب: 21
الخلفية التاريخية لأخلاقيات الحاسب: 22
تعريف أخلاقيات الحاسب: 23
أمثلة موضوعات في أخلاقيات الحاسب: 24
1- أجهزة الحاسب في مكان العمل Computers in the Workplace 24
2- جريمة إلكترونية Computer Crime 25
3- الخصوصية وإخفاء الهوية Privacy and Anonymity 25
4- الملكية الفكرية Intellectual Property 26
5- المسؤولية المهنية Professional Responsibility 26
6- العولمة Globalization 27
7- The Metaethics of Computer Ethics 27
أقسام أخلاقيات الحاسب الآلي 28
أولاً : أخلاقيات استخدام الحاسب بين الشخص ونفسه: 28
ثانياً : أخلاقيات استخدام الحاسب بين الشخص وغيره: 28
ثالثاً : أخلاقيات بين المستخدم والجهاز: 29
المشكلات الشائعة في أخلاقيات الحاسب 29
أولاً بالنسبة للمشاكل المتعلقة بالخصوصية: 30
ثانياً حقوق الملكية الفكرية: 31
ثالثاً: آثار آداب وأخلاقيات استخدام الحاسب على المجتمع. 31

الفصل الثالث 33

أخلاقيات المعلومات 33

The Ethics of the Information 33

تعريف أخلاقيات المعلومات: Information Ethics 34

المعلومات 35

أمن وحماية المعلومات: Information security and protection 36

ما هو الفرق بين الأمن السيبراني وأمن المعلومات؟ 37

ما هو الأمن السيبراني 37

ركائز أمن المعلومات 38

ما هي سياسة أمن المعلومات؟ 40

ما هي أهمية أمن المعلومات؟ 41

أهداف أمن المعلومات 41

عناصر أمن المعلومات 43

أنواع أمن المعلومات 44

تدابير أمن المعلومات 44

مجالات أمن المعلومات 46

شهادات أمن المعلومات 47

تحديات أمن المعلومات 51

كيف تحمي بياناتك من الاختراق؟ 52

طرق حماية المعلومات: 53

الفصل الرابع 55

الجرائم الإلكترونية 55

CYBERCRIME 55

فما هي الجرائم الإلكترونية؟ وما هي أنواعها؟ 55

ما هي خصائص الجرائم الالكترونية؟ 56

أنواع الجرائم الإلكترونية 56

مخاطر الجرائم الإلكترونية 58

الفرق بين الجريمة الإلكترونية والجريمة المعلوماتية؟ 58

أسباب انتشار الجرائم الإلكترونية 58

خصائص الجرائم الإلكترونية 61

أهداف الجرائم الإلكترونية..... 62
الجرائم الإلكترونية واثرها على المجتمع 62
آثار الجرائم الإلكترونية المادية..... 62
من هم مرتكبي الجرائم الالكترونية؟..... 62
مكافحة الجرائم الإلكترونية..... 63
عقوبة جرائم الإنترنت في مصر 63
الفصل الخامس 65
الملكية الفكرية وحماية البرامج 65
Intellectual property and software protection 65
الملكيّة الفكريّة... تعريفها ومفاهيمها..... 65
ما هي الحقوق التي يضمنها قانون الملكية الفكرية ؟ 68
لماذا يجب تطبيق قوانين الملكية الفكرية؟..... 68
أنواع الملكية الفكرية..... 70
أولا: الحقوق التقليدية للملكية الفكرية..... 70
ثانيا: الحقوق الرقمية للملكية الفكرية. 72
برمجيات الحاسب 74
براءة برمجيات 76
الاستنتاج..... 77
الملكية الفكرية وحقوق المؤلف في البيئة الرقمية..... 77
1- الملكية الفكرية في البيئة الرقمية:..... 77
2- حق الملكية الفكرية في البيئة الرقمية:..... 78
3- حق المؤلف في البيئة الرقمية:..... 79
4- إجراءات وطرق الحماية الآلية والقانونية لحقوق المؤلف في بيئة الإنترنت (الرقمية):..... 79
الفصل السادس 82
أخلاقيات القوانين والانترنت 82
ETHICS OF LAWS AND THE INTERNET 82
مميزات الانترنت: 83
ايجابيات الانترنت:..... 83
سلبيات الانترنت:..... 83
المنظور العربي لظاهرة الانترنت: 86

آداب وأخلاقيات استخدام الإنترنت..... 87
احترام خصوصية المعلومات..... 88
تعزيز الرقابة الذاتية..... 88
مراعاة آداب التواصل عبر الإنترنت..... 88
مراعاة حقوق النشر..... 89
الأخلاقيات في العمل والمؤسسات التعليمية..... 89
ضبط أخلاقيات الانترنت:..... 89
لوائح التنظيم الذاتي:..... 89
لوائح التنظيم المساعد:..... 90
آداب وأخلاقيات الإنترنت:..... 92
أهمية آداب الإنترنت..... **Error! Bookmark not defined.**
أمثلة على آداب الإنترنت..... **Error! Bookmark not defined.**
الفصل السابع..... 92
حقوق المؤلف وحماية البرمجيات..... 94
COPYRIGHT PROTECTION FOR SOFTWARE..... 94
حقوق المؤلف..... 94
المصنفات المحمية:..... 94
شروط إكتساب الحماية:..... 94
ما هي حقوق صاحب حق المؤلف:..... 95
إستثناءات من الحماية:..... 95
حماية الأفكار أم التعبير عن الأفكار ؟..... 95
حقوق المؤلف فى البيئه الرقمية..... 96
أنواع المصنفات الرقمية المحمية بحق المؤلف..... 96
برمجيـات وبـرامج الحاسـوب..... 96
الاعتداءات الواقعة على حقوق المؤلف على شبكة الانترنت..... 97
الطبيعة القانونية لبرامج الحاسب:..... 98
أولاً : حماية برامج الحاسب بقانون براءة الاختراع:..... 98
حماية برامج الحاسب بقانون حقوق المؤلف:..... 101
الحق الأدبي لمؤلف برنامج الحاسب:..... 103
الحق المالي لمؤلف البرنامج:..... 104

الوصف القانوني للعقود الواردة على برنامج الحاسب:..... **Error! Bookmark not defined.**
التنظيم القانونى للبرمجيات وقواعد البيانات..... 106
حماية البرمجيات (الملكية الفكرية) ..... **Error! Bookmark not defined.**
حماية الملكية الفكرية ..... **Error! Bookmark not defined.**
أنواع الملكية الفكرية:..... **Error! Bookmark not defined.**
الملكية الفكرية للمصنفات الرقمية:..... **Error! Bookmark not defined.**
برمجيات الحاسوب: ..... **Error! Bookmark not defined.**
الأهمية الاقتصادية لحماية برامج الحاسب الآلى: ..... **Error! Bookmark not defined.**
التطور التشريعى لحماية برامج الحاسب الآلي: ..... **Error! Bookmark not defined.**
الدور الأمنى فى حماية البرمجيات..... 109
الدور الأمنى في حماية البرمجيات..... 111
معوقات الدورالأمني في محاربة قرصنة البرامج، وتجارب الدول المختلفة لمواجهتها..... 113
مقترحات لترشيد الدور الأمني في مواجهة قرصنة البرمجيات..... **Error! Bookmark not defined.**
الحماية الدولية لبرامج الحاسب الآلي..... **Error! Bookmark not defined.**
حماية برمجيات الحاسب الآلي:..... **Error! Bookmark not defined.**
عقود ترخيص برامج الحاسب ..... **Error! Bookmark not defined.**
أهم المراجع 123

الفصل الاول

الأخلاقيات

ETHICS

من المتعارف عليه أنه على مر العصور لكل مهنة أو عمل يزاوله الإنسان أخلاقياته التي يجب الإلتزام بها. وفي عصرنا الحالي أصبحنا كثيرًا ما نسمع عن أخلاقيات استخدام المعرفة أو ما يسمى (أخلاقيات المهنة)، ومن خلال التسمية يمكننا الاستنتاج أن أي مهنة يمارسها الإنسان يوجد لها أخلاقيات وقواعد يجب الإلتزام بها، ومن منطلق الأهمية بدأت العديد من الجامعات والمعاهد العلمية بتدريس الأخلاقيات كجزء من كل تخصص، فمثلا كلية الطب تدرس أخلاقيات مهنة الطب وكلية التربية تدرس أخلاقيات التدريس... إلخ. وفي القرن الماضي بدأت حياة الأمم تتغير بسبب ظهور علم جديد وعصر جديد هو عصر (تكنولوجيا المعلومات- عصر الحواسيب)، هذا العلم الذي قدم خدمة كبيرة للبشرية ووفر لها حياة أفضل وأسهل في أغلب مجالات الحياة وعلى كافة المستويات سواء تلك التي تتمثل في عملية التواصل فيما بين الأفراد عن طريق الاتصالات أو إرسال الرسائل وغيرها، أو في تسيير الأعمال كأنظمة المعلومات التي تسير أعمال الشركات والمنظمات المختلفة.

فقد وفر لنا جهاز الحاسب خدمات كثيرة يطول الحديث في حصرها سنذكر منها على سبيل المثال إمكانية تخزين بياناتنا وملفاتنا الخاصة والقيام بأعمالنا المختلفة. وبعد التطور الذي طرأ بظهور شبكة الإنترنت أصبح بإمكاننا التواصل فيما بيننا بسرعة أكبر وإرسال البيانات المختلفة سوأ أكانت بيانات شخصية أو بيانات تتعلق بأعمالنا من وإلى أي مكان في العالم. إذًا كل ما ذكرناه حتى الآن جميل ورائع طالما أصبح بإمكاننا القيام بكل ما نحتاجه بواسطة الحاسوب فما المشكلة؟. الحقيقة التي كانت غائبة عن أذهاننا في الفترة الماضية أنه مع كل تلك الخدمات التي حصلنا عليها من تطور تكنولوجيا المعلومات هناك مشكلة خطيرة جدا صاحبت هذا التطور، كيف لا وقد أصبحنا نسمع بجرائم لا عدد لها تسمى (جرائم الحاسب) تحدث في العالم يقوم بها مجرمون من نوع جديد يطلق عليهم (مجرمي الحاسب)، فهذا تم اختراق جهازه والعبث بمحتوياته والاطلاع على خصوصياته وآخر تم سرقة برنامجه وبيعه، وهذه المؤسسة تم اختراق قاعدة بياناتها ومعرفة أسرارها وأخرى تم تدمير قاعدة بياناتها، ودولة تم كشف أسرارها، وفي هذا البنك تم سرقة عدد من أرصدة العملاء، والأمثلة كثيرة لا مجال لحصرها.

أخلاقيات استخدام الحاسوب

آداب وأخلاقيات استخدام الحاسب ضرورية من أجل احترام الآخرين وحقوقهم، من دون التعدي على أي أحد بسبب سرعة التواصل في الوقت الحالي.

- استخدم الحاسب لأغراض إيجابية فقط، وحافظ على نواياك الحسنة طوال استخدامك للحاسب.
- استخدم الحاسب بصورة محترمة ولا تتسبب في أذى للآخرين، ولا تخترق أجهزة أي شخص أو تتجسس على ملفاته وحساباته، ولو عرض عليك ذلك بمقابل، ارفضه.
- لا تحاول سرقة حسابات الآخرين، ولا تستخدم حاسبك في عمليات نصب أو احتيال.
- لا تسرق أفكار الآخرين ومجهودهم وكتبهم وبرامجهم وتنسبها لنفسك.
- استخدم الحاسب في الأمور المفيدة التي لها نتائج ايجابية على المجتمع.

تُعدّ أخلاقيات استخدام الحاسب نظاماً من المبادئ الأخلاقية التي يجب على المستخدم اتباعها أثناء استخدام الحاسب في المنزل، أو المدرسة، أو العمل، حيث قام معهد أخلاقيات الحاسوب(Computer Ethics Institute) بإطلاق عدة توجيهات لكيفية الالتزام بالأخلاق عند استخدام الحاسب، وهي كما يأتي:

- الحرص على استخدام الحاسب الآلي بما يحترم ويراعي الآخرين، وعدم استخدامه لإيذائهم.
- حرص المستخدم على عدم حدوث تداخل بين أعماله وأعمال الآخرين على جهاز الحاسب الآلي، وعدم حذف ملفات قد يحتاج إليها شخص آخر.
- عدم التطفل على عمل شخص آخر موجود على الحاسب الآلي.
- عدم استخدام الحاسب الآلي لأغراض السرقة.
- عدم نسخ أو استخدام برمجيات دون دفع ثمنها، وتجنب استخدام موارد حاسوبية خاصة بالآخرين دون إذن.
- الانتباه للعواقب الاجتماعية للبرنامج الذي يقوم مستخدم الحاسوب بكتابته أو النظام الذي يقوم بتصميمه.

آداب وأخلاقيات عامة

يجب مراعاة بعض الآداب والأخلاقيات العامة أثناء استخدام الحاسب، فيما يأتي بعض منها:

1. تجنب استعمال الحاسب بشكل خاطئ قد يخرّب قطعه وأجزاءه، خصوصاً الأجهزة العامة كأجهزة المدارس، والجامعات، والمكتبات العامة.
2. الحرص على سلامة أجزاء الجهاز، وبرامجه، ومحتوياته سواء من تحميل برامج تثقل الحاسب أو تسبب تلفه.

3. الالتزام بالقوانين التي وضعت لتنظيم عملية الاستفادة من الحاسب، كالحفاظ على اسم المستخدم وكلمة السر وعدم إعطائها للآخرين من غير المصرح لهم استخدام الأجهزة.
4. الحرص على جودة وفاعلية البرامج التي يتم تطويرها على أن تكون متوافقة مع متطلبات التي طلبها المستخدم.
5. الحرص على عدم استخدام أقراص مضغوطة أو أقراص فلاش تحتوي على فيروسات وبرامج تؤدي إلى تخريب الحاسب.

هناك بعض المصطلحات والتعريفات الهامة التى يجب أن تكون على دراية كاملة بها فى مجال أخلاقيات الحاسبات

الأخلاق على عكس القوانين التي تفرض قانونًا ما هو صواب أو خطأ. توضح الأخلاق آراء المجتمع حول ما هو صواب وما هو خطأ.

الأخلاق هي مجموعة من المبادئ الأخلاقية التي تحكم سلوك فرد أو مجموعة من الناس. أخلاقيات الحاسوب هي تطبيق المبادئ الأخلاقية على استخدام الحاسوب والإنترنت. تشمل الأمثلة حقوق الملكية الفكرية وسياسات الخصوصية وآداب التعامل عبر الإنترنت أو "آداب التعامل".

الأخلاق هي مجموعة من القواعد للسلوك الصحيح، وهو نظام يستخدم لتعديل وتنظيم سلوك. إنه نظام جودة في الأفعال البشرية نحكم من خلاله على صواب أو خاطئ، جيد أو سيء. هذا النظام يخلق الأشخاص الأخلاقيين الذين يمتلكون فضائل مثل حب الآخرين والرحمة والرغبة في العدالة؛ وبالتالي فإنه يبني سمات الشخصية في الناس. على وجه الخصوص، الأخلاق هي نص للبقاء نتبعه في حياتنا اليومية.

معايير أخلاقية

المعيار الأخلاقي هو المعيار الذي نقارن به أفعال البشر لتحديد صلاحهم أو شرهم. هذا المعيار يوجه ويفرض السياسة.

وقد أصدرت العديد من الجمعيات المهنية الوطنية والدولية والمنظمات وثائق مدونة الأخلاقيات لإعطاء المبادئ التوجيهية السلوكية الأساسية للمهنيين والمستخدمين الحوسبة. وتشمل هذه ال:

- **رابطة آلات الحوسبة**

مدونة الأخلاق والسلوك المهني

- **الجمعية الأسترالية للكمبيوتر**

مدونة أخلاقيات الرابطة

مدونة قواعد السلوك المهني للACS

- **جمعية الكمبيوتر البريطانية**

مدونة قواعد السلوك فيBCS

مدونة الممارسات الجيدة (تقاعد مايو 2011)

- **معهد أخلاقيات الحاسوب**

عشر وصايا لأخلاقيات الكمبيوتر

- **Ieee**

IEEEمدونة الأخلاق

مدونة قواعد السلوك فيIEEE

<u>علاقة الأخلاق بالدين والقانون</u>

علاقة الأخلاق بالدين والقانون هي علاقة معقدة ومترابطة، حيث تتداخل هذه المفاهيم بشكل كبير في تشكيل سلوك الأفراد والمجتمعات. دعنا نناقش كل جانب منها على حدة:

1. **علاقة الأخلاق بالدين:**

- الدين عادة ما يكون مصدرًا رئيسيًا للمبادئ والقيم الأخلاقية. كثير من الأديان تقدم تعاليم حول ما هو "خير" وما هو "شر"، وما يجب على الإنسان فعله وما يجب تجنبه.
- التعاليم الدينية تسهم في توجيه الضمير الأخلاقي للأفراد، وتوفر إطارًا للسلوك القويم. على سبيل المثال، معظم الأديان تشدد على قيم مثل الصدق، الأمانة، التعاون، والتسامح.
- رغم ذلك، ليس بالضرورة أن تكون جميع الأخلاق مستمدة من الدين؛ فهناك أيضًا أخلاقيات قائمة على فلسفات إنسانية وعقلانية مستقلة عن الدين.

علاقة الأخلاق بالقانون:

- القانون هو مجموعة من القواعد التي تفرضها الدولة لتنظيم سلوك الأفراد في المجتمع. في حين أن الأخلاق قد تكون شخصية وغير ملزمة قانونيًا، فإن القانون يعبر عن الأخلاق الجماعية التي يلتزم بها المجتمع.
- كثيرًا ما يتأثر القانون بالأخلاق العامة، ولكن لا يعني ذلك أن كل ما هو أخلاقي يصبح قانونًا أو أن كل ما هو قانوني يكون أخلاقيًا. على سبيل المثال، قد يكون من الأخلاقي مساعدة شخص محتاج، لكن القانون لا يُلزم بذلك.
- القوانين تهدف إلى تنظيم المجتمع والحفاظ على النظام العام، وتفرض عقوبات على السلوكيات التي يُعتبر أنها تضر بالمصلحة العامة، بينما الأخلاق قد تكون ذات طابع شخصي أكثر وتتعلق بالنية والضمير الفردي.

العلاقة بين الأخلاق والدين والقانون:

- أحيانًا يتداخل الدين والأخلاق والقانون بشكل كامل، كما هو الحال في بعض الدول التي تتبنى قوانين مستمدة من الشريعة أو القوانين الدينية الأخرى.
- في المجتمعات الاخرى يتم التفريق بين القانون والدين، حيث يُصاغ القانون على أساس المصلحة العامة بغض النظر عن المعتقدات الدينية.

ثلاثة مبادئ أخلاقية مفيدة:

- يعتبر الفعل أخلاقيًا إذا استفاد المجتمع بأسره من الفعل.
- يعتبر الفعل أخلاقيًا إذا تم التعامل مع الناس على أنه غاية وليس وسيلة لتحقيق غاية.
- يعتبر الفعل أخلاقيًا إذا كان عادلاً لجميع الأطراف المعنية.

الفرق بين المبادئ Morals والأخلاق Ethics والقوانين Laws

المبادئ(Morals) ، الأخلاق(Ethics) ، والقوانين (Laws) هي مفاهيم مترابطة ولكنها مختلفة من حيث المعنى والنطاق. كل منها يوجه السلوك البشري، ولكن بطرق مختلفة. إليك توضيح الفرق بينها:

1. المبادئ:(Morals)

- **التعريف** :المبادئ هي معتقدات شخصية أو ثقافية حول ما هو صواب وما هو خطأ. غالبًا ما تتشكل هذه المعتقدات من خلال التربية، العائلة، المجتمع، أو الدين.
- **الطبيعة** :شخصية وداخلية. تختلف من شخص لآخر بناءً على القيم التي نشأ عليها.
- **النطاق** :المبادئ تحدد السلوك الفردي وتُعتبر تعبيرًا عن "الضمير". هي مجموعة من القواعد الذاتية التي يشعر الفرد بأنه يجب أن يتبعها.
- **مثال** :قد يرى شخص ما أن الكذب دائمًا خاطئ بناءً على معتقداته الشخصية، حتى في الظروف التي قد يعتبرها البعض مبررة.

2. الأخلاق:(Ethics)

- **التعريف** :الأخلاق هي مجموعة من المبادئ أو القواعد التي تحدد ما هو السلوك الصحيح أو الخطأ ضمن سياق معين، عادة ما تكون هذه المبادئ مرتبطة بمجال مهني أو اجتماعي.
- **الطبيعة** :اجتماعية ومهنية. تعتمد الأخلاق على المعايير المجتمعية أو المهنية التي يتم الاتفاق عليها في جماعة معينة.
- **النطاق** :ترتبط بالممارسات المهنية أو المجالات العامة، مثل الأخلاقيات الطبية أو أخلاقيات العمل. تسعى الأخلاق إلى تنظيم السلوك بطريقة عادلة ومنصفة بناءً على المبادئ المتفق عليها.
- **مثال** :في الطب، تُعتبر السرية وعدم الكشف عن معلومات المرضى مبدأً أخلاقيًا يجب على الأطباء احترامه.

3. القوانين:(Laws)

- **التعريف** :القوانين هي مجموعة من القواعد المكتوبة التي تفرضها الحكومات لتنظيم سلوك الأفراد والمجتمعات. القوانين إلزامية، ويجب على الجميع الالتزام بها.
- **الطبيعة** :رسمية وقانونية. يضعها المجتمع أو الدولة وتكون ملزمة قانونيًا.
- **النطاق** :أوسع من الأخلاق والمبادئ، لأنها تشمل كل المجتمع وتفرض عقوبات على من ينتهكها.

- **مثال** :قانون المرور الذي يُلزم الأفراد بارتداء حزام الأمان أثناء القيادة. قد لا يرى البعض أن عدم ارتداء الحزام غير أخلاقي، ولكن القانون يُلزم بذلك ويُعاقب من يخالفه.

الاختلافات الأساسية:

- **المصدر**:
  - المبادئ تأتي من القيم الشخصية أو الدينية.
  - الأخلاق تأتي من معايير مهنية أو اجتماعية.
  - القوانين تُصاغ من قبل السلطات الحكومية.
- **الإلزام**:
  - المبادئ شخصية وغير ملزمة قانونيًا.
  - الأخلاق إلزامية في إطار المهني أو الاجتماعي، ولكن ليست دائمًا مدعومة بالقانون.
  - القوانين إلزامية قانونيًا، وتُفرض عقوبات على من يخالفها.
- **الطبيعة**:
  - المبادئ تتعلق بالضمير الشخصي.
  - الأخلاق تتعلق بالسلوك الصحيح داخل مجموعة أو مهنة.
  - القوانين تهدف إلى تنظيم المجتمع بشكل عام.

الحاسب الآلي، أو ما يعرف أيضًا بـ **الكمبيوتر**، هو جهاز إلكتروني يستخدم لمعالجة البيانات وتخزينها وتنظيمها. يقوم الحاسب الآلي بتنفيذ مجموعة من العمليات الحسابية والمنطقية بسرعة فائقة ودقة عالية، وهو يُعتبر من أبرز الاختراعات التي أحدثت ثورة في جميع جوانب الحياة.

مكونات الحاسب الآلي:

1. **المكونات المادية:(Hardware)**
   - **وحدة المعالجة المركزية :(CPU)** وهي "عقل" الحاسب، تقوم بمعالجة البيانات وتنفيذ الأوامر.
   - **الذاكرة :(RAM)** ذاكرة الوصول العشوائي، حيث يتم تخزين البيانات بشكل مؤقت أثناء تشغيل البرامج.

- **وحدات التخزين** :مثل الأقراص الصلبة(Hard Drives) ، والأقراص الصلبة من نوعSSD ، وتستخدم لتخزين البيانات بشكل دائم.
- **الأجهزة الطرفية** :تشمل لوحة المفاتيح، الفأرة، الشاشة، الطابعات، وغيرها من الأجهزة التي تسمح بالتفاعل مع الحاسب.

2. **المكونات البرمجية:(Software)**

- **نظام التشغيل** :**(Operating System)** مثلWindows ، macOS، Linux، وهو الذي يدير موارد الحاسب ويوفر واجهة للمستخدمين للتفاعل مع الجهاز.
- **البرامج والتطبيقات** :مثل برامج معالجة النصوص) مثل Microsoft (Word، البرامج الرسومية، البرامج المحاسبية، وغيرها التي تسمح بأداء وظائف محددة.

أنواع الحواسيب:

1. **الحواسيب المكتبية** :**(Desktop Computers)** تستخدم عادةً في المكاتب والمنازل، وتكون أكبر حجمًا.
2. **الحواسيب المحمولة** :**(Laptops)** تتميز بخفة وزنها وسهولة حملها، وتحتوي على جميع مكونات الحاسوب في جهاز صغير متنقل.
3. **الخوادم** :**(Servers)** تُستخدم لتوفير خدمات معينة مثل تخزين البيانات أو استضافة المواقع، وهي أقوى وأكبر حجمًا من الحواسيب العادية.
4. **الحواسيب اللوحية** :**(Tablets)** أجهزة صغيرة محمولة تعتمد بشكل أساسي على شاشات اللمس.
5. **الحواسيب العملاقة** :**(Supercomputers)** تُستخدم في مجالات البحث العلمي، الذكاء الاصطناعي، والمعالجة الكثيفة للبيانات.

وظائف الحاسب الآلي:

1. **معالجة البيانات** :يتم تحويل البيانات الخام إلى معلومات مفيدة من خلال العمليات الحسابية والمنطقية.
2. **التخزين** :يمكن للحاسب تخزين كميات ضخمة من البيانات على وحدات التخزين المختلفة.

3. **التواصل** :من خلال الإنترنت أو الشبكات المحلية، يمكن استخدام الحاسب لتبادل المعلومات بين الأجهزة المختلفة.
4. **تشغيل البرامج** :سواء كانت برامج مكتبية أو تطبيقات متقدمة، يمكن للحاسب تشغيل العديد من البرمجيات لأداء المهام المتنوعة.

أهمية الحاسب الآلي:

- **في التعليم** :يستخدم بشكل واسع في المدارس والجامعات لإعداد البحوث، الدراسة عن بُعد، والمحاكاة التعليمية.
- **في العمل** :لا غنى عنه في المكاتب والشركات لإدارة البيانات، المعاملات المالية، وتصميم المنتجات.
- **في الحياة اليومية** :يتم استخدامه في التسوق الإلكتروني، الترفيه، التواصل الاجتماعي، والخدمات الصحية.

تطور الحاسب الآلي:

منذ اختراع أول حاسوب في منتصف القرن العشرين، شهدت صناعة الحواسيب تطورًا هائلًا. أصبح الحاسب اليوم أصغر حجمًا، أسرع، وأكثر كفاءة، وقد ساهم في تغيير كيفية تفاعل البشر مع التكنولوجيا.

أخلاقيات الحاسب هو المجال الذي يتعامل مع القضايا الأخلاقية التي تنشأ عن استخدام أجهزة الكمبيوتر والتكنولوجيا. ويغطي موضوعات مثل الخصوصية والأمن والدقة والإنصاف في تصميم وتطوير وتطبيق أنظمة الكمبيوتر. تهدف أخلاقيات الكمبيوتر إلى ضمان استخدام التكنولوجيا بطريقة مسؤولة وخاضعة للمساءلة، مع المراعاة الواجبة لحقوق ورفاهية الأفراد والمجتمع ككل.

تتمثل أخلاقيات استخدام الحاسوب في مجموعة من القواعد والمبادئ الأساسية التي يجب اتباعها لضمان استخدام الحاسوب بطريقة صحيحة ومسؤولة .ومن أبرز هذه الأخلاقيات:

1. **الاحترام :**يجب احترام خصوصية الأفراد وعدم الاطلاع على معلوماتهم الشخصية دون إذنهم.
2. **الصدق:** يجب الامتناع عن اختراق أو تعديل أي نظام حاسوبي بدون إذن صريح.
3. **العدالة:** يجب التعامل بشكل عادل مع الأفراد وعدم الاستخدام المفرط للمعلومات الشخصية أو التحيز بحسب الجنس أو العرق أو الدين.

4. **النزاهة:** يجب عدم استخدام الحاسوب للغش أو الخداع أو الاحتيال، سواء في الأعمال التجارية أو الأكاديمية.
5. **الابتعاد عن الإساءة:** يجب تجنب تحميل أو نشر أي محتوى يشكل تشويهًا لصورة الشخص أو الجهة المعنية.
6. **الاحترام للملكية الفكرية** :يجب احترام حقوق الملكية الفكرية وعدم النسخ أو الاستخدام غير المشروع للبرامج أو الملفات المحمية بموجب حقوق الطبع والنشر.
7. **التحليل والتفكير النقدي** :في حالة التعامل مع المعلومات، يجب التحليل والتفكير النقدي للمعلومات المتاحة قبل القيام بإجراءات معينة.

كيفية استخدام أجهزة الكمبيوتر بطريقة مسؤولة وأخلاقية

تعد أخلاقيات الحاسب مجالًا حاسمًا يدرس الآثار الأخلاقية لتكنولوجيا الكمبيوتر وتأثيرها على المجتمع. وهو يتعمق في الاستخدام المسؤول والأخلاقي لأجهزة الكمبيوتر، ويتناول مختلف القضايا الأخلاقية والاجتماعية التي تنشأ في العصر الرقمي. يعد فهم أخلاقيات الكمبيوتر أمرًا ضروريًا لأنه يرشد الأفراد والمنظمات في **اتخاذ قرارات مستنيرة بشأن استخدام** التكنولوجيا، مما يضمن توافقها مع المبادئ الأخلاقية والقيم المجتمعية.

من وجهات نظر مختلفة، تشمل أخلاقيات الكمبيوتر مجموعة واسعة من المواضيع. فيما يلي بعض الأفكار الرئيسية:

1. **الخصوصية وحماية البيانات :**أحد الجوانب المهمة لأخلاقيات الكمبيوتر هو حماية المعلومات الشخصية وخصوصية البيانات. مع تزايد كمية البيانات التي يتم جمعها وتخزينها بواسطة أجهزة الكمبيوتر، من الضروري وضع ضمانات لمنع الوصول غير المصرح به إلى المعلومات الحساسة أو إساءة استخدامها أو استغلالها.
2. **الملكية الفكرية** :تتناول أخلاقيات الكمبيوتر أيضًا الاستخدام الأخلاقي للملكية الفكرية، بما في ذلك حقوق النشر وبراءات الاختراع والعلامات التجارية .ويؤكد على أهمية احترام والاعتراف بحقوق المبدعين والمبتكرين في المجال الرقمي.
3. **الأمن السيبراني** :يعد ضمان أمن أنظمة وشبكات الكمبيوتر جانبًا مهمًا آخر من أخلاقيات الكمبيوتر. وهو ينطوي على تنفيذ تدابير للحماية من الوصول غير المصرح به، وانتهاكات البيانات، والهجمات السيبرانية، وحماية كل من الأفراد والمنظمات من الضرر المحتمل.
4. **الفجوة الرقمية** :تعترف أخلاقيات الكمبيوتر بأهمية سد الفجوة الرقمية، والتي تشير إلى الفجوة بين أولئك الذين لديهم إمكانية الوصول إلى التكنولوجيا وأولئك الذين لا يستطيعون الوصول إليها. ويسلط الضوء على الحاجة إلى تكافؤ الفرص والوصول إلى الموارد الرقمية، وتعزيز الشمولية والحد من عدم المساواة الاجتماعية.

6. **الذكاء الاصطناعي الأخلاقي والأتمتة** :مع تقدم تقنيات الذكاء الاصطناعي والأتمتة، تستكشف أخلاقيات الكمبيوتر الآثار الأخلاقية لاستخدامها. فهو يثير تساؤلات حول المساءلة والشفافية والعدالة في خوارزميات صنع القرار، مما يضمن تصميم أنظمة الذكاء الاصطناعي ونشرها بشكل أخلاقي.

1. الاعتبارات الأخلاقية في جمع البيانات واستخدامها:

أهمية الموافقة المستنيرة والشفافية في ممارسات جمع البيانات.

الموازنة بين فوائد الرؤى المستندة إلى البيانات وحقوق الخصوصية الفردية.

الاعتبارات الأخلاقية في تبادل البيانات والوصول إلى طرف ثالث.

2. الحوسبة المسؤولة والأثر البيئي:

تعزيز الممارسات المستدامة في تصميم وتصنيع والتخلص من أجهزة الكمبيوتر.

تقليل استهلاك الطاقة والبصمة الكربونية في عمليات الحوسبة.

الاعتبارات الأخلاقية في إدارة النفايات الإلكترونية وإعادة تدويرها.

3. وسائل التواصل الاجتماعي والتواصل عبر الإنترنت:

معالجة قضايا التنمر الإلكتروني والتحرش وخطاب الكراهية.

تعزيز المواطنة الرقمية والسلوك المسؤول عبر الإنترنت.

الاعتبارات الأخلاقية في الإشراف على المحتوى وإدارة المنصة.

4. اتخاذ القرارات الأخلاقية في الذكاء الاصطناعي والأتمتة:

ضمان العدالة والشفافية والمساءلة في خوارزميات الذكاء الاصطناعي.

التخفيف من التحيز والتمييز في عملية صنع القرار الآلي.

الفصل الثانى

أخلاقيات الحاسب

COMPUTER ETHICS

أخلاقيات الحاسب:

من بين العديد من التقنيات التكنولوجية الحديثة التي ظهرت في القرن العشرين، يعد الحاسب أكثرها أهمية وأشدها تأثيرًا في حياة الإنسان، وينظر إلى الثورة المرتبطة بظهور الحاسب على أنها أبرز في تأثيرها الاجتماعي من الثورة الصناعية التي ظهرت في القرن التاسع عشر، والتي غيرت كثيراً في حياة الإنسان.

تدل الإحصائيات المتعلقة بحجم استخدام الحاسب وأنظمة المعلومات والإنترنت على تأثيرها الكبير في حياتنا، ففيما يخص الإنترنت، هنالك ما يزيد على 700 مليون مستخدم لهذه الشبكة في جميع أنحاء العالم.

وعلى الرغم من أن الحاسب قدم فوائد لا تحصى في شتى المجالات الصحية، والاتصالات، والمواصلات، والصناعة وغيرها، فإنه في الوقت نفسه خلق مجموعة من المشاكل الاجتماعية والأخلاقية، الناتجة عن سوء استعمال الحاسب من قبل بعض المستخدمين، ويكفي لكي ندرك بعض المشاكل الناتجة عن انتشار الحاسب أن نعلم أن قيمة المبالغ التي ترتبط بجرائم الحاسب التي يتم التبليغ عنها، تبلغ 50 مليار دولار سنوياً.

الخلفية التاريخية لأخلاقيات الحاسب:

إن البدايات الحقيقية لـ"أخلاقيات الحاسب" كانت في معهد MIT مع الأستاذ البروفيسور نوبيرت واينر Norbert Wiener في بدايات الأربعينات من القرن الماضي، عندما طرح تساؤلاً عن إمكانية أن تتحول التكنولوجيا إلى "شيطان" يتسبب في دمار البشرية.

وتوجه واينر بكتابه المعروف The Human Use of Human Being الذي تناول فيه رؤيته الفلسفية لأخلاقيات الحاسب، والتي طرح فيها مسائل مهمة، مثل الهدف الذي يسعى له الإنسان في حياته، ومبادئ العدالة التي يجب أن تسود المجتمع، ومجموعة الأسئلة المتعلقة بأخلاقيات الحاسب، ومجموعة من الأمثلة التطبيقية على المشكلات الأخلاقية لاستخدام الحاسب.

بدأ الدكتور دون باركر Donn Parker في الستينات من القرن الماضي في التركيز على ممارسات غير الأخلاقية وغير القانونية لاستخدام الحاسب، ويعلق الدكتور باركر على هذه الممارسات بقوله: "يبدو أن الناس عندما يدخلون مراكز الكمبيوتر يضعون مبادئهم الأخلاقية خلف الباب".

وعلى الرغم من أن أدبيات "أخلاقيات الحاسب" بدأت في الأربعينات من القرن الماضي فإن مصطلح "أخلاقيات الحاسب" لم يظهر إلى العلن إلا في منتصف السبعينات، وكان ذلك على يد الدكتور والتر مانر Walter Maner.

كان الدكتور مانر أول من أدخل مقررًا جامعيًا باسم "أخلاقيات الحاسب"، وأقام العديد من ورش العمل التي تتناول هذا الموضوع في المؤتمرات العلمية التي كانت تقعد في الولايات المتحدة.

في الثمانينات من القرن الماضي أصبحت المشكلات الأخلاقية والاجتماعية المرتبطة بالحاسب من ضمن القضايا العامة التي تشغل المجتمع في الولايات المتحدة وأوروبا. وفي منتصف الثمانينات نشر الأستاذ الدكتور جيمس مور James Moor في جامعة Dartmouth مقالة مهمة بعنوان "ماهي أخلاقيات الحاسب؟".

اتسم عقد التسعينات بغزارة المساهمات من قبل المفكرين المهتمين "بأخلاقيات الحاسب"، فبالإضافة إلى إسهامات غوتير بارن، كانت هناك العديد من المساهمات عبر مجموعة من المفكرين المعروفين من أمثال سيمون ريجرسون Simon Rogerson، وديان مارتن Dianne Martin، و كيلث ميلر Keith Miller التي صبت في نفس الاتجاه.

تعريف أخلاقيات الحاسب:

من وجهة نظر والتر مانر Walter Maner فإن "أخلاقيات الكمبيوتر": *هو الفرع الذي يبحث في المشكلات الأخلاقية التي خلقتها تكنولوجيا الحاسب.*

أما دوبرا جونسن Deborah Johnson فقدمت تعريفًا آخر في كتابها Computer Ethics،

"أخلاقيات الحاسب": *أنه الحقل الذي يبحث في كيف فرض الحاسب مجموعة من المشكلات الأخلاقية، والأسئلة الأخلاقية، مما يفرض علينا تطبيق النظريات الأخلاقية التقليدية بنظرة جديدة.*

عام 1989 قدم تيريل بيونم Terrell Bynum تعريفًا آخر "لأخلاقيات الحاسب"، ويرجع هذا التعريف في الأصل إلى واينر، الذي طرحه في كتابه The Human Use Of Human Being.

وفقًا لهذا التعريف فإن حقل أخلاقيات الحاسب يحدد ويحلل تأثير تكنولوجيا المعلومات على القيم الإنسانية والاجتماعية من قبيل الصحة والديمقراطية والخصوصية والأمن والملكية والحرية.

من جهة أخرى قدم دونالد غوتيربارن Donald Gotterbarn تعريفه الذي يرى فيه أن حقل أخلاقيات الحاسب "يجب أن ينظر إليه على أنه أحد فروع أخلاق المتخصصين، والتي تعني بوضع معايير وضوابط ممارسة تخصص معين". ومن خلال هذه الرؤية فإن غوتيربارن اهتم بصياغة ميثاق شرف Code of Ethics لهندسة البرمجيات Software engineering.

خلال التسعينيات، ظهرت دورات جامعية جديدة، ومراكز بحث، ومؤتمرات، ومجلات، ومقالات، وكتب مدرسية، واشتركت فيها مجموعة متنوعة من الباحثين والموضوعات الإضافية. على سبيل المثال، قاد مفكرون مثل دونالد جوتيربارن وكيث ميلر وسيمون روجرسون وديان مارتن - بالإضافة إلى منظمات مثل Computer Professionals for Social Responsibility وElectronic Frontier Foundation وACM-SIGCAS مشاريع ذات صلة بالحوسبة والمسؤولية المهنية.

عندما قرر استخدام مصطلح "أخلاقيات الحاسب" في منتصف السبعينيات، عرّف والتر مانر المجال على أنه مجال يبحث في "المشكلات الأخلاقية التي تفاقمت أو تحولت أو خلقتها تكنولوجيا الحاسب".

أمثلة موضوعات في أخلاقيات الحاسب:

1. أجهزة الحاسب في مكان العمل.
2. جرائم الحاسب.
3. الخصوصية وإخفاء الهوية.
4. الملكية الفكرية.
5. المسؤولية المهنية.
6. العولمة.
7. The Metaethics of Computer Ethics.

1- أجهزة الحاسب في مكان العمل Computers in the Workplace

باعتبارها "أداة عالمية" يمكنها -من حيث المبدأ- أداء أي مهمة تقريبًا، من الواضح أن أجهزة الحاسب تشكل تهديدًا للوظائف. على الرغم من أنهم يحتاجون أحيانًا إلى الإصلاح، إلا أن أجهزة الحاسب لا تتطلب النوم، ولا تتعب، ولا تعود إلى المنزل مريضة أو تأخذ إجازة للراحة والاسترخاء. في الوقت نفسه، غالبًا ما تكون أجهزة الحاسب أكثر كفاءة من البشر في أداء العديد من المهام. لذلك، فإن الحوافز الاقتصادية لاستبدال البشر بأجهزة محوسبة عالية جدًا. في

الواقع، في العالم الصناعي، تم بالفعل استبدال العديد من العمال بأجهزة محوسبة- صرافو البنوك، عمال السيارات، مشغلو الهاتف، الطابعون، رسامو الرسوم، حراس الأمن، عمال خطوط التجميع، وما إلى ذلك. بالإضافة إلى ذلك، حتى المهنيين مثل الأطباء والمحامين والمدرسين والمحاسبين وعلماء النفس يجدون أن أجهزة الكمبيوتر يمكنها أداء العديد من واجباتهم المهنية التقليدية بشكل فعال للغاية.

2- جريمة إلكترونية Computer Crime

في عصر "فيروسات" الحاسب والتجسس الدولي من قبل "المتسللين" الذين يبعدون آلاف الأميال، من الواضح أن أمن الحاسب هو موضوع مثير للقلق في مجال أخلاقيات الحاسب. لا تكمن المشكلة في الأمن المادي للأجهزة (حمايتها من السرقة والحرائق والفيضانات وما إلى ذلك)، بل تكمن في "الأمان المنطقي"، الذي يقسمه Spafford و Heaphy و Ferbrache [Spafford، et al، 1989] إلى خمسة النواحي:

1. الخصوصية والسرية.
2. النزاهة - ضمان عدم تعديل البيانات والبرامج دون تفويض مناسب.
3. الخدمة غير منقوصة.
4. الاتساق Consistency- ضمان أن البيانات والسلوك الذي نراه اليوم سيكون هو نفسه غدًا.
5. التحكم في الوصول إلى الموارد توفر أنواع البرامج الضارة، أو "التهديدات المبرمجة"، تحديًا كبيرًا لأمن الكمبيوتر. وتشمل هذه "الفيروسات"، التي لا يمكن أن تعمل من تلقاء نفسها، بل يتم إدراجها في أجهزة الحاسب أخرى.

وتشمل هذه "**الفيروسات**"، التي لا يمكن أن تعمل من تلقاء نفسها، بل يتم إدراجها في برامج الحاسب الأخرى؛ "**الديدان**" التي يمكن أن تنتقل من آلة إلى آلة عبر الشبكات، وقد يكون لها أجزاء منها تعمل على أجهزة مختلفة؛ "**أحصنة طروادة**" التي تبدو وكأنها نوع واحد من البرامج، لكنها في الواقع تسبب الضرر وراء الكواليس؛ "**القنابل المنطقية**" التي تتحقق من ظروف معينة ثم تنفذ عندما تنشأ تلك الظروف؛ و"**البكتيريا**" أو "**الأرانب**" التي تتكاثر بسرعة وتملأ ذاكرة الكمبيوتر. عادة ما يتم ارتكاب جرائم الحاسب، مثل الاختلاس أو زرع القنابل المنطقية، من قبل أفراد موثوق بهم لديهم إذن باستخدام نظام الحاسب. لذلك، يجب أن يهتم أمان الحاسب أيضًا بإجراءات مستخدمي الحاسب الموثوق بهم.

3- الخصوصية وإخفاء الهوية Privacy and Anonymity

كانت الخصوصية من أولى موضوعات أخلاقيات الحاسب التي تثير الاهتمام العام. على سبيل المثال، في منتصف الستينيات، أنشأت الحكومة الأمريكية بالفعل قواعد بيانات كبيرة من المعلومات حول المواطنين العاديين (بيانات التعداد، وسجلات الضرائب، وسجلات الخدمة العسكرية، وسجلات الرفاهية، وما إلى ذلك). لسوء الحظ، يمكن أيضًا

استغلال الخصوصية وإخفاء الهوية لتسهيل الأنشطة غير المرغوب فيها وغير المرغوب فيها بمساعدة الكمبيوتر في الفضاء الإلكتروني، مثل غسيل الأموال، وتجارة المخدرات، والإرهاب، أو استغلال الضعفاء (انظر [Marx، Nissenbaum] and [2001، 1999]).

4- الملكية الفكرية Intellectual Property

أحد المجالات الأكثر إثارة للجدل في أخلاقيات الكمبيوتر يتعلق بحقوق الملكية الفكرية المرتبطة بملكية البرمجيات. يعتقد بعض الأشخاص، مثل ريتشارد ستالمان الذي أسس مؤسسة البرمجيات الحرة، أنه لا ينبغي السماح بملكية البرمجيات على الإطلاق. ويدعي أن جميع المعلومات يجب أن تكون مجانية، ويجب أن تكون جميع البرامج متاحة للنسخ والدراسة والتعديل من قبل أي شخص يرغب في ذلك [ستلمان، 1993]. ويرى آخرون أن شركات البرمجيات أو المبرمجين لن يستثمروا أسابيع وأشهر من العمل وأموالاً كبيرة في تطوير البرمجيات إذا لم يتمكنوا من استرداد الاستثمار في شكل رسوم ترخيص أو مبيعات [Johnson، 1992].

تدعي صناعة البرمجيات أن مبيعات ملايين الدولارات تضيع بسبب هذا النسخ. تعد الملكية مسألة معقدة نظرًا لوجود العديد من الجوانب المختلفة للبرنامج الذي يمكن امتلاكه وثلاثة أنواع مختلفة من الملكية:

حقوق النشر والأسرار التجارية وبراءات الاختراع.

يمكن للمبرمج أن يمتلك الجوانب التالية من البرنامج:

- ✓ تمت كتابة "source code_" بواسطة المبرمج (المبرمجين) بلغة كمبيوتر عالية المستوى مثل Java أو C ++.
- ✓ " object code_"، وهو ترجمة لغة آلية لكود المصدر.
- ✓ "ال خوارزمية algorithm"، وهي تسلسل أوامر الآلة التي يمثلها كود المصدر وكود الكائن.
- ✓ " look and feel_" البرنامج، وهي الطريقة التي يظهر بها البرنامج على الشاشة ويتفاعل مع المستخدمين.

5- المسؤولية المهنية Professional Responsibility

يمتلك المتخصصون في مجال الحاسب معرفة متخصصة وغالبًا ما يكون لديهم مناصب تتمتع بالسلطة والاحترام في المجتمع. لهذا السبب، يمكنهم التأثير بشكل كبير على العالم، بما في ذلك العديد من الأشياء التي يقدرها الناس. إلى جانب هذه القوة لتغيير العالم يأتي واجب ممارسة تلك القوة بمسؤولية [Gotterbarn، 2001]. يجد متخصصو الكمبيوتر أنفسهم في مجموعة متنوعة من العلاقات المهنية مع أشخاص آخرين [جونسون، 1994]، بما في ذلك:

تتضمن هذه العلاقات مجموعة متنوعة من المصالح، وفي بعض الأحيان يمكن أن تتعارض هذه المصالح مع بعضها البعض. لذلك، سيكون محترفو الكمبيوتر المسؤولون على دراية بتضارب المصالح المحتمل ويحاولون تجنبه.

6- العولمة Globalization

تتطور أخلاقيات الحاسب اليوم بسرعة إلى مجال أوسع وأكثر أهمية، والذي يمكن أن يسمى بشكل معقول "أخلاقيات المعلومات العالمية". تعمل الشبكات العالمية مثل الإنترنت وخاصة شبكة الويب العالمية على ربط الناس في جميع أنحاء الأرض. كما لاحظت كريستينا جورنياك-كوتشيكوسكا في ورقتها البحثية، "ثورة الكمبيوتر ومشكلة الأخلاق العالمية" [Gorniak-Kocikowska، 1996]، لأول مرة في التاريخ، الجهود المبذولة لتطوير معايير السلوك المتفق عليها بشكل متبادل، والجهود المبذولة للنهوض والدفاع عن القيم الإنسانية، يتم صنعها في سياق عالمي حقيقي.

7- The Metaethics of Computer Ethics

علم الأخلاق هو دراسة الفكر الأخلاقي واللغة الأخلاقية. بدلاً من معالجة أسئلة حول الممارسات الصحيحة والخطأ، وما هي إلتزاماتنا تجاه الآخرين أو الأجيال القادمة - أسئلة حول ما يسمى بالأخلاق "المعيارية" - تتساءل الميتا الأخلاق عن ماهية الأخلاق في الواقع. يهتم عالم ما وراء الأخلاق بما إذا كان يمكن أن تكون هناك معرفة بالحقائق الأخلاقية، أو فقط المشاعر والمواقف الأخلاقية، ويسأل كيف نفهم الخطاب الأخلاقي مقارنة بأشكال الكلام والكتابة الأخرى.

أقسام أخلاقيات الحاسب الآلي

تنقسم أخلاقيات الحاسب الآلي إلى ثلاثة أقسام:

أولاً : أخلاقيات استخدام الحاسب بين الشخص ونفسه:

وهنا تبرز أهمية التربية ووجود الوازع الديني والأخلاقي لمراقبة الذات لعدم جدوى القوانين عندما يتعامل الشخص مع نفسه.

ومن الأخلاقيات التي يجب علينا الالتزام بها: احترام الذات وعدم تعريضها للأخطار التي تنعكس على المستخدم فقط. مثال على ذلك: عدم إضاعة الوقت عند استخدام الحاسب الآلي، وعدم النظر إلى المحرمات، وعدم الاطلاع على خصوصيات الغير حتى لو كانت متاحة، وأخيراً وليس آخراً عدم الإضرار بالجسم وإعطائه قسطاً من الراحة وعلى وجه الخصوص العينين.

لذلك يجب علينا زرع الأخلاق في نفوس طلابناوموظفينا في كلياتنا ومعاهدنا لأنه لا يوجد ضابط لهذه الأفعال سوى مراقبة الشخص لنفسه.

ثانياً : أخلاقيات استخدام الحاسب بين الشخص وغيره:

هذا النوع من الأخلاقيات نستطيع أن نطبقه بوضع بعض الأنظمة والقوانين التي تحمي المستخدمين والأجهزة أيضاً. ولكن يبقى المحور الأساسي لتطبيق هذه الأنظمة وهو الوازع الشخصي.

ومن أهم الأمثلة لهذا النوع:

1- احترام الملكية الفكرية Intellectual Property.

1- يجب علينا وضع مصدر الأفكار والصور والمقالات المقتبسة وعدم سرقه الأعمال والادعاء أنها من صنعنا وعدم نسخ البرامج واستخدامها بالمجان وطبعا هذا واضح في

مجال تكنولوجيا المعلومات ويمكن استخدام المصادر المفتوحة بدلا من ننسب أعمال ليست ملكنا إلينا.

2- الحفاظ على خصوصية وأسرار الآخرين وعدم نشرها ويتضمن ذلك بالطبع عدم الإضرار بالآخرين والاطلاع على ملفاتهم بالتجسس أو صنع وإرسال الفيروسات والبرامج التخريبية.

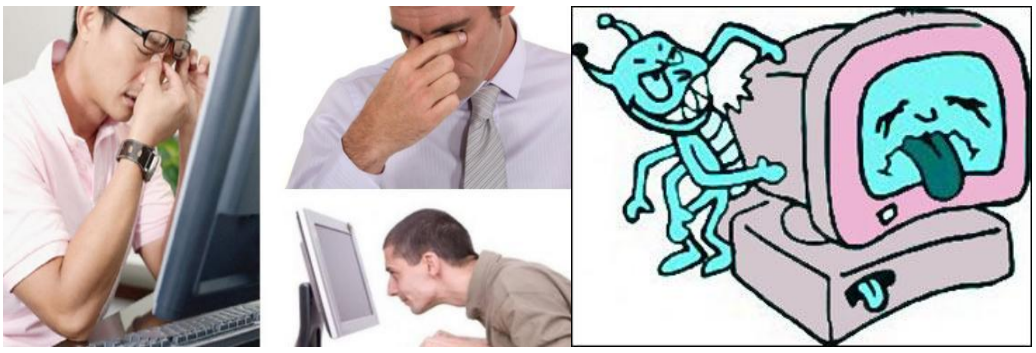
3- عدم التجني على الغير سواء للونهم أو عرقهم أو دينهم أو مستواهم الاجتماعي أو المساس بسمعتهم أو الانتقام منهم والتجني عليهم.

ثالثاً : أخلاقيات بين المستخدم والجهاز:

1. عدم إساءة استعمال الآلة computer Abuse خصوصاً العام منها كأجهزة المدارس والجامعات والمكتبات العامة.
2. الحرص على سلامة أجزاء الجهاز وبرامجه ومحتوياته سواء من تحميل برامج تثقل قد تسبب تلف الأجهزة.
3. الالتزام بالقوانين التي وضعت لتنظيم عملية الاستفادة من الحاسب كالحفاظ على اسم المستخدم وكلمة السر وعدم إعطائها للآخرين من غير المصرح لهم استخدام الأجهزة.

لا يوجد معايير أخلاقية يتم فرضها علي مستخدمي الحاسوب أثناء استخدامه مما يخلق نوع من الحرية واعتقاد الكثير أن فعل أي شيء هو أمر عادي وبسيط جداً، ولكن يجب على الجميع معرفة آداب وأخلاقيات استخدام الحاسب لكي يحترم الآخرين فقد يؤدي عدم الأخلاقيات إلي إيذاء شخص نفسيا والتأثير عليه بشكل كبير واهم أخلاقيات وآداب استخدام الحاسب.

المشكلات الشائعة في أخلاقيات الحاسب.



هناك الكثير من الأضرار التي قد تحدث من خلال الحاسوب سواء أضرار شخصية أو أضرار للآخرين ومن أبرز هذه المشكلات الشائعة في أخلاقيات الحاسب.

أولاً بالنسبة للمشاكل المتعلقة بالخصوصية:

فهنا نجد أن هناك الكثير من الاهتمامات التى تتعلق بهذا الموضوع مثل:

أ-القرصنة (الإختراق)

القرصنة هي ببساطة عبارة عن سرقة محتوى مؤسسة أو شركة أو شخص أخر بهدف الربح من هذا أو توزيع هذا المحتوى المسروق..

أما الإختراق فهو التسلل غير المشروع إلى أى جهاز الحاسب أو شبكة بهدف سرقة محتويات هذا الحاسبأو ابتزاز صاحب هذا الحاسب مقابل مبلغ من المال أو شئ أخر..

أو استخدام هذا الحاسب فى عمليات اختراق اخرى حيث يمكن للمتسلل اختراق مستويات الأمان الخاصة بأنظمة الحاسبأو الشبكات ويمكنه الحصول على وصول غير مصرح به إلى أجهزة الحاسب الأخرى.

ب- البرامج الضارة أو البرمجيات الخبيثة

هنا نعني البرامج الضارة التي يتم إنشاؤها من قبل المخترقين لتعطيل أو السيطرة على أنظمة الحاسب. من ضمن أنواع البرامج الضارة والشائعة هي الفيروسات وبرامج التجسس والديدان وأحصنة طروادةوفيروس الفدية أو المسمى بالرانسوم وير Ransomware وغيرهم.

يمكن للفيروس العادى حذف الملفات من القرص الصلب الخاص بحسابك الشخصى بينما تستطيع برامج التجسس جمع البيانات من جهاز الحاسب وإرسالها إلى المخترق للإطلاع عليها، كما يقوم فيروس الفدية بتشفير جميع البيانات على جهازكولن يقوم بفكها إلا عندما تقوم بإرسال مبلغ الفدية إلى المخترق وغيرها من البرامج الضارة والخبيثة.

جـ- حماية البيانات والمعروفة أيضًا باسم خصوصية المعلومات أو خصوصية البيانات أيضاً من ضمن آداب وأخلاقيات استخدام الحاسب

فهي عبارة عن عملية حماية البيانات التي تقوم بالتأثير على التوازن بين حقوق خصوصية الأفرادمع السماح في الوقت نفسه باستخدام البيانات لأغراض تجارية كالإعلانات وغيرها...

فكما سمعنا فى الآونة الأخيرة عن الكثير من الشركات التى قامت ببيع بيانات الأشخاص لأغراض مشبوهةوكانت من أشهر هذه الشركات هي شركة" فيسبوك "وفضيحتها مع شركة "كامبريدج أنالاتيكا" لذا فهذه نقطه هامة جداً فى آداب وأخلاقيات استخدام الحاسب.

د- إخفاء هوية المستخدمين

وهي وسيلة للحفاظ على هوية المستخدمين من خلال مختلف التطبيقات كالفى بى إن VPN وغيرهم من التطبيقات.

ثانياً حقوق الملكية الفكرية:

التي تعد جزء لا يتجزأ من العمود الفقرى الخاص بآداب وأخلاقيات استخدام الحاسب.

أ- **حقوق الطبع والنشر:** وهي شكل من أشكال قوانين الملكية الفكرية والتي توفر بدورها حقوق النشر والتوزيع والاستخدام للمؤلف وحده.وهذا يعني أن أي فكرة قام المؤلف بإنشائها لا يمكن استخدامها أو توزيعها أو نشرها من قبل أي شخص آخر دون أخذ إذن المؤلف.وبالطبع يتم احترام هذه القوانين وادب وأخلاقيات استخدام الحاسوب بشكل عام،فى الخارج ويوجد قوانين وعواقب صارمة لمن يقوم بمخالفة هذه القوانين،ولكن – مع الأسف – فى وطننا العربى لا توجد منظومة قوانين شاملة يتم تطبيقها على أرض الواقع للمخالفينوالأشخاص الذين يقومون بانتهاك حقوق الطبع والنشر ولكننا نتمنى أن يتم تنظيم وتطبيق قوانين خاصة بهذا الموضوع فى المستقبل القريب.

ب- سرقة المحتوى: وهي ببساطة عبارة عن عملية نسخ ونشر عمل شخص آخر دون ذكر صاحب هذا العمل أو دون أخذ إذن صاحب هذا المحتوى.

وهذا عمل خبيث حيث أنك تقوم بعمل يشبه سرقة عمل شخص آخر ونشر هذا العمل أو توزيعه وكأنه عملك أنت الخاص.

جـ- الكراك Crack: هو نوع من أنواع القرصنة والذي يتم استخدامه كوسيلة لاقتحام أنظمة البرامج من خلال تجاوز ميزات ونظم الأمان الخاصة بهذا البرنامج. وهي ببساطة طريقة لتخطي خطوات التسجيل والتفعيل عند تثبيت أحد البرامج. ويتم استخدام هذه الطريقة لتخطى تفعيل البرامج،

حيث – وكما نعلم – يجب عليك شراء البرامج التى تريد استخدامها ولكن هذا لا يحدث فى كثير من الأحيان ويقوم الأشخاص بتحميل البرامج المقرصنة والتى تكون مُفعلة ولا تحتاج إلى أى شراء وهذه البرامج تم تفعيلها بواسطة الكراك.

د- ترخيص البرامج: هي ببساطة عبارة عن اتفاقية بين الشخص أو الشركة صاحبة البرنامج وبائع أو موزع هذا البرنامج. وتسمح هذه الإتفاقية للبائعين ببيع واستخدام هذه البرامج أو المواد الرقمية باتباع اتفاقية الترخيصولكن ستظل الملكية الخاصة بهذه البرامج تابعة لمالك البرنامج الأصلي والذى يمتلك كافة حقوق الطبع والنشر، ولكننا نقصد هنا أنه يتم منح البائعين أو الموزعين أو المستخدمين تراخيص لاستخدام هذه البرامج أو المواد الرقمية بناءً على اتفاقية الترخيص.

ثالثاً: آثار آداب وأخلاقيات استخدام الحاسب على المجتمع.

بالطبع لا يمكننا التحدث عن آداب وأخلاقيات الحاسب دون التحدث عن أثارها فى المجتمع الذى نعيش فيه. وبعض هذه الأثار هي:

أ- الوظائف: تم إلغاء بعض الوظائف بسبب التكنولوجيا بينما أصبحت بعض الوظائف أكثر بساطة

حيث استحوذت أجهزة الحاسب على الشركات والموسسات احكومية وغير الحكومية.
فمثلا في الماضي كان يجب عليك انتظار ساعي البريد حتى تقوم باستلام الرسائل من الخارج من أحد أصدقاءك أو عائلتكوكان هذا يستغرق أياماً وربما أسابيع، بينما يمكنك يمكنك الآن إرسال الرسائل فوراً على الإنترنت والتسوق وكل هذه الأشياء بنقرة واحدة بينما من قبل كنت تقوم باتخاذ خطوات كثيرة متعددة لأداء مهمة ما.
ولكن هناك أيضاً جوانب سلبية للتكنولوجية، حيث هناك أيضًا مخاوف أخلاقية بشأن صحة وسلامة الموظفين الذين يمرضون من الجلوس المستمر والتحديق على شاشات الكمبيوتروالكتابة على لوحة المفاتيح أو النقر فوق الماوس.
ب- التأثير البيئي: حيث تأثرت البيئة بأجهزة الحاسب والإنترنت، حيث أن استخدام الكثير من الوقت في استخدام الحاسب يزيد من استهلاك الطاقة مما يؤدي بدوره إلى زيادة انبعاثات الغازات الدفيئة وزيادة معدل ثاني أكسيد الكربون في الجو والذي بدوره يؤدي إلى الاحتباس الحراري.
ج- التأثير الاجتماعي: حيث تساعد أجهزة الحاسب والإنترنت الناس على البقاء على اتصال مع العائلة والأصدقاء.كما أصبحت وسائل التواصل الاجتماعي شعبية جدا في الوقت الحاضر.
كان هذا موضوعنا اليوم عن بعض الأشياء الهامة التي تتحدث عن آداب وأخلاقيات استخدام الحاسب.

الفصل الثالث

أخلاقيات المعلومات

The Ethics of the Information

مقدمة

التكنولوجيا بجميع أشكالها وأنواعها في العصر الحاضر وبخاصة الحديثة منها، مثل أجهزة الكومبيوتر والإنترنت والهواتف المحمولة والكاميرات الرقمية وألعاب الفيديو، قد وجدت لتسهل وتيسر للإنسان والمجتمع حياته ورفاهيته. لكن الواقع الحالي يؤكد على أن هناك من يجهل أو يتجاهل الأهداف الأساسية من اختراع وتطوير هذه التكنولوجيات، كما لا يعرف كيفية استخدامها استخداما أخلاقيا سليما، والمثال على ذلك، الاستخدام غير الأخلاقي لشبكة الإنترنت، من اعتداء على الخصوصيات والتجسس المعلوماتي وسرقة الهويات الشخصية وانتهاك حقوق الملكية الفكرية، وسرقة البعض للنتاج الفكري للآخرين من بحوث ومقالات ونسبها لأنفسهم، أو سرقة الأرصدة والأموال البنكية عبر التحويل الإلكتروني، أو سرقة البرامج أو إعادة نسخها، أو إتلاف وإزالة وتشويه والتلاعب بالبيانات والمعلومات، أو التخريب والتدمير الإلكتروني لأنظمة الكومبيوتر أو الترويج لمواد ومحتويات ضارة غير هادفة عبر رسائل بالبريد الإلكتروني أو في الإساءة إلى أشخاص وتلويث وتشويه سمعتهم، والمخاطر التي تنجم عن التحاور مع الآخرين عبر مواقع المحادثة أو ما يسمى بغرف الدردشة (الشات). وكذلك من يستخدمون الهواتف الجوالة لإزعاج الآخرين بالمعاكسات أو نشر صور مخلة بالآداب عبر كاميرات هذه الهواتف.

يقصد بأخلاقيات التكنولوجيا: هي الأخلاقيات المتعلقة بمستخدميها التي تحكم تصرفاتهم وسلوكياتهم نحوها، وتتضمن مجموعة من القواعد والقوانين لكي يلتزم بها الأفراد وتبنى عليها قراراتهم وأفعالهم عند استخدام هذه التكنولوجيا. وقد تكون هذه الأخلاقيات بين الفرد المستخدم للتكنولوجيا ونفسه أو بينه وبين الآخرين، هذا بالإضافة إلى أخلاقيات بين المستخدم والمكونات المادية للتكنولوجيا، والتي تشمل الحرص على سلامة الأجهزة ومحتوياتها من التكسير والإتلاف.

تدفق المعلومات إلى حياتنا عبر قنوات متعددة مثل التليفزيون والراديو والكتب وشبكة الإنترنت؛ فنحن نعاني -كما يقول البعض- من تخمة معلوماتية. ولكن ما هي المعلومات؟

إن مفهوم المعلومات من المفاهيم العميقة التي تضرب بجذورها في علم الرياضيات، غير أن له أهمية بالغة في حياتنا اليومية؛ فالحمض النووي يقدم المعلومات التي تُكّون أجسادنا، ونحن نتعلم من خلال المعلومات التي تتدفق إلى أذهاننا، ونتواصل مع بعضنا من خلال نقل المعلومات بطرق متعددة مثل الثرثرة وأثناء المحاضرات والقراءة.

تعريف أخلاقيات المعلومات: Information Ethics

يقصد بالأخلاقيات مجموعة القواعد التي تنظم العلاقة بين الأفراد والمؤسسات في المجتمع، بغرض ضبط السلوكيات، والتحكم فيها، وتحديد الحقوق والواجبات، وجودة الأداء. ويطلق على هذه القواعد مسميات كثيرة منها أخلاقيات المهنة أو العمل، وشرف المهنة، وآداب المهنة، والقيم المهنية، ونحوها من المصطلحات التي تحدد الواجبات التي ينبغي أن يلتزم بها من ينتمي إلى مهنة معينة. وبالنسبة لمفهوم (أخلاقيات المعلومات) على وجه الخصوص، وهو في الواقع ما يعنينا بشكل أكثر في بيئة العمل، فيشمل الضوابط الأخلاقية من القيم والتشريعات التي تحكم النشاط المعلوماتي في مؤسسات المعلومات. فينبغي أن تتبنى مهنة المعلومات دستورًا أو تشريعًا ينظم الأخلاقيات التي تحكم علاقة المنتمين إلى هذه المهنة بمؤسسات المعلومات والعاملين والمستفيدين والناشرين والمجتمع بشكل عام، فإن القواعد الثابتة تساعد المهني على تحديد موقفه وفقاً لتقاليد المهنة والأصول المتعارف عليها."

تُعرّف أخلاقيات المعلومات: بأنها إحدى فروع فلسفة الأخلاق الكبيرة المعنية بالممارسات السلوكية للبشر وقواعد منظوماتهم الاجتماعية، وهي تندرج تحت مظلة الأخلاق التطبيقية التي تشمل أيضاً أخلاقيات التعامل مع الإنسان الآخر، ومع الحيوان، ومع البيئة، كما تشمل الأخلاقيات الطبية، والتجارية، والصناعية، والسياسية، والعسكرية، وأخلاقيات العمل، وغيرها، وبدورها تشمل أخلاقيات المعلومات . التي تبلورت خلال الأربعة عقود الماضية فقط . أخلاقيات استخدام المكتبات ومصادر المعلومات، وأخلاقيات البحث العلمي، وأخلاقيات استخدام التقنية ووسائل الاعلام والاتصال، وأخلاقيات استخدام الانترنت وبيئة شبكات التواصل الاجتماعي.

ساهمت تكنولوجيا المعلومات والاتصالات وخصوصاً في السنوات العشر الأخيرة التي رافقت الانتشار الواسع لشبكات التواصل الاجتماعي، ساهمت في خلق تحديات غير مألوفة بالنسبة لأخلاقيات المعلومات، وهناك اليوم ثلاث قضايا أو تحديات رئيسية ترتبط بأخلاقيات المعلومات في العصر الرقمي وتحديداً في البيئة المفتوحة للمعلومات التي لم تعد تخضع لأي عوائق أو قيود مرتبطة ببث وتداول المعلومات، ويمكن اختزال تلك التحديات في الحقيقة، والمسؤولية، وحرية التعبير، وبما أن المعلومات في قالبها الرسمي أو التقليدي تخضع للنقد أو المراجعة والتدقيق قبل بثها ونشرها، فإنها في البيئة المفتوحة للمعلومات

تتجاوز كل قواعد الاتصال، وتسبح المعلومات في فضاءها الرقمي بحرية مطلقة لتمثّل صعوبة كبيرة للمتلّقي العادي في إدراك وفهم الرسالة التي تحملها، وما إذا كانت حقيقة أو مظللة، فالكثير من المعلومات فعل محمود، ولكن فقط في حال كانت تلك المعلومات دقيقة وحديثة ومفيدة.

المعلومات

تعرف المعلومات بأنها مجموعة من البيانات طرأت عليها عمليّات تغيير ومُعالجة حتى تحمل معنى وأهمية، ويكون ارتباطها وثيقاً بسياقٍ ما، ويمكن استخدامها في عدة مجالات نظراً لتعددية المعاني التي تحملها، ويعتبر هذا المصطلح له علاقة وثيقة بكلٍّ من المعرفة والتعليمات والتواصل والمعاني. تصّنف هذه المعلومات إلى عدة أنواع من أبرزها:

- المعلومات التطويرية: ويطلق عليها أيضاً المعلومات الإنمائية، ويشمل هذا النوع المعلومات التي يتم الحصول عليها من قراءة ومطالعة الكتب والمقالات، والتي يمكن للإنسان من خلالها اكتساب عدد من المصطلحات والحقائق الحديثة التي تهدف إلى رفع المستوى العلمي للإنسان وتوسيع دائرة الإدراك لديه.
- المعلومات الإنجازية: وهو نتاج ما يحصل عليه الفرد من مصطلحات ومفاهيم جديدة تُحفزه على إتمام عمله وإنجازه على أكمل وجه، وبالتالي اتخاذ القرار الصائب.
- المعلومات التعليمية: هو ما يَكتسبه الطالب خلال وجوده على مقاعد الدراسة طول فترة تعليمه بشتّى مراحلها، ويكون مصدرها المقرّرات الدراسية.
- المعلومات الفكرية: هي مجموعة من الفرضيّات والنظريات المُرتبطة بنوعٍ ما من العلاقات التي يمكن العثور عليها بين أبعاد مشكلة ما.
- المعلومات البحثية: وهي تلك المعلومات التي تعتمد على إجراء البحوث والتجارب والتوصّل لنتائجها للوصول إلى المعلومات اللازمة، وقد تكون من علمية أو أدبية.

- المعلومات الأسلوبية النظامية: ويضمّ هذا النوع جميع المَعلومات ذات العلاقة بالأساليب العلميّة التي تتيح للباحث الفرصة لتأدية البحث بشكل دقيق جداً.
- المعلومات الحافزة و لمعلومات السياسية و المعلومات التوجيهية والمعلومات الفلسفية.

أمن وحماية المعلومات: Information security and protection

يُعرف أمن المعلومات بأنّه أحد فروع العلم الباحث في مجال توفير الحماية اللازمة للمعلومات ومنع الوصول إليها وهدرها من غير ذوي الصلاحية، وحمايتها من أيّ تهديد خارجي، ويشمل هذا المصطلح(Information security)، وفي بعض الأحيان يتمّ اختصار هذا الاسم على النحو التالي(Info Sec) : الأدوات والطرق والإجراءات اللازمة الواجب توفرّها لتحقيق الحماية من المخاطر التي قد تواجهها من الداخل والخارج. ويُعتبر هذا العلم نوعاً من تمكين المستخدم فرض سيطرته على المعلومات بشكل كامل، ومنع الآخرين من الاطلاع عليها أو إجراء أي تغيير عليها دون إذن مسبق، فإذن أمن المعلومات هي عبارة عن حزمة من العمليات والطرق والإجراءات يتمّ انتهاجها من قبل بعض القطاعات ومنظّمات التأمين لبسط أقوى طرق الحماية على المعلومات الخاصة بها وعلى أنظمتها ووسائطها لمنع الوصول إليها لغير المصرّح لهم بذلك.

ظهر مصطلح أمن المعلومات منذ بدايات التواصل وتبادل الملفات والمعلومات أي منذ بداية البشرية، إذ تمثل ذلك تاريخيًا بحماية المعلومات السرية ولا سيما العسكرية منها من التعرض للاختراق أو السرقة من قبل جهات غير مصرح لها، وخصوصًا الأعداء .حيث كان أمن المعلومات في بادئ الأمر يتضمن حماية المعلومات المادية من التعرض للسرقة بعد ذلك تطور المفهوم ليشمل المعلومات السيبرانية والتقنيات الإلكترونية بشكل كامل.

عمِد المهتمين بحماية المعلومات إلى تشفيرها وابتكار شيفرات سرية تمكنهم من التواصل وتبادل الرسائل بشكل يضمن انعدام إمكانية سرقتها، بالإضافة إلى عدم قدرة السارق على فهمها وتسريبها، بالتالي الفشل في الاستفادة منها.أخذت طرق حماية المعلومات مع التقدم

التكنولوجي والأمني تصبح أكثر تعقيدًا عمّا سبق، عبر استخدام وسائل تشفير أكثر فعالية وبالتالي إمكانية استخدام وسائل التواصل العادية في نقلها دون الخوف من تعرضها للاختراق . حيث تعد المخابرات المركزية الأمريكية (CIA) من أولى الجهات التي تبنّت مبدأ حماية المعلومات وحمايتها لضمان حماية الأمن القومي ومنع الوصول إليها من قبل المخترقين سواءً من الأعداء أو من قبل المستخدمين أصحاب الخبرة والفضول.

تبلور مصطلح أمن المعلومات بشكله الحالي بعد اختراع الإنترنت والحواسيب التي تتضمن المعلومات السرية، والتي لا يرغب الأفراد والشركات والدول على حد سواء في تسريبها وتعرضها للسرقة والتخريب .لهذا أخذت الشركات تعمل على تطوير وسائل حماية المعلومات بشكل كبير، بسبب ازدياد التنافسية بينها بالإضافة إلى اتساع آفاق استخدام الشبكة العنكبوتية (الإنترنت) في تبادل وتخزين المعلومات (التخزين السحابي)

تمتاز حماية المعلومات بأنها مستمرة، أي إنها تحتاج بالضرورة إلى الاستمرارية في مواكبة كل ما هو مستحدث ومتطور من درجات الامان وأساليبها في حماية هذه المعلومات، كما تتطلّب الاستمرارية بفرض الرقابة على المخاطر وافتراضها، والسعي الدائم لإيجاد حلول وابتكارات دائمة، ولذا لا يطلق النظام المعلوماتي الأمني الحقيقي على نظام أيّ مُنظّمة إلا في حال كان فعّالاً ومحققاً للاستمرارية في مواكبة العمليات الأمنية والتقنية سعياً للوصول إلى أقل فرصةٍ من المخاطر التي من الممكن تواجه المعلومات الخاصة بها.

ما هو الفرق بين الأمن السيبراني وأمن المعلومات؟

قبل التعرف على الفروق التي تميز أمن المعلومات عن الأمن السيبراني علينا أن نتعرف على معنى مصطلح الأمن السيبراني أو Cyber Security.

ما هو الأمن السيبراني

هو مجموعة الإجراءات التي تهدف إلى حماية الأجهزة والشبكات ككل من الهجمات غير المتوقعة، بالإضافة إلى منع الوصول غير المصرح فيه إلى المعلومات التي تحتويها.

يشمل الأمن السيبراني حماية كلٌ من :

- الحواسيب.
- السيرفرات.
- التخزين السحابي.

حيث تسعى الشركات ولا سيما الكبيرة منها إلى توظيف فريق من المختصين ذوي الخبرة العالية في مجال الأمن السيبراني، حيث يعود الأمر إلى إمكانية تعرض الشركة أو أحد منتجاتها إلى هجمات ومحاولات اختراق إما بهدف السرقة أو التخريب من قبل الشركات المنافسة.

إذ تعد التنافسية العالية بين الشركات إحدى أكثر الأسباب التي تؤدي إلى حصول الهجمات الإلكترونية، علاوةً على ما سبق تسعى الدول والمنظمات لتأمين بياناتها ومعلوماتها عبر حماية الخوادم الحكومية وغيرها من الحواسيب التي تحمل معلومات خاصة.

ذلك بغرض تفادي جميع أنواع الهجمات الإلكترونية التي تكون لأغراض سياسية بالمرتبة الأولى، والتي بدورها قد تؤدي إلى مشاكل دبلوماسية وغيرها، حيث تتم الهجمات الإلكترونية بشكل رئيسي عبر الإنترنت.

يمكن اعتبار الفرق الرئيسي بين أمن المعلومات والأمن السيبراني هو في نوعية المواد المحمية، حيث يسعى أمن المعلومات بشكل رئيسي إلى المحافظة على بيانات الشركات أو المستخدمين على حد سواء من التعرض للسرقة أو الاختراق أينما وجدت بغض النظر عن الأجهزة التي تحويها.

بينما يعمل الأمن السيبراني على حماية الأجهزة المادية التي تتضمن المعلومات من التعرض للسرقة أو الاختراق لأغراض تخريبية أو لغيرها.

علاوةً على ما سبق يستطيع المستخدم أو الجهة المسؤولة تحديد تصريحات وإمكانيات بالإضافة إلى مدى تطبيق أمن المعلومات .

يظهر نظام حماية المعلومات للجهة المسؤولة أي محاولة للاختراق وسرقة البيانات بينما يتمثل الأمن السيبراني في عملية الكشف عن محاولات السرقة والاختراق بالإضافة إلى تتبع الجهة المُخترقة والوصول إليها.

يتطلب التمكن من الأمن السيبراني امتلاك خبرات عالية المستوى وذلك لحماية الحواسيب والخادمات التي تحوي المعلومات من التعرض للهجمات ومحاولات الوصول غير المصرح به، بالإضافة إلى ذلك يشمل الأمن السيبراني حماية النظم والحواسيب والشبكات ككُل من التعرض للاختراق بينما يستهدف أمن المعلومات حماية المعلومات بشكل خاص من أي عملية سرقة أو تخريب.

بلغة أخرى إذا أمكن التشبيه بالدماغ البشري، أمن المعلومات يحمي الأفكار من السرقة والاختراق بينما الأمن السيبراني يحمي الدماغ من التعرض للاختراق والتخريب المتعمد بشكل كامل.

ركائز أمن المعلومات

يرتكز أمن المعلومات عند حماية المعلومات على عدد من الأنظمة التي ظهرت بالتزامن مع التطور التكنولوجي:

- أنظمة حماية نظم التشغيل: ويشمل تحقيق الحماية للطبقة الأقرب لجهاز الحاسوب؛ إذ يتم بهذا النظام إخفاء كافة التفاصيل الخاصة بمنظمة ما، ويعتبر هذا النظام بمثابة موزّع عادل للمهام بين الأجهزة في المنظومة، وتفرض سيطرتها على جميع أنظمة الولوج إلى الذاكرة وجدولة المهام.

- أنظمة حماية البرامج والتطبيقات: وهي الأنظمة التي تفرض على ما تستخدمه مُنظّمة ما من برامج وتطبيقات، وتسّد الثغرات التي تكون بمثابة فرصة للوصول إليها وانتهاكها.

- أنظمة حماية قواعد البيانات: هي عبارة عن مجموعة من البرمجيّات التي تُعالج الأخطاء البرمجية وتسّد الثغرات التي قد يحتويها أي نظام في إدارة قواعد البيانات، فتؤدّي بالتالي إلى إلحاق الضرر والضعف بأمن نظام قواعد البيانات، لذلك لا بدّ من استخدام التحديثات المستحدثة أولاً بأول، ومن هذه السبل:

  - ✓ استخدام وسائل تحديد صلاحيات الاستخدام المناسبة.
  - ✓ ضبط الوصول الإلزامي.
  - ✓ ضبط الوصول المرتكز على الدور.
  - ✓ ضبط الوصول الاختياري.
  - ✓ أنظمة حماية الولوج للأنظمة.

المبادئ الأساسية

يعتمد أمن وحماية المعلومات على ثلاثة مبادئ أساسية مرتبطة به منذ عشرين عاماً، وتُشكّل بمجموعها الثالوث(CIA) ، وهي:

- السرية (Confidentiality): يشير هذا المصطلح إلى الحد من قدرة الأفراد غير المخولين بالوصول إلى المعلومات وكشفها والاطلاع عليها، وتعد بطاقة الائتمان من أكثر الأنظمة التي تخضع لسرية عالية إلا أنها بالرغم من ذلك تتعرض للانتهاك والسرقة، وتكمن السرية في بطاقات الائتمان بالتشفير لرقم البطاقة.
- التكاملية (Integrity): وهي سلامة المعلومات، وتشمل حماية البيانات من أي تغيير قد يطرأ عليها من جهة غير مخوّلة بذلك أو تعديلها، ويكون القصد من هذا التغيير التخريب أو الانتهاك للملفات الهامة وإلحاق الضرر بها.
- التوافر (Availability): يستلزم في أي منظومة تستخدم أنظمة معلومات خاصة بها توفّر البيانات فور طلبها والحاجة إليها، وحتى يتوفّر ذلك لا بد لعناصر النظام أن تعمل على أكمل وجه، ويشمل:

- ✓ ضمان عمل الأنظمة الحاسوبية بشكل صحيح وسليم وخاص تلك المستخدمة في تخزين المعلومات ومعالجتها.
- ✓ وفرة الضوابط الأمنية الخاصة بالنظام وحمايته. سلاسة انتقال المعلومات عبر قنوات الاتصال الواجب توفرها.
- ✓ ضمان استمرارية الحماية للأنظمة بكل الأوقات وذلك من خلال توفير أنظمة سرية عالية الجودة.
- ✓ توفير أنظمة للترقيات والتحديث باستمرار للحدّ من انقطاع الخدمة إثر حدوث فصل في الكهرباء أو عطل في الأجهزة.
- ✓ التأكّد من عدم وقوع هجمات الحرمان من الخدمة ومنعها.

ما هي سياسة أمن المعلومات؟

تركز سياسة حماية المعلومات على تطبيق المعايير الدولية في حماية المعلومات واتخاذ الإجراءات المناسبة في هذا الصدد، حيث تشتمل سياسة أمن المعلومات بشكل رئيسي على:

1. تحديد الغرض من حماية المعلومات

رغم أنه يعد من البديهي قليلًا تحديد الغرض من أمن المعلومات ألا وهو حمايتها من الوصول غير المصرح به، تسعى الشركات إلى تحديد الغرض بغية إيضاح ما تريد الوصول إليه في ضمان أمن المعلومات وسلامتها

2. نطاق تطبيق مفهوم حماية المعلومات

يشمل تحديد الجهات الخارجية والداخلية على حد سواء التي تخضع إلى سياسة حفظ المعلومات، أي بلغة أخرى تبيان المعلومات التي تهتم الشركات في المحافظة عليها بشكل رئيسي دون غيرها.

3. تحديد الجهات المسؤولة والراعية

يعني المصطلح السابق تحديد المسؤولين المخولين بإجراء التعديلات والتغييرات على سياسات أمن المعلومات دون غيرهم بالإضافة إلى تحديد الجهات المسؤولة عن ضمان تطبيق سياسة الأمن وسرية المعلومات. تتغير سياسات الشركات تبعًا لتغيرات أوساط وزمن وآليات تبادل المعلومات بشكل مستمر، وذلك لضمان حمايتها من الاختراق بشكل مطلق وصحيح.

4. تحديد قيود التنفيذ

حيث ترسم المؤسسات والشركات لتحديد قيود تفعيل سياسة حماية المعلومات والتبعات المترتبة على مخالفة قواعد أمن المعلومات، والتي قامت برسمها مسبقًا.

5. تاريخ تطبيق السياسة

أي تحديد المدة الزمنية التي ينبغي فيها تطبيق السياسة ومدة نفاذ القوانين التي تحددها الشركات في مجال أمن المعلومات.

ما هي أهمية أمن المعلومات؟

يعد أمن المعلومات من الأساسيات التي تسعى كل شركة أو فرد إلى تأمينها، وذلك بهدف الحفاظ على سرية المعلومات وتجنب تعرضها للسرقة والتخريب المتعمد.

بسبب التنافسية العالية بين الشركات، تسعى بعضها إلى النيل من منافسيها عبر القيام بهجمات ممنهجة بغية تعطيل وتخريب معلوماتها أو سرقتها من أجل تقليدها ومعرفة أسرارها.

تتجلى أهمية حماية المعلومات في عدد من النقاط أهمها:

- تحديد الجهات المخولة بالوصول إلى المعلومات.
- تجنب عمليات الاختراق العشوائية التي يقوم بها الهواة أو المحترفون.
- الحرص على استمرار عملية الإنتاج ومنع عرقلتها عبر تخريب المعلومات.
- ضمان تميز الشركات والمنشآت عبر حماية سرية المعلومات ومنع تسريبها.
- تقليل التكاليف وتفادي الخسائر، عبر حماية المعلومات تقل الحاجة إلى إعادة إنتاجها من الصفر.

أهداف أمن المعلومات

يهدف أمن المعلومات بشكل رئيسي إلى تقديم الحماية المُثلى للمعلومات من الاختراق والتعرض للتخريب المتعمد والممنهج، بالإضافة إلى تفادي تعرضها للسرقة .من أهم أهداف أمن المعلومات:

أولًا: تحديد الجهات المؤهلة بالوصول إلى المعلومات

يفيد تحديد الجهات المصرح لها بالولوج إلى المعلومات في ضمان عدم دخول أطراف أو أفراد غير مصرح بهم. الأمر الذي يضمن حماية المعلومات ويضيق نطاق البحث عن الجهة المسؤولة عن إحدى التعديلات عند عدم تعرض المعلومات لأي اختراق أو سرقة، بالإضافة إلى ما سبق يُعنى تحديد الجهات المخولة بالوصول إلى المعلومات بتخصيص صلاحيات محددة لكل منها، الأمر الذي ينظّم عمل أمن وحماية المعلومات.

ثانيًا: حماية المعلومات من السرقة والاختراق

يهدف أمن المعلومات إلى حماية ومنع اختراق البيانات من أطراف خارجية، حيث وبسبب التسارع التقني وازدياد حجم المنافسة بين الأفراد والشركات تقوم بعض الجهات بمحاولات تخريبية بغية إلحاق أكبر ضرر ممكن بالشركات المنافسة، وبالتالي فتح المجال لها للتقدم والسيطرة على حصص سوقية أكبر.

يمكن حماية المعلومات المخزنة على المواقع الإلكترونية عبر إضافات يتم تثبيتها لبرنامج إدارة المواقع ووردبريس WordPress، حيث تهدف إلى زيادة وضمان حماية وسرية المعلومات مثال على ذلك يمكنك الاطلاع على أفضل إضافات ووردبريس لحماية موقعك من الاختراق.

ثالثًا: تقليل الخسائر المحتملة من عمليات تخريب أو سرقة المعلومات

يفيد أمن المعلومات في حال تعرضت البيانات إلى هجوم أو سرقة أو تخريب سواء بسبب وجود ثغرات أمنية أو بسبب قوة الهجوم على المعلومات، في حماية أكبر قدر ممكن من المعلومات .أي بلغة أخرى، الحد من التسريب وحماية ما يمكن حمايته من المعلومات بأكبر قدر ممكن.

رابعًا: الحد من تعطل الخدمات والأعمال جراء العمليات التخريبية

يتم ذلك عبر إجراء نسخ احتياطية للبيانات بشكل دوري، وذلك لإتاحة المجال أمام استرجاعها بعد تعرضها للتخريب والسرقة، الأمر الذي يقلل من الخسائر المحتملة، بالإضافة إلى تقليل الوقت اللازم لإصلاح الأضرار. الأمر الذي يحد من مدة تعطل إنتاجية المؤسسات والشركات ويسمح لها بالتعافي بشكل أسرع.

خامسًا: ضمان تطبيق القوانين والضوابط التي تمنع التعديلات غير المصرح بها

عند تحديد الصلاحيات والجهات المخولة بالوصول إلى المعلومات، يؤمن بهذه الطريقة مبدأ أمن المعلومات حمايتها من أي تعديلات عشوائية، حيث تحتفظ أنظمة أمن المعلومات المتقدمة بسجلات تفيد في معرفة أي تعديل قامت به أي جهة من الجهات المصرح لها بالوصول إلى المعلومات.

عناصر أمن المعلومات

يقوم مفهوم أمن المعلومات على مبادئ أساسية لا يمكن لأي من التقنيات الحديثة ضمان نجاحها حيث تشمل عناصر أمن المعلومات كلًا من:

1. سرية المعلومات التامة

يؤمن أمن المعلومات الحماية للبيانات عبر تشفيرها، وذلك للحيلولة دون قدرة المخترقين في حال تمكنوا من الوصول إلى المعلومات .تتمثل عملية المحافظة على سرية المعلومات العديد من الأمثلة منها :

- كلمات المرور القوية التي تتضمن رموزًا يصعب على أي أحد تخمينها بسهولة.
- مستشعرات العلامات الحيوية مثل آليات مسح البصمات وقرنية العين بالإضافة إلى برامج التعرف على الوجوه، هذا الأمر الذي يحد من وصول الأشخاص غير المخول لهم إلى المعلومات وتعديلها.
- تشفير المعلومات وتفكيكها إلى رموز ومحارف عند تبادلها عبر الشبكات والإنترنت، مما يؤمن سلامة وصولها دون حدوث أي تسريب لها.

علاوةً على ما سبق، تعد السرية إحدى الأركان الأساسية التي تجعل من عملية الحفاظ على المعلومات وتأمينها الأولوية القصوى لجميع الأفراد والشركات.

2. تأمين توفر المعلومات وإمكانية الوصول إليها

عوضًا عن حفظ المعلومات وتخزينها لمنع تعرضها للسرقة مما يصعّب من إمكانية الوصول إليها عند الحاجة بشكل سلس، يؤمن أمن المعلومات إمكانية توافر المعلومات بشكل دائم للمستخدمين المخولين بالوصول إليها، دون مواجهة أي عوائق أو عقبات، الأمر الذي يضمن سلاسة واستمرارية الإنتاجية والاستفادة منها بشكل مستمر.

3. سلامة المعلومات من البرامج الضارة والضياع

يتجلى الأمر بشكل أوضح في حماية المعلومات من التعرض لأي حادث قد يؤدي لتخريبها أو ضياع أجزاء منها .إذ يؤمّن مفهوم سلامة المعلومات إمكانية نسخها احتياطيًا وحفظ النسخة بشكل آمن وبالتالي التأمين على المعلومات من الضياع بشكل دائم.

أنواع أمن المعلومات

بفضل التطور الكبير في عالمنا اليوم، تتنوع أنواع وأشكال أمن المعلومات والتي تعمل جميعها بشكل متكامل لتأمين الوصول إلى بيئة آمنة تحمي المعلومات من الاختراق والسرقة والتخريب.

1. أمن البرمجيات والتطبيقات

يعني ذلك تطوير برامج مكافحة الاختراق والجدران النارية بالإضافة إلى اكتشاف مَواطن الضعف والثغرات في التطبيقات المختلفة عبر جميع الأنظمة والمنصات.

2. أمن وسائل التخزين السحابي

التخزين السحابي هو إمكانية رفع المعلومات عبر شبكة الإنترنت لإتاحة الوصول إليها في أي زمان ومكان من قبل الأشخاص المخولين بذلك، ولكن يعد حفظ المعلومات عبر الإنترنت أمرًا خطيرًا فيما يتعلق بسلامتها من الهجمات الإلكترونية .بالتالي يُعنى الأمن السيبراني في تأمين بيئة تخزين سحابي آمنة للاحتفاظ بالمعلومات وتخزينها.

3. بناء بنية تحتية صلبة

لا ينحصر الأمن التقني على حماية المعلومات في بعض الأحيان بل يتجاوز مفهومه التقليدي ليشمل الأجهزة والأدوات التي تحفظ فيها المعلومات مثل الحواسيب والمخدمات .يؤمن ذلك تقليل احتمال وقوع عمليات السرقة والتجسس إلى حدودها الدنيا.

4. التشفير

تم اعتماد التشفير مثل وسيلة لحماية وتأمين المعلومات من السرقة منذ القدم، وتوسع المفهوم ليشمل تشفير مختلف أنواع المعلومات ولا سيما الإلكترونية منها، حيث يعني تشفير المعلومات تحويلها إلى محارف ورموز يستحيل على الجهات غير المخولة بالوصول إلى المعلومات فهمها واستخدامها.

5. مكافحة الثغرات الأمنية

يتم ذلك عبر محاكاة عمليات الاختراق المحتمل وقوعها، مما يساعد الخبراء على تفادي حصولها بالإضافة إلى تعزيز وسائل حماية سرية المعلومات.

تدابير أمن المعلومات

يتمثل المفهوم السابق باهتمام الشركات بتعزيز واتخاذ التدابير اللازمة من ناحيتين وهما:

1. الاهتمام بالكفاءات البشرية

- **اختيار مسؤولو الأمن السيبراني من ذوي الخبرة**

أي توظيف الشركة واختيار أفضل المرشحين من أجل ملئ مناصب خبراء أمن المعلومات، حيث يفيد الأمر في تعزيز الأمن السيبراني في حال تمتع المسؤولون عن تطبيق عن أمن البيانات بالخبرات الكافية التي تساعدهم على تفادي الهجمات السيبرانية.

يمكن العثور على أصحاب الخبرات الذين يستطيعون تلبية مهام إدارة أمن المعلومات إما عبر الإعلانات المباشرة، أو عبر منصات العمل الحر مثل موقع خمسات أكبر سوق عربي لبيع وشراء الخدمات المصغرة، والذي يقدم الكثير من خدمات الأمن والحماية.

- **توعية الموظفين بأهمية أمن المعلومات**

يتم ذلك عبر إقامة ندوات ودورات لجميع الموظفين مما يخلق بيئةً من الموظفين أصحاب الخبرة والمعرفة بالأساسيات التي تساهم بدورها في تقليل الأذى الناتج عن اختراق البيانات وسرقتها.

2. تعزيز الأمن الرقمي

يعني تعزيز الأمن الرقمي اعتماد الشركات والمؤسسات على تثبيت وتنصيب أحدث الإصدارات من برامج الحماية من الفيروسات بالإضافة إلى استخدام برمجيات الجدار الناري .الأمر الذي يساهم وبشدة في حماية ومساعدة خبراء أمن المعلومات في حماية سرية المعلومات وحذف البرامج الضارة فور تنزيلها.

3. رسم الخطط المادية

من أهم تدابير أمن المعلومات رسم الخطط المادية التي تنوي المؤسسات والشركات رصدها لحماية المعلومات، الأمر الذي يعني اختيار الخبراء والبرمجيات التي تتناسب مع إمكانيات الشركة المادية وتقديم دورات وندوات وبرامج تدريبية أفضل للموظفين.

إذ لا ينحصر ذلك على التدابير الرقمية بل تفيد رسم الخطط المادية في اختيار الشركات للأدوات التي سوف تستعملها لحماية معلومات ومقرات الشركة. على سبيل المثال الأبواب والأقفال وأنظمة التعرف على العلامات الحيوية.

4. تدابير التنظيم والتخطيط

تقدم تدابير التنظيم إمكانية رسم هيكلية شاملة لبرامج حماية المعلومات، حيث يعني ذلك تحديد صلاحيات كل من الأفراد المخول لهم بالوصول إلى المعلومات.

مجالات أمن المعلومات

سابقًا كان من الممكن لشخص واحد أن يكون ملمًا بكل ما يتعلق بأمن المعلومات وحمايتها، حيث كانت الحكومات والشركات تعمد إلى توظيف شخص أو فريق من الأشخاص من أصحاب المهارات المتماثلة لتقديم خدمات حماية المعلومات.

لكن مع التطور الكبير الذي طرأ على أنظمة العمل والعالم الرقمي والمادي أخذت مهام أمن المعلومات تتشعب بشكل كبير مما يجعل تقريبًا من المستحيل امتلاك شخص واحد لجميع الخبرات المطلوبة لتحقيق الحماية المُثلى للمعلومات.

حيث ظهرت عدة مجالات فيما يتعلق بأمن المعلومات منها:

1. مسؤول أمن المعلومات Security specialist

يعد مسؤول أمن المعلومات اللبنة الأولى في أي فريق مختص في حماية المعلومات، إذ يمتلك الخبرات الأساسية التي يجب أن يتمتع بها أي مختص في أمن المعلومات .يقدم مسؤول أمن المعلومات الخدمات الضرورية واللازمة للحفاظ على سلامة المعلومات من مختلف المخاطر المحدقة بها مثل السرقة أو التخريب.

تعتمد المنشآت ذات مخاطر الاختراق القليلة نسبيًا على موظفي أمن البيانات من هذا الاختصاص بشكل رئيسي حيث يستطيعون تأمين الحماية اللازمة من المخاطر وضمان أمن وسرية المعلومات.

2. مسؤول أمن الشبكات Web security manager

يُعنى مسؤول أمن الشبكات بحماية المعلومات عند تبادلها أو تخزينها على منصات التخزين السحابي، وذلك عبر تهيئة البيئة الآمنة والخالية من المخاطر التي قد تؤدي إلى تلف المعلومات أو ضياعها أو حتى سرقتها.

3. مختص إدارة المخاطر Chief risk officer

ينطوي العمل الرئيسي لمسؤولي إدارة المخاطر على تقييم حالة أنظمة الشركات وتحديد مواطن الضعف فيها، مما يساعد باقي فريق أمن المعلومات على تلافيها بأسرع شكل ممكن دون الحاجة إلى فحص جميع أجزاء الأنظمة والتي قد تستغرق وقتًا أطول من المعتاد.

4. مهندس أو مسؤول تحليل البيانات الأمنية Security analyst/engineer

يعمل مسؤولو تحليل البيانات الأمنية على تتبع محاولات الاختراق وذلك من أجل معرفة مصدر الهجمات الإلكترونية أو معرفة حجم الضرر الذي تسببت به .حيث تجرم الكثير من الدول محاولات تهديد الأمن الإلكتروني وبالتالي يعد الوصول إلى المخترق أمرًا مفيدًا لملاحقته قانونيًا وتسليمه للقضاء المختص.

يشتمل عملهم أيضًا على تحليل عمليات الوصول إلى التطبيقات من قبل الأفراد المخول لهم بذلك بشكل دقيق لكشف أي محاولة انتحال شخصية أو تزوير أو وصول غير مصرح به إلى المعلومات.

5. مسؤول البرمجيات والتطبيقات Apps Specialist

تعد المهمة الرئيسية أمام مهندس التطبيقات والبرمجيات تأمين حفظ المعلومات عبر مختلف المنصات والعمل على تصحيح أي من الأخطاء التي قد تهدد أمنها .بالإضافة إلى دراسة الأكواد البرمجية للتطبيقات للتأكد من سلامتها من البرامج الضارة والأخطاء التي تجعلها أكثر عرضةً للسرقة والاختراق.

يعد مسؤولي البرمجيات من المختصين في كل من أمن المعلومات والهندسة التقنية والمعلوماتية، أي يمتلكون خبرة كبيرة فيما يتعلق بمجالات البرمجة الرقمية.

6. المخترقون الأخلاقيون Ethical hackers

كي تعلم كيف تتفادى محاولات الاختراق عليك أن تفكر كالمخترق تمامًا، هذا الأمر دفع الكثير من الشركات لتوظيف عدد من الخبراء في مجال الاختراق الأخلاقي، أي أنهم لا يقومون بعمليات الاختراق لأغراض تخريبية أو بداعي السرقة.
حيث ينطوي مجال عملهم الرئيسي على كسف أي ثغرات أمنية قد تجعل المعلومات عرضة للهجمات السيبرانية، وجعل مختصي أمن المعلومات على دراية بها مما يساعدهم على تلافيها وإصلاحها.

شهادات أمن المعلومات

يعني مصطلح شهادات حماية المعلومات الحصول على ما يثبت إمكانية الفرد أو المؤسسة على تقديم الحماية الأمثل للبيانات في المجال الذي تتعلق به الشهادة.

حيث يوجد عدد من الشهادات التي يمكن للمرء الحصول عليها وبالتالي اثبات إمكانيته في تقديم خدمات ضرورية وأساسية للعديد من المؤسسات. التي تبحث عن توظيف الخبراء لضمان حماية المعلومات الهامة وتفادي تعرضها لأي من البرامج الضارة أو محاولات الدخول غير المصرح به .من أهم الشهادات التي تتعلق بأمن المعلومات هي:

1. شهادة المبادئ الأساسية في أساسيات الأمن السيبراني GSEC GIAC

تعد شهادة GSEC من الشهادات الأولى التي يسعى الراغبون في التمكن من مكافحة اختراق البيانات للحصول عليها، حيث تعد الشهادة إثباتًا أن صاحبها يتمتع بالمهارات الكافية والمرغوبة بشدة من قبل مختلف الشركات والمؤسسات التي تسعى إلى حماية المعلومات والحفاظ عليها من الهجمات السيبرانية.

تتميز شهادة GSEC بأنها من أسهل الوسائل التي تساعد المبتدئين في مجالات أمن المعلومات في التميز والبروز من بين أقرانهم من المختصين في حماية المعلومات، إذ تقدم لهم إمكانية اكتساب الفرص مما يساعد في تطوير مسيرتهم العملية.

2. شهادة المخترق الأخلاقي Certified Ethical Hacker (CEH)

تمكّن شهادة المخترق الأخلاقي الفرد من مهارات الاختراق التي يمتلكها المخترقون وبالتالي معرفة الثغرات التي تتواجد في الطرق التي يتبعها المخترقون، حيث يُمكن امتلاك الخبرة الكافية لاكتشاف أي ثغرات أمنية وسيلة مميزة تمنح المؤسسات الأفضلية في تفادي الهجمات قبل حدوثها بالإضافة إلى قطع الطريق على المخترقين قبل محاولاتهم حتى في اختراق وسرقة وتخريب البيانات.

إذ تعد أفضل وسيلة لأي شركة لحماية نفسها من القراصة اعتماد قراصنة مثلهم لحماية سرية المعلومات وسلامتها، تعد شهادة المخترق الأخلاقي إضافةً قويةً تمكن الخبراء من تقديم الخدمات الأمثل فيما يتعلق بمجال أمن المعلومات.

تتطلب الشهادة امتلاك خبرة سنتين على الأقل للتقدم لامتحان الحصول على شهادة المخترق الأخلاقي، حيث يشمل الامتحان الإجابة على ما يقارب الـ 125 سؤال بعد دفع الرسوم التي تؤهل المتقدمين للتقدم للاختبار.

3. شهادة الأمن السيبراني Security+

تعد شهادة Security+الخيار الأمثل للمبتدئين الذين يرغبون في امتلاك المهارات الكافية التي تخولهم احتراف آليات ووسائل حماية المعلومات.

يؤمن الحصول على شهادة الأمن السيبراني ضمان امتلاك الفرد للإمكانيات الكافية في اجتياز الأساسيات اللازمة لاحتراف أمن المعلومات، تعد شهادة الأمن السيبراني شهادةً دوليةً ذات

اعتراف من مختلف منظمات العالم، الأمن الذي يضمن للأفراد الحاصلين عليها سهولة ملاقاة فرص العمل في مختلف المؤسسات والشركات.

تشمل الدراسة والتدريبات التي يخضع لها المتقدمون للحصول على هذه الشهادة تعلم عدد معين من المواد بغية الوصول إلى الاحترافية المناسبة والمطلوبة للحصول على الشهادة.

1. مادة إدارة المخاطر الإلكترونية.
2. آلية التعامل مع أي ثغرات أمنية.
3. تعلم أساسيات التشفير الإلكتروني أو ما يدعى بـ PKI.
4. معرفة الأدوات والوسائل المُثلى للنجاح في التصدي ومكافحة الهجمات السيبرانية.

علاوةً على ما سبق يتطلب الحصول على شهادة الأمن السيبراني اجتياز عدد من النقاط الأساسية أثناء تعلم قواعد أمن المعلومات، ألا وهي:

- الالتزام بالقواعد والقوانين المتبعة في برنامج الحصول على الشهادة.
- التمكن من تنصيب وتثبيت برامج حماية الأنظمة المختلفة.
- التمتع بإمكانية تحليل التهديدات ووضع خطط حل المشاكل وتفادي المخاطر بشكل سليم.

بالتالي يمكننا القول، إن الشهادة تعد اليوم من أفضل الشهادات التي ينبغي على الراغبين في احتراف أمن المعلومات السعي للحصول عليها.

4. شهادة A+

تضمن شهادة A+ للحاصلين عليها ضمان امتلاكهم للخبرات الكافية التي تؤهلهم لحل المشاكل وتفادي العقبات التي قد يصادفها المستخدمون المبتدئون لأنظمة أمن المعلومات.

تعد شهادة A+ معترف بها عبر مختلف المنظمات والشركات حول العالم، الأمر الذي يجعل تلبية متطلبات الشركات أمرًا سهلًا وبالتالي الحصول على فرص عمل أكثر.

تتميز شهادة A+ بكل من:

- **التحديث المستمر والتطوير**

الأمر الذي يعني مواكبة التغيرات التكنولوجية بشكل مستمر وبالتالي ضمان امتلاك المتقدمين للحصول على الشهادة لخبرات متجددة وعالية المستوى

- **تقديم خبرات عبر مختلف المنصات**

لا تنحصر الخبرات التي يكتسبها المستخدمين من حصولهم على شهادة A+ على أحد أنظمة التشغيل دون غيرها .حيث تشمل خبرات أمن المعلومات التي يكتسبها المتقدمون كلًا من نظام ويندوز windows و mac OSبالإضافة إلى أنظمة تشغيل الهواتف المحمولة أي أندرويد android و.iOS

- **اكتساب مهارات حل المشاكل ورسم خطط العمل الصحيحة**

إذ تتميز شهادة A+ دونًا عن غيرها من الشهادات في منح المستخدمين القدرة على اكتساب مهارات التفكير النقدي والقدرة على حل المشاكل، الأمر الذي يساعد في اتباع أكثر الطرق نجاحًا وسهولةً في مكافحة اختراق البيانات .يتطلب حيازة شهادة A+ اجتياز اختبارين رئيسيين هما:

- CORE 1.
- CORE 2.

يعد هذان الاختباران شاملان لكل المتطلبات الأساسية التي ينبغي على الراغبين في احتراف مجال حماية المعلومات واكتشاف أي ثغرات أمنية في الأنظمة التي يعملون عليها اجتيازهما. تتوافر عدد من الشهادات التي تقدم أنماطًا مشابهةً لشهادة A+ والتي تقدم إمكانية اختيار المستخدمين للبرنامج الأفضل والأنسب لهم دون التقيد بإحدى الشهادات دونًا عن غيرها .من هذه الشهادات شهادة.Network+

5. شهادة محرر البيانات المعتمد CISA Certification

تجعل هذه الشهادة الحاصلين عليها مؤهلين للحصول على أفضل فرص للعمل، وذلك لما يمتلكونه من خبرات تقنية عالية المستوى. وهو ما جعل تكاليف التقدّم لها باهظة بعض الشيء، إذ تكلّف قرابة 800$، لكنها تعد معيارًا عالميًا في مجال أمن وحماية المعلومات ضد الهجمات السيبرانية. ويمتلك الحاصل على تلك الشهادة العديد من المهارات منها:

- خبرة في إدارة أنظمة المعلومات والتحكم الكامل فيها.
- معرفة كيفية تطوير أنظمة تكنولوجيا المعلومات وبنائها بشكلٍ صحيح.
- اكتساب خبرة تتجاوز الأساسيات في مجالات حماية المعلومات وتفادي الهجمات الإلكترونية.
- توفير الدعم والحماية للأنظمة المختلفة، وتأمينها ضد محاولات الاختراق.

6. شهادة CCNA

تعني اختصارًا CCNA (Cisco Certified Network Associate Security) وهي واحدة من أهم الشهادات الدولية التي ينبغي على أي مختص أمن معلومات الحصول عليها .حيث تقدم لخبير حماية المعلومات الأساسيات الرئيسية التي تمكنه من حل المشاكل والأخطاء عند وقوعها، بالإضافة إلى امتلاكه للخبرة الكافية التي تؤمن سرية المعلومات وحمايتها من الهجمات السيبرانية المختلفة.

علاوةً على ما سبق تتميز شهادة CCNA بالكثير من النقاط أهمها:

- التكلفة المنخفضة نسبيًا.

تعد شهادة CCNA من الشهادات المقبولة والرخيصة نسبيًا، إذ تكلف المستخدم الذي يود الحصول عليها حوالي الـ 200$، الأمر الذي يجعلها اختيار الكثير من الراغبين في احتراف مجال أمن المعلومات دون تكبد عناء التكاليف الباهظة للشهادات الأخرى.

- إمكانية إجراء الامتحانات عن بعد أي عبر الإنترنت.
- إمكانية الحصول على الدورات التدريبية عبر مدرس أو عبر تعليم افتراضي.

هذا الأمر يجعل شهادة CCNA جذابةً للكثير من المستخدمين من جميع أنحاء العالم على حد سواء.

- امتلاكها لأكثر من 160 برنامج تدريبي مختلف.

مما يعني احتواء موقع شهادة CCNA على كافة المعلومات والمفاهيم التي ينبغي على الراغبين في احتراف مجال أمن المعلومات تعلمها، ولكن دون الحاجة للبحث عن مصادر للتعلم .إذ يقدم الموقع الكثير من الدورات المختلفة والتي تخول المستخدمين في نهاية المطاف للتقدم للامتحان والحصول على الشهادة ذات الاعتراف الدولي.

تحديات أمن المعلومات

يواجه أمن المعلومات في يومنا هذا الكثير من التحديات التي تهدد إمكانية حماية البيانات والحفاظ عليها من الهجمات السيبرانية المختلفة .إذ تتمثل تحديات أمن المعلومات بعدد من النقاط منها:

1. التطور التكنولوجي

يعد التطور التكنولوجي سيف ذو حدين، فعلى الرغم من أهميته في ابتكار وسائل جديدة في حماية المعلومات وتفادي الهجمات السيبرانية. إلا أنه يقد وسائل جديدةً للمخترقين تساعدهم في اكتشاف ثغرات أمنية قد تؤدي إلى وصولهم إلى المعلومات وتخريبها وسرقتها.

2. اختراق الرسائل والمعلومات المرسلة

حيث يكون ذلك عبر اعتراض البيانات سواءً المادية أو الرقمية أثناء إرسالها إلى الجهات المعنية بها، إذ تعد البيانات في مرحلة الإرسال في أضعف حالاتها نظرًا لانتقالها من مكان إلى آخر. حيث تقدم معظم خدمات الأمن الإلكتروني الحماية للمعلومات في أماكن تخزينها.

3. الفيروسات

الفيروسات عبارة عن برمجيات خبيثة تهدف إلى إلحاق الضرر وإتلاف المعلومات، وفي بعض الحالات السيطرة عليها وقفلها مقابل مطالب ماليةً معينةً .ترتبط الفيروسات عادةً بالبيانات المرسلة من جهة إلى أخرى وتتفعل عند وصولها إلى الهدف، الأمر الذي يستدعي التطوير والتحديث المستمر لبرامج مكافحة الفيروسات.

4. انتحال الشخصيات

عوضًا عن القيام بهجمات ومحاولات اختراق قد تؤدي لتفعيل أنظمة أمن المعلومات، يعمد بعض المخترقين إلى انتحال شخصيات الأفراد المخول لهم بالوصول إلى المعلوماتـ، الأمر الذي يجعل من الصعب كشفهم ومنعهم من سرقة أو تخريب البيانات.

5. التجسس على الوسائل المادية لحفظ المعلومات

يعني المفهوم السابق القيام بالتجسس على أجهزة تخزين المعلومات دون اختراق أنظمتها بشكل مباشر. أي مثل محاولة سرقة المعلومات عبر اختراق كابلات نقل البيانات وغيرها من الوسائل المادية لحفظ المعلومات.

كيف تحمي بياناتك من الاختراق؟

تتوفر عدد من الآليات التي تضمن تطبيق مفهوم حماية المعلومات بالشكل الأمثل ومنها:

1. تثبيت برامج مضادات الفيروسات

حيث تعمل هذه البرامج على فحص المعلومات بشكل دوري وحمايتها من التعرض للفيروسات التي تحتوي على برمجيات تخريبية أو تجسسية.

2. كشف نقاط الضعف

من أهم عناصر أمن المعلومات هي كشف نقاط الضعف في الأنظمة والتي تجعلها عرضةً للهجمات ومحاولات الاختراق، يتم ذلك عبر الاستعانة بالخبراء والمختصين الذين تتمثل مهمتهم في محاكاة عمليات الاختراق للكشف عن نقاط الضعف والتي قد تمثل خطرًا على سلامة المعلومات وسريتها.

3. اعتماد سياسة النسخ الاحتياطي

يتيح النسخ الاحتياطي للمعلومات تأمينها من عمليات التخريب والتلف المحتملة جراء التعرض للهجمات ومحاولات الاختراق، حيث تسعى بعض أنظمة الحماية إلى إتلاف المعلومات وحذفها بشكل كامل عند تعرضها لمحاولات الاختراق، تعد هذه الوسيلة الملاذ

الأخير الذي يهدف إلى منع تسريب المعلومات والوصول إليها من قبل جهات غير مصرح لها.

4. تشفير المعلومات

يفيد تشفير المعلومات في إضافة قيم إضافية إلى عملية حماية المعلومات، بالإضافة إلى إتاحة المجال لتبادل المعلومات وإرسالها دون الخوف من تسريبها أو تعرضها للاختراق .إذ تضمن عملية التشفير عدم استفادة الجهة المخترِقة للمعلومات منها في حال استطاعت الوصول إليها.

5. تحديد الجهات المخولة بالوصول للمعلومات

يؤمن تحديد الجهات المخولة في استخدام وتعديل المعلومات في الكشف عن محاولات الوصول بشكل غير قانوني إليها .

طرق حماية المعلومات:

- إمداد الأجهزة والمعدات بالتأمين المادي.
- استخدام مضاد للفيروسات يمتاز بالقوة والحداثة، ويجب استمرارية تحديثه.
- استحداث أنظمة للكشف عن الاختراقات.
- الكشف عن نقاط الضعف التأمينية والتنبيه بها من خلال استخدام أنظمة مراقبة الشبكة.
- اتباع سياسة النسخ الاحتياطية.
- تشفير المعلومات المرسلة بالاعتماد على الأنظمة القوية.
- تقديم الدعم والإمداد الكهربائي اللازم للأجهزة لضمان عدم انقطاعها.
- توسيع نطاق الوعي الأمني وتوعية المستخدمين.

والآن مع تطوّر التكنولوجيا استطاع الإنسان التوصّل إلى كثيرٍ من الطرق لتدوين ما يحتاج إليه، ولكن أيضاً انعكس هذا التطوّر بشكلٍ آخر على هذه المعلومات فأصبح اختراقها سهل نتيجة ارتباط الأجهزة والسيرفرات معاً على شبكة الانترنت. قد يستهتر البعض بأهمية المعلومات التي يمتلكها ولا يعلم أنّها قد تساوي الكنوز عند بعض الأشخاص أو الجهات، لذلك لا بدّ لكلّ مؤسسةٍ أن توعّي موظفيها بأهمّية أمن المعلومات لتحقيق السلامة العامّة.

الفصل الرابع

الجرائم الإلكترونية

CYBERCRIME

ظهور الجرائم الإلكترونية احتلّ التقدّم في مجال المعلومات والاتّصالات جانباً كبيراً ومُهمّاً في حياة النّاس وتعاملاتهم؛ فصار الحاسوب أساس التّعامل بين الأشخاص والشّركات والمؤسسات، وقد ازداد التوجّه لاستخدام شبكات المعلومات الإلكترونيّة في الفترة الأخيرة بصِفَتها أداة اتّصال دولية في مُختلف مناحي الحياة، مُوفِّرةً بذلك الكثير من السّرعة والمسافات والجهد على الإنسان. إنّ الاستخدام الكبير لِلأنظمة التكنولوجية قاد إلى الكثير من المنافع والفوائد بجانب المشاكل والمَخاطر، وقدّم أصنافاً من الجرائم لم تكن مُتداولةً سابقاً، سُميّت بالجرائم الإلكترونية.

فما هي الجرائم الإلكترونية؟ وما هي أنواعها؟

الجريمة الإلكترونية هي جريمة استهداف ومحاولة استخدام جهاز كمبيوتر أو شبكة كمبيوتر أو جهاز متصل بالشبكة. يرتكب معظم جرائم الإنترنت من قبل اللصوص أو المتسللين الذين يتطلعون إلى كسب المال، وفي بعض الأحيان يكون الهدف من الجرائم الإلكترونية هو تدمير أجهزة الكمبيوتر لأسباب غير ربحية. قد تكون هذه الأسباب سياسية أو شخصية.

الجرائم الإلكترونية تُعرّف بانه الجرائم الإلكترونية بالإنجليزية (Electronic crime or e-crime) بأنّها المُمارسات التي تُوقَع ضدّ فرد أو مجموعةٍ مع توفّر باعثٍ إجراميّ بهدفِ التَّسبُّبِ بالأذى لسمعة الضحيّة عمداً، أو إلحاق الضَّرر النفسيّ والبدنيّ به سواءً أكان ذلك بأسلوبٍ مباشر أو غير مباشر بالاستعانة بشبكات الاتّصال الحديثة كالإنترنت وما تتبعها من أدوات كالبريد الإلكتروني وغرف المُحادثة، والهواتف المحمولة وما تتبعها من أدوات كرسائل الوسائط المُتعدّدة. تحملُ الجرائم الإلكترونيّة مُسمّياتٍ عدّة، منها:

- جرائم الكمبيوتر والإنترنت.
- جرائم أصحاب الياقات البيضاء بالإنجليزية (white collar crime).
- الجرائم السايبيرية بالإنجليزية (Cyper crime).
- جرائم التقنية العالية بالإنجليزية (High Tech Crime).

ما هي خصائص الجرائم الالكترونية؟

تتسم الجرائم الإلكترونية بعدة سمات أهمها ما يلي:

- يتميز بسهولة الوقوع في المصيدة، حيث أن عدم وجود ضوابط أمنية يساعد على انتشاره ويسهل ذلك.
- لا يمكن قياس الضرر الناجم عن الجرائم الإلكترونية لأنه يمكن أن يتسبب في أضرار جسيمة.
- بصرف النظر عن الأساليب الأمنية والتقنية المشددة، من الصعب تحديد الجاني.
- سلوك غير عادي وغير أخلاقي اجتماعيًا.
- أقل عنف وجهد من الجريمة التقليدية.
- جريمة لا ينحصر فيها الزمان والمكان بخصائص المسافة الجغرافية وليس لها حد زمني.
- نظرًا لأن الرموز المخزنة على وسيط التخزين المغناطيسي مشفرة، فمن السهل إخفاء آثار الجريمة وأدلة الجاني.

أنواع الجرائم الإلكترونية

للجرائم الإلكترونية أنواعٌ كثيرةٌ، منها:

1. **جرائمٌ إلكترونية ضدّ الأفراد:** هي الجَرائم التي يتمّ الوصول فيها إلى الهويّة الإلكترونية للأفراد بطرقٍ غير مشروعة؛ كحسابات البريد الإلكتروني وكلمات السِّر التي تخصُّهم، وقد تصل إلى انتحالِ شخصيّاتهم وأخذ الملفّات والصّور المُهمّة من أجهزتهم، بهدفِ تهديدهم بها ليمتَثلوا لأوامرهم، وتُسمّى أيضاً بجرائم الإنترنت الشّخصية.
2. **جرائم إلكترونية ضدّ الحكومات**: هي جرائمٌ تُهاجم المواقع الرّسمية للحكومات وأنظمة شبكاتها وتُركّز على تدمير البنى التحتيّة لهذه المواقع أو الأنظمة الشّبكية بشكلٍ كاملٍ، ويُسمّى الأشخاص المرتكبون لهذه الجريمة بالقراصنة، وغالباً ما تكون أهدافُهم سياسيّة.

3. **جرائم إلكترونية ضدّ الملكية:** هي جرائمٌ تستهدف المؤسسات الشخصيّة والحكومية والخاصّة، وتهدف لإتلاف الوثائق المُهمّة أو البرامج الخاصة، وتتمُّ هذه الجرائم عن طريق نقل برامج ضارّة لأجهزة هذه المؤسسات باستخدام الكثير من الطُّرق كالرسائل الإلكترونية (بالإنجليزية E-mail).

4. **الجرائم السّياسية الإلكترونية:** هي جرائم تستهدفُ المواقع العسكرية للدول بهدف سرقة معلومات تتعلّق بالدّولة وأمنها.

5. **هجمات الحرمان من الخدمات:** يتم تنفيذ هذه الهجمات باستخدام مجموعات من أجهزة الكمبيوتر الكبيرة التي يتم التحكم فيها عن بعد من قبل شخص ما يقالسيوم باستخدام النطاق الترددي المشترك. تم تصميم هذه الهجمات لإغراق الموقع المستهدف بكميات كبيرة من البيانات في وقت واحد، مما يتسبب في إبطاء المستخدمين ومنع الوصول إلى الموقع.

6. **برامج الفدية الضارة:** تمنع هذه البرامج صاحب الجهاز من الوصول إلى ملفاته المخزنة على القرص الصلب، ويطلب المجرم مبلغًا من المال من الضحية كفدية لاستعادة الملفات التي يحتاجها.

7. **التصيد الاحتيالي:** هذا النوع من الجرائم الإلكترونية هو الأكثر انتشارًا وهو إرسال جماعي لرسائل البريد الإلكتروني التي تحتوي على روابط لمواقع أو مرفقات ضارة وبمجرد أن ينقر المستخدم عليها، قد يبدأ في تنزيل برامج ضارة على جهاز الكمبيوتر الخاص به.

8. **القرصنة :**تُعرَّف القرصنة بأنها الوصول غير القانوني إلى البيانات والمعلومات الموجودة على جهاز كمبيوتر أو شبكة الإنترنت من خلال استغلال نقاط الضعف في هذه الأنظمة.

9. **مجموعة الاستغلال:** يُعرَّف هذا النوع على أنه استخدام البرامج المصممة لاستغلال أي خلل أو ثغرة أمنية في الكمبيوتر، وهذه البرامج متوفرة على شبكة الويب المظلمة، ويمكن للمتسللين التسلل إلى مواقع الويب الشرعية واستخدامها لإيقاع الضحايا.

10. **سرقة الهوية:** يحدث هذا النوع من الجرائم عندما يحصل شخص بشكل غير قانوني على المعلومات الشخصية لشخص آخر ويستخدمها لأغراض غير لائقة مثل الاحتيال والسرقة.

11. **الهندسة الاجتماعية:** يعتمد هذا النوع من الجرائم على العوامل البشرية للتلاعب بعقل الضحية وإجبارها على ارتكاب أعمال غير قانونية أو تسريب معلومات سرية.

12. **البرمجيات الضارة:** يتم تعريف البرامج الضارة على أنها برامج تؤثر على الأداء العادي لجهاز الكمبيوتر، ومن الأمثلة على البرامج الضارة حصان طروادة، و الفايروس.

13. **قرصنة البرامج:** يتم تعريف قرصنة البرامج على أنها إعادة توزيع البرامج واستخدامها دون إذن من الشركة التي تمتلكها، وتتم القرصنة من خلال إنتاج برامج تجارية مزيفة واستخدام العلامة التجارية للبرنامج الأصلي، و تنزيل نسخ غير قانونية من البرنامج، و انتهاك اتفاقيات استخدام البرامج التي تحد من عدد مستخدمي نسخة واحدة من البرنامج.

14. **جرائم التّشهير**، بهدف تشويه سُمعة الأفراد. جرائم السبّ والشتم والقدح.
15. **المطاردة الإلكترونية:** هي الجرائم المُتعلّقة بتعقّب أو مطاردة الأفراد عن طريق الوسائل الإلكترونيّة لغاية تعريضهم للمضايقات الشّخصية أو الإحراج العام أو السّرقة المالية، وتهديدهم بذلك؛ حيث يجمع مرتكبو هذه الجرائم معلوماتِ الضّحية الشخصية عبر مواقع الشّبكات الاجتماعي وغرف المحادثة وغيرها.

مخاطر الجرائم الإلكترونية

مخاطر الجرائم الالكترونية يُؤدّي انتشار الجرائم الإلكترونية في المُجتمعات إلى الكثير من المخاطر والتهديدات، ومنها:

- المساس بالاقتصاد والأمن الوطني وتهديده.
- المساس بالعلاقات الأسرية وتشكيل الخلافات بين أفراد الأسرة ممّا يؤدّي إلى التفكك الأسري، وذلك بسبب الكثير من النتائج التي تُسبّبها بعض أنواع الجرائم الإلكترونية كالتّشهير ببعض الأفراد ونشر الأخبار الكاذبة والإشاعات.

الفرق بين الجريمة الإلكترونية والجريمة المعلوماتية؟

الجريمة الإلكترونية والجريمة المعلوماتية هما مصطلحان يستخدمان لوصف أنواع مختلفة من الأنشطة الإجرامية المتعلقة بالتكنولوجيا والمعلومات، ولكن بينهما اختلافات واضحة في نطاقهما وتعريفاتهما. إليك الفرق بين الجريمة الإلكترونية والجريمة المعلوماتية:

1. الجريمة الإلكترونية

التعريف:

- **الجريمة الإلكترونية تشير إلى الأنشطة الإجرامية التي تتم باستخدام الحواسيب أو الشبكات الإلكترونية كوسيلة لتنفيذ الجريمة أو كهدف لها.**

الأمثلة:

- **القرصنة الإلكترونية :(Hacking) الدخول غير المصرح به إلى الأنظمة أو الشبكات الإلكترونية.**
- **الفيروسات والبرمجيات الخبيثة :إنشاء أو نشر برامج ضارة تهدف إلى تدمير البيانات أو سرقتها.**
- **الاحتيال عبر الإنترنت :استخدام طرق احتيالية عبر الإنترنت لسرقة الأموال، مثل رسائل البريد الإلكتروني الاحتيالية أو مواقع الويب المزيفة.**
- **التسلط الإلكتروني :(Cyberbullying) استخدام الإنترنت للتنمر أو الإساءة إلى الأفراد.**

النقاط الرئيسية:

- **الوسيلة :الجريمة الإلكترونية تعتمد على استخدام التكنولوجيا والأنظمة الرقمية كوسيلة لتنفيذ الجريمة.**
- **الهدف :يمكن أن تشمل الأهداف الأفراد، الشركات، أو الأنظمة الحكومية.**
- **التكنولوجيا :تشكل التكنولوجيا جزءًا أساسيًا من الجريمة، سواء كأداة أو كهدف.**

2. الجريمة المعلوماتية

التعريف:

- **الجريمة المعلوماتية تشير إلى الأنشطة الإجرامية التي تتعلق بالبيانات والمعلومات بشكل رئيسي، وتشمل استخدام التكنولوجيا للحصول على أو تعديل أو تدمير البيانات والمعلومات بشكل غير قانوني.**

الأمثلة:

- **سرقة البيانات :الحصول على بيانات حساسة أو سرية بطرق غير قانونية، مثل البيانات المالية أو المعلومات الشخصية.**
- **تعديل البيانات :تغيير أو تزوير البيانات بطرق غير قانونية لأغراض الاحتيال أو التلاعب.**
- **التجسس الإلكتروني :استخدام التكنولوجيا للحصول على معلومات سرية من كيانات أخرى بدون إذن.**
- **التحليل غير المصرح به :استخدام أدوات تحليل البيانات للحصول على معلومات محمية أو حساسة دون إذن.**

النقاط الرئيسية:

- **الوسيلة :الجريمة المعلوماتية قد تستخدم التكنولوجيا كوسيلة، لكن التركيز الأساسي هو على المعلومات والبيانات.**
- **الهدف :الأهداف تشمل بيانات شخصية، معلومات تجارية، أو معلومات حكومية.**

- **البيانات :التلاعب أو السرقة أو الوصول غير المصرح به إلى المعلومات هي الجوانب الأساسية.**

التشابه والاختلاف:

- **التشابه:**
  - **كلا النوعين من الجرائم يشملان استخدام التكنولوجيا.**
  - **يمكن أن تؤدي كلا الجريمتين إلى أضرار مالية أو شخصية كبيرة.**
- **الاختلاف:**
  - **الجريمة الإلكترونية تركز على استخدام التكنولوجيا كوسيلة لتنفيذ الجريمة أو كهدف لها، بينما الجريمة المعلوماتية تركز على البيانات والمعلومات كموضوع رئيسي للجريمة.**
  - **الجريمة الإلكترونية تشمل مجموعة واسعة من الأنشطة التي قد تتضمن الاعتداء على الأنظمة والشبكات، بينما الجريمة المعلوماتية تركز على التلاعب أو الوصول غير المصرح به إلى المعلومات والبيانات.**

بالتالي، بينما قد تتداخل الجريمة الإلكترونية والجريمة المعلوماتية في بعض النواحي، فإن كل نوع له نطاقه الخاص وموضوعاته التي تميّزه.

أسباب انتشار الجرائم الإلكترونية

تتنوع أسباب الجرائم الإلكترونية ويمكن تصنيفها على النحو التالي:

أولاً: أسباب فردية و تتمثل بـ :

- احترام الذات، اعتقاد الفرد بأنه محل تقدير وله كيانه الخاص والمنفصل من خلال المظهر الذي يجده في القيام بهذه الأعمال.
- إعطاء المجرمين الفرصة لارتكاب الجرائم بطريقة تجعل حياتهم أسهل، دون أي أثر، وخطر ضئيل، وصعوبة الوصول إلى مواقع الجريمة.
- تراجع السيطرة الأخلاقية، كلما زادت فرصة الشخص، زادت فرصته في أن يكون عرضة للجريمة دون ندم، وهذا نتيجة تربيته أو سماته الشخصية التي يمكن أن تؤثر على كل جانب من جوانب حياته. شعور متزايد بالذات لدى الشخص الذي يضع مصالحه الشخصية فوق كل اعتبار شيئا ما.

ثانياً: أسباب مجتمعية:

- أدت البطالة والأوضاع المالية الصعبة إلى لجوء الشباب والمبرمجين إلى ارتكاب جرائم إلكترونية مختلفة لإيجاد مكافآت مالية لهم.
- مطاردة الثروة: نرى الكثير من الشباب يرتكبون جرائم إلكترونية، بعضها يلحق الأذى والأضرار بالآخرين، سعياً وراء الثروات والمال الفوري.

- الدافع للانتقام: يلجأ الكثير من الأشخاص إلى الجرائم الإلكترونية للرد على شخص ما، سواء كانت سرقة حساباتهم أو ابتزازهم أو تهديدهم أو غيرها من الجرائم التي يرون أنها انتقام.
- الترفيه: أحياناً يلجأ الكثير من الشباب المتهورين إلى ابتزاز أو تهديد الآخرين، أو اختراق أجهزتهم والعديد من الجرائم الإلكترونية، كما يطلق عليهم الترفيه والمزاح مع الآخرين.
- أسباب سياسية: في كثير من الحالات تعتبر بعض الجرائم السيبرانية جرائم خاصة بين دول، وقد رأينا الكثير في الآونة الأخيرة في العديد من الدول وخاصة الولايات المتحدة والصين وإيران وإسرائيل وروسيا والعديد من الدول التي تتسلل إلى أنظمة دول أخرى لإضعافها و لتحقيق أهدافهم السياسية الخاصة.
- التطبيق غير الملائم للقوانين لمكافحة الجرائم الإلكترونية: يرجع حدوث الجرائم الإلكترونية وازديادها إلى التطبيق غير الفعال للعقوبات الجنائية في العديد من البلدان، مما يؤدي إلى التقصير الجنائي في أداء الواجب، والمعاملة المتساهلة، والافتقار إلى وسائل فعالة لإنفاذ القانون. رادع فعال ضدهم.
- إن الضغوط المختلفة التي تواجه المجتمع، مثل الفقر والبطالة وغيرها، والتي تؤدي إلى فرار الشباب، يسهل ارتكابها من خلال الجرائم الإلكترونية أكثر من الجرائم الفعلية.
- يسيطر الفراغ على أوقات الشباب وشغفهم، مما يدفعهم إلى ارتكاب الجرائم الإلكترونية.
- استخدام ما يسمى بالهندسة الاجتماعية، والتي تهدف إلى الاستفادة من بعض الأشخاص من خلال الاستفادة من الخير والغباء.

خصائص الجرائم الإلكترونية

للجرائم الإلكترونية عدّة خصائص، منها:

1. صعوبة معرفة مرتكب الجريمة، إلّا باستخدام وسائل أمنيّة ذات تقنية عالية. صعوبة قياس الضّرر المُترتِّب عليها، كونه ضرراً يمسّ الكيانات المعنوية ذات القيم المعنوية أو القيم الماديّة أو كلاهما سويّةً.
2. سهولة الوقوع فيها؛ بسبب غياب الرّقابة الأمنية.
3. سهولة إخفاء وطمس مَعالم الجريمة وآثارها والدّلائل التي تُدلّ على مرتكبها. هي أقلْ جهداً وعُنفاً جسديّاً من الجرائم التّقليدية. سلوكٌ غير أخلاقيّ في المجتمع. جريمةٌ لا تتقيّد بمكانٍ أو زمانٍ مُحدّدين.

أهداف الجرائم الإلكترونية

تهدفُ الجرائم الإلكترونية لجملةٍ من الغايات، منها: تحصيل مكسبٍ سياسيّ أو ماديّ أو معنويّ غير مشروع عبر تقنيات المعلومات كعمليّات تزوير بطاقات الائتمان، والاختراق، وتدمير المواقع على الإنترنت وسرقة الحسابات المالية. تحصيلُ معلوماتٍ ووثائق سريّة للمؤسسات والجهات الحكوميّة والمصرفية والشخصية لابتزازهم من خلالها. الوصول لمعلوماتٍ غير مُخوّل للعامّة الاطلاع عليها بشكلٍ غير مشروع، وسرقتها أوحذفها أوتعطيلها أو التعديل عليها لتحقيق مصالح مرتكب الجريمة.

الجرائم الإلكترونية واثرها على المجتمع

أصبحت الجرائم الإلكترونية واحدة من أكبر المخاطر التي يتعرض لها مستخدمو الإنترنت حيث تمت سرقة بيانات ملايين المستخدمين حول العالم في السنوات الأخيرة، قال رئيس (IBM)إن الجرائم الإلكترونية أصبحت أكبر تهديد لأي مهنة وأي صناعة وأي شركة، والتي يشير إلى تأثير كبير للجرائم الإلكترونية ضد المجتمع والعالم، مع ما يقرب من 48٪ من انتهاكات أمن البيانات بسبب الجرائم الإلكترونية التي تؤدي إلى زيادة متوقعة في وظائف أمن الكمبيوتر بأكثر من 3 أضعاف بحلول عام 2021م.

آثار الجرائم الإلكترونية المادية

غالبًا ما تهدف الجرائم الإلكترونية إلى الحصول على فوائد مادية، والخسارة الاقتصادية التي تسببها الجرائم الإلكترونية هي الضرر الرئيسي، مع الاستخدام العالي للإنترنت وتنفيذ الإجراءات المصرفية عن بُعد، ازدادت مخاطر الجرائم الإلكترونية، وكذلك حماية البيانات الشخصية والشركات والحفاظ على النسخ الاحتياطية من البيانات المهمة، تؤثر الجريمة الإلكترونية بشكل مباشر على اقتصادات دول كثيرة.

من هم مرتكبي الجرائم الالكترونية؟

هاكر أو كراكر :(Hacker or Cracker) هواة و خبراء بالكمبيوتر يستخدمون الكمبيوتر بشكل غير قانوني للترفيه ويكتشف بفضول أجهزة كمبيوتر الآخرين. الكراكرز أو الهاكرز المحترفون هم عصابات متخصصة في جرائم الإنترنت.

مكافحة الجرائم الإلكترونية

تسعى الدّول والحكومات بشكلٍ جديّ للحدّ من الجَرائم الإلكترونيّة وآثارها عبر طُرقٍ كثيرة منها:

1. فرضُ سياساتٍ دوليّة وعقوباتٍ كبيرة على مُرتكبي هذه الجَرائم. تفعيل أحدث التقنيات والوسائل للكشفِ عن هويّة مُرتكبي الجرائم.
2. نشر التّوعية في المُجتمعات حول الجرائم الإلكترونية ومَخاطرها، وتَعريف الأفراد بكيفيّة الحِفاظ على معلوماتهم وخصوصيّاتهم؛ كحساباتهم البنكية وبطاقاتهم الائتمانية.
3. إنشاء خطوط هاتفيّة ومؤسسات مُعيّنة تابعة للدّولة للإبلاغ عن الحالات التي تتعرّض لمثل هذا النّوع من الجرائم.
4. توجيه التّشريعات والقوانين وتحديثها بما يَتماشى مع التّطورات التكنولوجية، لفرض قَوانين جديدة فيما يستجدّ من هذه الجرائم.

للحد من الجريمة الإلكترونية اتبع هذه الطرق:

1. استخدام كلمات مرور قوية، و حاول دائماً تغيير كلمة السر بشكل دوري حتى لا تكون عرضة للإختراق.
2. لا تفتح المرفقات أبدًا في رسائل البريد الإلكتروني العشوائية.
3. التنبّه لعناوين مواقع URL التي تزورها.
4. استخدم مجموعة أمان الإنترنت "مكافحة الفيروسات" كاملة الخدمات.
5. إبقاء البرنامج ونظام التشغيل محدّثَين.
6. عدم تقديم المعلومات الشخصية لأي شخص.
7. وضع قوانين عقوبات رادعة لمرتكبي الجرائم المعلوماتية، وذلك للحد من انتشارها.
8. توعية الوالدين بكيفية حماية أطفالهم من قناصة الإنترنت.
9. بالنسبة للمؤسسات، يجب عليها اعتماد العديد من تدابير الحماية الأمنية الموصى بها وفقًا للمعايير الدولية لحماية بياناتها وأنظمة الكمبيوتر الخاصة بها من هجمات القرصنة، وتطوير سياسات الأمان التي تتم مراجعتها بانتظام.

عقوبة جرائم الإنترنت في مصر

- تتمثل عقوبة كل من يقوم بإرسال أي من البيانات التي تنتهك حرمة الحياة الشخصية، أو من يقوم بالتعدي على أي من الضوابط الأسرية، أو من يقوم باستخدام وسائل تقنية المعلومات بصورة تنتهك الخصوصية في السجن لمدة 6 أشهر كحد أدنى، بالإضافة إلى

دفع الغرامة المالية التي تبلغ قيمتها 50 ألف جنيه مصري كحد أدنى، وتصل قيمة الغرامة حتى 100 ألف جنيه مصري كأقصى حد.

- بينما تتمثل عقوبة كل من يقوم بإنشاء، أو استخدام موقع إلكتروني بهدف ارتكاب أي من الجرائم الالكترونية بالسجن لمدة عامين على الأقل، مع التكفل بدفع غرامة مالية تقدر ب100 ألف جنيه على الأقل، ولا تتجاوز هذه الغرامة عن 300 ألف جنيه مصري.
- وتنص المادة 26 من قانون مكافحة جريمة تقنية المعلومات على أنه: "يعاقب بالحبس مدة لا تقل عن سنتين ولا تجاوز خمس سنوات وبغرامة لا تقل عن مائة ألف جنيه لا تجاوز 300 ألف جنيه أو بإحدى العقوبتين كل من تعمد استعمال برنامج معلوماتي أو تقنية معلوماتية في معالجة معطيات شخصية للغير لربطها بمحتوى منافٍ للآداب العامة أو لإظهارها بطريقة من شأنها المساس باعتباره أو شرفه".

الفصل الخامس

الملكية الفكرية وحماية البرامج

Intellectual property and software protection

الملكيّة الفكريّة... تعريفها ومفاهيمها

الملكيّة الفكريّة حسب منظمة "الويبو" (المنظمة العالمية للملكية الفكرية) هي: حقوق امتلاك شخص ما لأعمال الفكر الإبداعية أي الاختراعات والمصنّفات الأدبية والفنية والرموز والأسماء والصور والنماذج والرسوم الصناعية، التي يقوم بتأليفها أو إنتاجها.

وتنقسم الملكية الفكرية إلى فئتين هما الملكية الصناعية التي تشمل الاختراعات (البراءات) والعلامات التجارية والرسوم والنماذج الصناعية وبيانات المصدر الجغرافية من جهة وحق المؤلف الذي يضم المصنفات الأدبية والفنية كالروايات والقصائد والمسرحيات والأفلام والألحان الموسيقية والرسوم واللوحات والصور الشمسية والتماثيل والتصميمات الهندسية من جهة أخرى. وتتضمن الحقوق المجاورة لحق المؤلف حقوق فناني الأداء المتعلقة بأدائهم وحقوق منتجي التسجيلات الصوتية المرتبطة بتسجيلاتهم وحقوق هيئات الإذاعة المتصلة ببرامج الراديو والتلفزيون.

يرجع تاريخ حقوق الملكية الفكرية إلى سنة ١٨٧٣ م، وبالتحديد في المعرض الدولي للاختراعات بفيينا حيث حدثت صدمة للقائمين على المعرض وللجمهور عندما امتنع عدد كبير من المخترعين الأجانب عن المشاركة. وكان السبب في الامتناع هو خشية هؤلاء المخترعين من أن تتعرض أفكارهم للنهب والاستغلال التجاري في بلدان أخرى.... لقد أظهرت هذه الحادثة الحاجة إلى توفير الحماية الدولية لبراءات الاختراع (وللملكية الفكرية

بوجه عام)، الأمر الذي كانت نتيجته انبثاق أول معاهدة دولية مهمة ترمي إلى منح مواطني بلد معين حق حماية أعمالهم الفكرية في بلدان أخرى.

إنها اتفاقية باريس بشأن حماية الملكية الصناعية والتي صدرت في ٢٣ مارس عام ١٨٨٣، ودخلت حيز التنفيذ في العام التالي، وأصبح بمقتضاها للملكية الصناعية حماية تتخذ شكل حقوق تعرف بمصطلحات محددة، وهي: «براءات الاختراع»، و«العلامات التجارية» و«الرسوم الصناعية».. كانت اتفاقية باريس مجرد البداية التي توالت بعدها الاتفاقيات والترتيبات على المستوى الدولي من أجل حماية الملكية الفكرية في شتى صورها (مصنفات فنية وأدبية.. الخ)، حتى أصبح لكافة شؤون الملكية الفكرية منظمة دولية مكلفة بإدارتها، بإقرار من الدول الأعضاء في الأمم المتحدة، بدءاً من ١٧ ديسمبر ١٩٧٤، وهي المنظمة العالمية للملكية الفكرية (والتي يشار إليها بالفرنسية بالمختصر OMPI وبالإنجليزية بالمختصر (WIPO).

ثم فوجئت الدول الأعضاء في مفاوضات اتفاقيات الجات بورقة مقدمة من الشركات العملاقة متعددة الجنسيات إلى سكرتارية الجات في جنيف (في يونيو ١٩٨٨ (بخصوص تضمين اتفاقيات الجات اتفاقية خاصّة بما يسمى: «حقوق الملكية الفكرية المرتبطة بالتجارة». والجدير بالانتباه هنا أن هذه الشركات فرضت ورقتها على المفاوضات رغم عدم عضويتها في تلك المفاوضات، حيث إن العضوية للدول. والجدير بالانتباه أيضًا أن ذلك قد تم من وراء منظمة ويبو (المنظمة العالمية للملكية الفكرية والتابعة للأمم المتحدة).

كانت الشركات ذات النشاط الدولي ترغب في تأمين مستويات أعلى من الحماية للملكية الفكرية (وعلى وجه الخصوص لبراءات الاختراع والعلامات التجارية)، وصدرت - بالفعل - اتفاقيات الجات متضمنة اتفاقية لحقوق الملكية الفكرية المرتبطة بالتجارة. والتي يطلق عليها اختصاراً اتفاقية «تريبس». ووقعت اتفاقيات الجات في إبريل ١٩٩٤، ونشأت بموجبها منظمة التجارة العالمية World Trade Organization حيث بدأت مع أول يناير ١٩٩٥ ممارسة أعمالها في السهر على (أو حراسة) تنفيذ اتفاقيات الجات، والتي صارت تعرف الآن باتفاقيات التجارة العالمية .

إنَّ جميع الكتب والمراجع والأبحاث والفتاوى العربية التي تناولت موضوع "الملكية الفكرية" والتي عثرتُ عليها، لم تبحث في أصل مصطلح "الملكية الفكرية" وكيفية نشأته؟ باستثناء مرجع وحيد. لنرى كيف سارت الأمور؟ تقسم الأشياء التي يمكننا إدراكها إلى صنفين : مادية ومعنوية. فالمادية هي كل ما وقع تحت سلطان الحواس، والمعنوية هي كل ما لا يمكن للحواس أن تطاله، كالمفاهيم المجردة والعواطف الإنسانية والاجتهادات الفكرية وغير ذلك.

وكما يدرك كل عاقل، فلا يمكن التعامل مع المعنويات كما نتعامل مع الماديات، فلا يمكننا حساب وزن الروح، أو ثقل الكراهية، أو طول الإبداع ! كما لا يمكننا بيع الحب، أو إقراض الذكاء، أو حتى امتلاك الأفكار!! نعم هذا لم يكن ممكناً حتى ظهور مصطلح "المادة الفكرية (Intellectual material) "على أيدي منظمة الـ SPA أو(اتحاد ناشري البرامج)، ليس المقصود بهذا المصطلح "المنتجات الفكرية" التي هي الوسائط المادية التي تُخزّن عليها الأفكار، كالكتب، والأقراص الليزرية، وشرائط الكاسيت، بل إنه التسمية الجديدة للفكرة ذاتها!

قد يبدو هذا صعب التقبل للوهلة الأولى، فالمقصود بـ"المادة الفكرية" هو الفكرة ذاتها، التي تسكن دماغاً ما، وقد يعبّر عنها شفويًا أو بشكل مكتوب وقد تترجم إلى منتج مادي، الفكرة نفسها أصبحت تسمى بـ "مادة"، ولأول مرة في تاريخ البشرية تم إعطاء صفة مادية لشيء معنوي.

الآن أصبحت الأفكار عبارة عن مادة أخرى، الآن أصبح بإمكاننا الحديث عن "الملكية الفكريةIntellectual Property "، لأن الفكر هو الآخر أصبح "مادة "فلمَ لا يتم الحديث عن امتلاكه وبيعه ... والأهم من ذلك احتكاره.

لم يظهر مصطلح "الملكية الفكرية" أولاً، في البداية كان يتوجب تحويل الفكر إلى مادة فتم وضع مصطلح "المادة الفكرية" الذي لم يكن أحدٌ على الإطلاق يتخيل وجوده في يوم ما، فعندما يتوقف الربح والمزيد من الربح على بيع المعنويات، سنجد من يحول هذه المعنويات إلى أشياء مادية ليسهل بيعها.

قبل أن نتناقش في "مَن يملك الفكرة؟ وما حدود ذلك ؟ والخ.."، ألا يجدر بنا أن نتساءل " هل يمكن للأفكار أن تُمتلك أصلًا ؟ " وهذا السؤال مهمل تمامًا.

لقد سلّم جميع الباحثون والمفكرون والفقهاء بصحة مصطلح "الملكية الفكرية "دون أن يناقشه أحدٌ البتّة، رغم أن هذا المصطلح استند في وجوده إلى تحويل الفكر إلى مادة عن طريق "المادة الفكرية". لم يكن "امتلاك" الأفكار مطروحًا قبل مصطلح "المادة الفكرية"، اليوم لا أحد يناقش هذا المصطلح ... لكن الحقيقة التي لا يمكن تجاهلها أن الفكر أصلًا ليس بمادة، الفكر غير موجود في الحيز المادي، نعم المنتجات الفكرية (كالكتب مثلًا) هي أشياء مادية، ويجوز الحديث عن "امتلاكها"، لكن الأمر أعمق من ذلك بكثير، الحديث هنا عن الفكرة ذاتها والتساؤل يدور حول (من يمتلكها؟).

في هذه الدراسة سنسلم – افتراضًا - بصحة مصطلح "المادة الفكرية" (متجاهلين أن الفكر لا يملك طبيعة مادية)، وذلك حتى نتمكن من مناقشة أفكار "الملكية الفكرية" وعرضها ...

ما هي الحقوق التي يضمنها قانون الملكية الفكرية ؟

بالنسبة للكتب: "يمنع طبع هذا الكتاب أو جزء منه بكل طرق الطبع والتصوير والنقل والترجمة والتسجيل المرئي والمسموع والحاسوبي وغيرها من الحقوق إلا بإذن خطي من ... "

بالنسبة للبرامج فإن اتفاقية المستخدم الأخير (EULA) تضم العديد من البنود، فهي تضمن كتم الكود المصدري للبرامج[٤] وتجريم كشفه أو نشره أو تعديله[٥]، كما أنها تعطي المستخدم حق "استخدام" البرنامج وليس "امتلاك" البرنامج، وهي تجبر المستخدم على شراء عدة نسخ من البرنامج عند الحاجة، فإن من يملك في منزله ثلاثة أجهزة كمبيوتر أو في شركته مئة جهاز فعليه شراء مئة ترخيص في الحالة الثانية وثلاثة في الحالة الأولى، وهنا نحن نتحدث عن شراء التراخيص وليس شراء البرنامج !إن اتفاقية المستخدم الأخير (الأكثر شهرة ضمن اتفاقيات ترخيص البرامج) تضمن أن المستخدم لن يعطي البرنامج لصديقه أو جاره (حتى لو لم يكن جاره يملك ثمن نسخة أصلية) كما أنها تمنع المستخدم من تطوير البرنامج أو تعديله ..... باختصار فإن هذه الرخصة تتيح لك استخدام البرنامج فقط.

بالنسبة للشرائط الصوتية والمرئية فإنه يمنع نسخها أو نقلها إلى الكمبيوتر أو توزيعها.

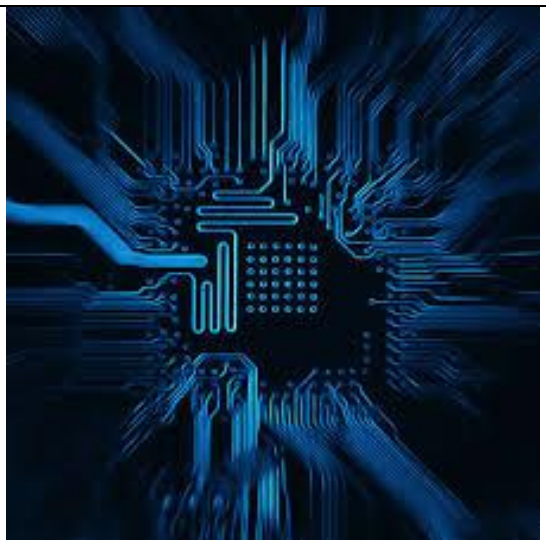
بعض الرخص تذهب لأكثر من ذلك، لكن ما ذكرناه هو الشائع، أحيانًا تمنع شروط الملكية الفكرية الاقتباس من الكتاب إلا بإذن خطي! وبالنسبة للبرامج تباع أحيانًا رخصة استخدامه لمدة زمنية معينة كعام أو عامين مثلًا ثم يجب تجديدها !!.

لماذا يجب تطبيق قوانين الملكية الفكرية؟

تطبيق قوانين الملكية الفكرية يعتبر أمرًا بالغ الأهمية لعدة أسباب، منها:

1. حماية حقوق المبدعين والمبتكرين: قوانين الملكية الفكرية تضمن للمبدعين، سواء كانوا كتابًا، فنانين، مطورين، أو مخترعين، حقوقهم في استخدام واستغلال أعمالهم. هذه الحماية تشجع على الابتكار والإبداع من خلال ضمان أن جهودهم ومواهبهم لن تذهب سدى بسبب النسخ أو السرقة.

2. تشجيع الابتكار والتقدم التكنولوجي: عندما يعرف المبتكرون أن أفكارهم واختراعاتهم ستكون محمية بموجب القانون، فإنهم يكونون أكثر استعدادًا لاستثمار الوقت والموارد في تطوير منتجات وخدمات جديدة. هذا يعزز الابتكار ويساهم في تقدم المجتمع بأسره.
3. تحفيز الاقتصاد: الملكية الفكرية تساهم في الاقتصاد من خلال حماية الاستثمارات في البحث والتطوير. الشركات والأفراد يشعرون بالأمان للاستثمار في تطوير منتجات جديدة إذا كانت محمية قانونيًا من التقليد غير المشروع، مما يدفع عجلة الاقتصاد ويخلق فرص عمل جديدة.
4. ضمان الجودة والسلامة: قوانين الملكية الفكرية تساعد في حماية المستهلكين من المنتجات المقلدة التي قد تكون ذات جودة منخفضة أو حتى ضارة. العلامات التجارية المسجلة، على سبيل المثال، تضمن للمستهلكين أن المنتج الذي يشترونه هو الأصلي ويخضع للمعايير التي يتوقعونها.
5. تعزيز التنوع الثقافي: حقوق الملكية الفكرية تحمي التراث الثقافي والفني من الانتحال والضياع. هذا يساهم في الحفاظ على التنوع الثقافي ويشجع على نشر وتقدير الأعمال الثقافية والفنية في جميع أنحاء العالم.
6. منع الاستغلال غير العادل: بدون قوانين الملكية الفكرية، يمكن للأطراف القوية اقتصاديًا أو تقنيًا أن تستغل إبداعات الآخرين دون تعويض مناسب، مما يخلق بيئة غير عادلة ولا تحفز على الإبداع.
7. الحماية القانونية على الصعيد الدولي: قوانين الملكية الفكرية، عندما تكون جزءًا من اتفاقيات دولية، توفر الحماية على مستوى عالمي. هذا يتيح للمبدعين والمبتكرين الاستفادة من حقوقهم في أسواق متعددة وليس فقط في بلدهم الأم.
8. تطبيق قوانين الملكية الفكرية هو جزء أساسي من نظام قانوني عادل يسعى لتحقيق التوازن بين حقوق الأفراد والمجتمع ككل، وبين تشجيع الإبداع وحماية المصلحة العامة.



أنواع الملكية الفكرية

يمكن تصنيف مكونات وحقوق الملكية الفكرية إلى مجموعتين:

1- مكونات الملكية الفكرية التقليدية: وهي المكونات والحقوق المعروفة وتتمتع بالحماية وهي: الأسرار التجارية، والبراءة، والعلاقة التجارية، وحق النشر.

2- المكونات والحقوق الرقمية للملكية الفكرية: وقد ظهرت في ظل الإنترنت، وذات طبيعة رقمية في جانبها الأهم وتشمل البرمجيات، قواعد البيانات، والمواقع الالكترونية.. إلخ.

أولا: الحقوق التقليدية للملكية الفكرية

أ. الأسرار التجارية

إن السرية التي هي سمة الحصر في استخدام المعلومات أو تداولها تقابل مفهوم النطاق العام (Public Domain) الذي يشير إلى أن المعلومات تكون شائعة الاستخدام للجمهور. والأسرار التجارية (Trade Secrets) هي طرق العمل وخططه وتفاعلاته، التي يتم حمايتها من خلال القانون، ومن خلال الإلزام التعاقدي المباشر. كما هو الحال في عقود استخدام العاملين التي يجب أن تتضمن تحديدا لالتزاماتهم المتعلقة بالسرية التي إن خرقوها يتعرضون للمسائلة القانونية[1]. وهذا ما تقوم به الشركة أيضا في اتفاقاتها مع زبائنها في مطالبتهم بعدم كشف هذه الأسرار، وفي الوقت نفسه فأنها تعمل على حماية هذه الأسرار من التحول إلى النطاق العام.

ب. براءة الاختراع

إن براءة الاختراع (Patent) هي وثيقة قانونية تمنح المبتكر أو الشركة المالكة للابتكار حقا احتكاريا على الأفكار أو المعارف التي تتضمنها، والقابلة للتحول إلى آلة أو جهاز أو طريقة عمل أو خدمة محددة، ولا يمكن استخدامها من الآخرين إلا بإذن من المالك أو التزام تعاقدي. والبراءة هي الشكل الأكثر استخداما والأكثر أهمية في التعبير عن الابتكارات والانجازات التكنولوجية التي كانت الأساس في التطور منذ العصر الصناعي حتى الآن.

ج. العلامات التجارية

إن العلامة التجارية (Brand) هي نتاج تاريخ الشركة ونجاحاتها في الجودة (خصائص أفضل من المنافسين)، أو الخدمة (إيفاء متكرر أفضل لحاجات الزبون)، والثقة (علاقات معول عليها ومخاطرة شراء أقل)، والتفوق (البقاء في المقدمة لفترة طويلة نسبيا).. إلخ. لهذا كله يكون من حق الشركة أن تحقق منافع أو علاوة سعرية من علامتها بالاستخدام، ومنافع وعوائد مالية من ترخيص استخدام علامتها التجارية المحمية بالقانون كأحد الحقوق الرئيسية للملكية الفكرية، والعلامات التجارية يمكن أن تكون علامات المصنّع أو الموزّع، كما قد تكون فردية (تخصص لمنتج معين)، أو عائلية (العلامة تستخدم لمجموعة من المنتجات وترخص لشركات أخرى)، وهناك العلامات المشتركة (Co-Brand) (كما في استخدام علامتين على منتج واحد.

د. النماذج الصناعية

النماذج الصناعية (Industrial Models) أشكال ومجسمات ثلاثية الأبعاد، وتستخدم فيها الخطوط والألوان التي تعطي مظهرا معينا يستخدم في الصناعة أو في الحرف، وتتمتع بالحماية القانونية جراء الخصائص المتميزة الجديدة التي تتسم بها.

هـ. حق النشر

إن حق النشر أو المؤلف (Copyright) من الحقوق القديمة المحمية بالقانون. حق النشر أسهل في الحصول من براءة الاختراع، كما أن الفترة الزمنية التي يغطيها هي أطول من فترة حماية البراءة. وهذا ما يظهر جليا في أن حق النشر يستمر طوال حياة المؤلف، كما أن بعض القوانين تجعل هذا الحق يستمر لفترة تمتد إلى سبعين سنة بعد موت المؤلف[4]. ومع ذلك فإن حق النشر يتضمن كل قواعد حماية الملكية في الحق الحصري للمؤلف في عدم إعادة إنتاج العمل الخاضع لحق النشر إلا بعد أخذ الموافقة منه مع القدرة على منع الآخرين من عمل نسخ منه. وهناك شروط أساسية لابد من توافرها في العمل الذي يحصل على حق النشر هي:

1- **التثبيت**: أي أن يكون معبرا عنه بشكل مادي، والتوصل إليه أولا كنص مكتوب كما في الجداول أو المصنفات (Compilations) كقواعد المعلومات، والوثائق، والصور، والرسوم، والأكثر حداثة يتمثل ببرامج الحاسوب.

2- **الأصالة**: أن يكون العمل أصيلا وقيمته أصيلة.

3- **الحقوق المعنوية**: إن العمل الإبداعي هو في جانب منه عمل مادي، يمثل المصلحة المادية للمؤلف في نشره وتقديمه وإيصاله للجمهور، وهذا ما يسمى الحق الاقتصادي الذي يحمى بالوسائل القانونية. وفي الوقت نفسه هو جزء من الملكية الفكرية للمؤلف وشخصيته الإنسانية مما يخرج عن نطاق المصلحة المادية. وكل شيء له قيمة أعلى من الملكية المادية ويوجد خارج الشخصية يمثل الحق المعنوي (Moral Right).

ثانيا: الحقوق الرقمية للملكية الفكرية.

إن الملكية هي الامتداد الأقوى لقدرة الفرد أو الشركة، وهذا ما يمكن أن ينطبق على حقوق الملكية الفكرية التقليدية، وعلى مكونات الملكية الفكرية الرقمية التي تسمى أيضا الحقوق الرقمية (Digital Rights).

إن المكونات الرقمية (البرمجيات، قواعد البيانات، المواقع الالكترونية.. إلخ) تدخل ضمن هذه الحقوق، شأنها شأن المنتجات المادية والفكرية التقليدية، إذا ما توفرت فيها شروط شمولها بالحماية القانونية. ولكن بالمقابل لابد من مراعاة الخصائص المتميزة لهذه المكونات، وخصائص الإنترنت كشبكة عالمية سريعة الإرسال، والنسخ، والتقاسم، للمعلومات وغيرها مما يؤثر على الحقوق الرقمية تأثيرا كبيرا.

ونعرض فيما يأتي لمكونات الملكية الفكرية الرقمية أو الحقوق الرقمية:

1- البرمجيات

البرمجية (Software) خلاف الأجهزة (Hardware) هي تعليمات وقواعد ونماذج تساعد على معالجة البيانات، والقيام بالوظائف المحددة التي صممت من أجلها بسرعة فائقة. والبرمجيات هي من أكثر المنتجات الرقمية حاجة للحماية، لأنها الأكثر عرضة للقرصنة. بل إن قرصنة البرمجيات (.Piracy S) لا يكاد يخلو منها بيت من بيوت المستخدمين للحاسوب أو الإنترنت. ويشير لوكس (H.C.Lucas) إلى أن قرصنة البرمجيات في بعض الدول تقدر بحوالي (90-98 ٪) من مجموع البرمجيات المستخدمة فيها، وإن محامي مايكروسوفت يقدرون أن الشركة خسرت ما يعادل نصف عوائدها عبر العالم عن طريق القرصنة.

وعلى الرغم من أن البرمجيات (بنوعيها برمجيات النظام وبرمجيات التطبيق) كانت موجودة قبل الإنترنت والاستخدام التجاري الواسع لشبكات الأعمال، إلا أنها أصبحت في ظل الإنترنت تشكل القدرة الفكرية والخبرة العظيمة التي تحرك اقتصاد المعلومات كله والمصدر الأكثر فاعلية وكفاءة في صنع الثروة في الأعمال الإلكترونية.

ومع أن البرمجية تأليف شأنها شأن أي بحث أو كتاب - مما يتطلب شمولها بحماية حق النشر - إلا أنها قد تكون بمثابة نظام أو طريقة جديدة لتأدية الوظائف أو الأعمال، لذا فإنها تخضع أيضا إلى حماية قانون براءة الاختراع.

إن التوجه العام سواء على الصعيد الوطني في كل دولة، أو على المستوى الدولي (كما في المنظمة العالمية للملكية الفكرية)، يميل إلى توسيع التشريعات الحالية لتغطي المنتجات الرقمية وفي مقدمتها البرمجيات. وإن كان البعض يرى أن القوانين الحالية لا تصلح لأن تطبق عليها، وأن الحاجة ماسة لأنظمة جديدة لحقوق الملكية الفكرية في الاقتصاد الجديد.

2- قواعد البيانات الالكترونية

لا يشترط بقواعد البيانات أن تكون إلكترونية لكي تكون محمية بقوانين حماية الملكية، شأنها شأن الأعمال الأخرى التي تتوافر فيها متطلبات التمتع بالحماية القانونية. فهذه القواعد تبنى (تؤلف) للقيام بوظائف أسرع وأرخص، وبمهنية عالية مما يمنحها مبررا للحماية. فهي تتمتع - بكونها طريقة جديدة لمعالجة وظائف معينة تم التوصل إليها بقدرات عالية - بحق البراءة مثل أولئك الذين يبتكرون طرقا جديدة ذات قيمة وظيفية عالية التي يمكن أن تنعكس على جودة أفضل، وتكلفة أقل، وأداء أسرع تبرر حمايتها. كما أن مثل هذه القواعد قد تتمتع - من جانب آخر - بحق النشر الذي يتمتع به أولئك الذين يبدعون أعمالا من مختلف الأنواع، مما يحميها من الاستنساخ واستغلال الآخرين. ويعمل البعض من أجل حمايتها بحق خاص هو حق قاعدة البيانات (Database Right)، ووفقا لذلك تعرف قاعدة البيانات بأنها مجموعة من

الأعمال، والبيانات، والموارد الأخرى التي ترتب بطريقة منهجية ونظامية قابلة للوصول إليها بوسائل الكترونية أو غيرها على أن تكون أصيلة.

3- الموقع الالكتروني

الموقع الالكتروني هو توصيف للمعلومات (نصوص، صور، رسوميات.. إلخ) التي تعرض على صفحات الموقع الالكتروني الخاصة بالشركة. والموقع الالكتروني هو من نتاجات الإنترنت بعد استخدامها لأغراض تجارية إذ أصبح ممثلا لقدرات الشركة في التصميم، والعرض، والإعلان، والإقناع، وتقديم الخدمات، والتفاعل، والبيع، والشراء، وغيرها مما يمكن تلخيصه بكونه طريقة متميزة خاصة بالشركة في تقديم الأعمال؛ ولأنه كذلك فإنه يمكن أن يتمتع بالحماية القانونية. كما أن الموقع الالكتروني يحمل اسم الشركة وترويستها الإعلانية مما يجعله يتمتع بالحماية القانونية الخاصة بالعلامة التجارية. لأنه يمكن أن يعرض منتجات رقمية كالألعاب والكتب والبرمجيات للسرقة لذلك يحظى بالحماية القانونية الخاصة بحق النشر.

لقد حصلت شركة أمازون على براءة الاختراع (التسوق بنقرة واحدة One-Click Shopping) على الانترنت، وبعدها شركة (Priceline) على مزاداتها المعاكسة. لتبدأ فترة جديدة من إمكانية الحصول على براءات الاختراع لنماذج الأعمال التي يتم تصريفها وتأديتها عن طريق الموقع الالكتروني.

برمجيات الحاسب

تعد البرمجيات software ملكية شخصية ولا يمكنك استخدام ملكية شخص آخر بدون إذن منه، ويضن الكثير من الناس أن الملكية هي شيء ما ملموس، أو قابل لآن يدرك باللمس ونمارس عليه سلطة كتلك التي نمارسها على ملكية حقيقية كقطعة أرض مثلا، وكلما يمكن وضعه عليها هو ملكية شخصية أيضا ويحق لنا الدفاع عنها ومنع الآخرين من ممارسة أي سلطة عليها. وفي الاستخدام العام نقول أيضا أن البرمجيات الحاسوبيه هي ملكية شخصيه ملموسة ويقوم الناس بشرائها من المحلات ويدفعون ثمنها بذات النقود التي يشترون بها قطعة أرض أو منزل مثلا.

ولكن مفهوم البرمجيات كملكية فكرية هو أكبر من الاسطوانة التي تحمل البرمجيات، وتعتبر الأخيرة من مخرجات التفكير الإنساني وبالتالي نوع من الملكية الفكرية ويسمح القانون لمالكها أن يتحكم فيها، فالمبرمج الذي كتب البرنامج أو الشركة التي تستأجر ذلك الشخص الذي كتب البرمجيات، يعتبر المالك الأول للملكية الفكرية المضمنة بالبرمجيات، ويحق للمالك ممارسة السلطة على هذه الملكية فيمكن اعطاؤها للغير أو بيعها أو اجازة استخدامها من قبل الآخرين، ويحق له أن يعمل نسخا منها ويحق له أيضا منع الآخرين من الاستخدام أو عمل نسخ أو بيع منتجه الفكري. ونظرا لوجود جانب ملموس وجانب آخر غير ملموس في برمجيات الحاسوب فإنه من الممكن امتلاكها من قبل أطراف مختلفة وهي عبارة عن:

- النسخة الملموسة للبرمجيات التي تشترى من المحلات أو تستجلب عبر الإنترنت
- الملكية الفكرية المتجسده في تلك البرمجيات
- حرية البرمجيات والمصدر المكشوف

تقدم الأنظمة المفتوحة open systems وعدا بالسماح لكل أفراد المجتمع بالاستفادة من مفهوم حرية البرمجياتsoftware freedom ، ويرتبط مفهوم حرية البرمجيات بمفهوم المصدر المكشوف open source ويعني هذا المصطلح أن تكون التدوينه المصدر للبرنامج source code مكشوفة ومتاحة للجميع حتى يمكن دراسة البرنامج وتعديله وتطويره، وتعتبر التدوينة المكشوفة متطلب أساسي لحرية البرمجيات. لذا فإن حرية البرمجيات هي الهدف وأما الأدوات لتحقيق هذا الهدف هو المصدر المكشوف open source وتقسم حرية البرمجيات إلى أربعة أنواع رئيسيه

- حرية تنفيذ البرمجيات لأي غرض
- حرية دراسة الكيفية التي تعمل بها البرمجيات وتكييفها لحاجة المستخدم
- حرية إعادة توزيع نسخ من البرمجيات
- حرية تطوير البرمجيات وتوزيع النسخ المحسّنة للجمهور

وتوجد سياسة عامة تعكس مفهوم المصدر المكشوف وتوضح أمور أخرى تتعلق بالتراخيص المقبولة في ظل هذه المعايير وهي:

1. حرية إعادة التوزيع

لا تقيد الرخصة الممنوحة أي طرف في بيع أو منح البرمجيات كوحدة أو كبرنامج متكون من عدد من الوحدات المندمجة من عدة مصادر مختلفة، ولا تتطلب الرخصة جُعالة أو أية رسوم.

2. تدوينة المصدر

يجب أن يتضمن البرنامج التدوينة المصدر، ويجب أن يسمح بالتوزيع في شكل مصدري أو في صيغة مُجمّعهcompiled ، وفي الحالات التي لا يوزّع فيها المنتج بشكل تدوينة المصدر يجب توفير وسائل محددة للحصول على التدوينة المصدر ويفضل استجلابها عبرالشبكة المعلوماتية internet وبدون مصاريف، ويجب أن تكون التدوينة المصدر الصيغة المفضلة التي بها يستطيع المبرمج التعديل في البرنامج.

3. الأعمال المُشتقّة

يجب أن يسمح الترخيص بالتعديل في البرنامج الأصلي وإنتاج أعمال مُشتقّه ويجب أن يسمح بإعادة توزيع الأعمال في ظل ذات الشروط التي يحملها الترخيص الممنوح للبرنامج الأصلي.

4. دمج التدوينه المصدر

قد يعمل الترخيص على الحد من توزيع التدوينة المصدر في شكل معدّل فقط إذا كان الترخيص يسمح بتوزيع " ملفات الحزمة " patch file بصحبة التدوينة المصدر لغرض تعديل البرنامج في فترة البناء والتطوير، ويجب أن يسمح الترخيص بشكل صريح توزيع البرمجيات المكوّنة من تدوينة المصدر المعدّلة، وقد يتطلب أن تحمل الأعمال المشتقة أسما مختلفا أو رقم نسخة آخر عما هو مخصص للبرنامج الأصلي.

5. عدم التعصب ضد أشخاص أو جماعات

يجب أن لا يعمل الترخيص على التمييز ضد أي شخص أو مجموعة من الأشخاص.

عدم التمييز ضد مجالات الاهتمام

لا يجب أن يقيد الترخيص أي شخص من استخدام البرنامج في مجال اهتمام محدد، فمثلا لا يمكن منع استخدام البرنامج في الأعمال التجارية أو استعماله

براءة برمجيات

تعد براءة الاختراع بتقديم حق السيطرة للمخترعين كمقابل لاكتشافهم أو اختراعهم ولمدة زمنية محددة تسمح لهم بتغطية تكاليف الاختراع أو الاكتشاف، وتُمنح براءة الاختراع على المنتجات الملموسة أو العمليات الصناعية في مجالات التقنية الحديثة والمفيدة، ويستثنى من ذلك الخوارزمات الرياضية mathematical algorithms والأفكار المجردة abstract ideas. ومع ظهور التقنيات المصاحبة للحاسوب وصناعة البرمجيات أصبح من الضروري إيجاد حقوق ملكية فكرية مناسبة لحماية هذا المجال التقني المهم، وهناك إجماع عام بأن برامج الحاسوب computer programs سواء كانت في شكل مصدري source code أو تدوينة تنفيذيه، يجب ان تُحمى بقانون حق النشر copyright وبالتالي فإن الأفكار التي تكمُن وراء برمجيات الحاسوب هي خارج نطاق أية حماية. وفي الولايات المتحدة الإمريكية فإن برامج الحاسوب التي تنفذ على الحاسوب أو تدوّن على وسط قابل للقراءة، يمكن الحصول على براءة اختراع لها. اما في أوروبا فإن آراء مختلفة حول السماح بإصدار براءة اختراع للبرمجيات ما زالت قائمة وهناك من يدعو إلى استبعاد برامج الحاسوب من قائمة الاختراعات وعدم اعتبارها مساهمة تكنولوجيه، ولدول العالم الثالث فإن تقليل الحماية وخاصة براءة

الاختراع في هذا الوقت هو أمر ضروري للسماح للمؤسسات والشركات الوطنية والجمعيات الأهلية المتخصصة بالتقدم في هذا المجال إذ ان الحماية هي فقط في صالح الشركات العملاقه.

الاستنتاج

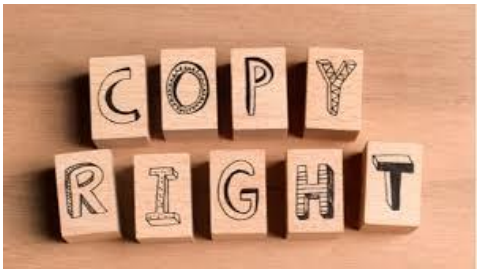
تثير التغيرات التي تحدث في بيئتنا اليوم فيما يتعلق بتقنية المعلومات والاتصالات وسياسة الملكية الفكرية أهمية خاصه في عدة جوانب منها: أولا، نظرا لأن الحقوق قائمة طالما توفرت قوة تحميها فإنه علينا معرفة الكيفية التي تؤثر بها قوة القانون الدولي للملكية الفكرية في نظام الملكية الفكرية محليا لتأسيس توازن بين كل من المبدع والمجتمع. ثانيا: يجب معرفة تأثير المعلومات وقوانينها الوطنية والدولية في صناعة المعلومات المحلية.

الملكية الفكرية وحقوق المؤلف في البيئة الرقمية

1- الملكية الفكرية في البيئة الرقمية:

في ظل التطور الإلكتروني الحالي والمستمر، وبصفة خاصة ما أتاحته شبكة الإنترنت من إمكانية التواصل بين الحاسبات، أصبح مجال حماية حقوق الملكية الفكرية في بيئة الإنترنت (الرقمية)، اثار تساؤل وجدل للكثيرين، وذلك بشأن تحديد المصنفات محل الحماية، واستقصاء الحماية اللازمة لمواجهة الاعتداءات والمخاطر التي تعترض هذه الحقوق، وتقييم ما إذا كانت تقع ضمن تشريعات الملكية الفكرية، أو غيرها من التشريعات الكافية لتوفير الحماية لتلك الحقوق، أم أن هناك حاجة إلى تشريعات خاصة للمصنفات في بيئة الإنترنت، ونحن حين نبحث في حقوق المؤلف، والحقوق المجاورة له في محيط تلك البيئة، فإنه يجدر بنا أن نتحدث عن:

1. أصحاب حق المؤلف والحقوق المجاورة، سواء المؤلف نفسه، أو المرخص له، أو المتنازل إليه من المؤلف عن حق الاستغلال المالي (كلياً أو جزئياً).
2. عن مستخدمي المصنفات الخاضعة للحماية مثل الأفراد الذين يرغبون في استعمال تلك المصنفات سواء لمنفعة شخصية.



وهذه المسائل ما تزال مثار جدل وبحث، وقد أدت هذه المشكلات الناجمة عن مستحدثات التطور التقني وظهور الإنترنت إلى تسارع خطوات التعاون الدولي في مجال تنظيم تلك الحقوق والحقوق المجاورة، وذلك في محيط تلك الشبكة، أو المحيط الرقمي؛ حيث صدرت بعض

النصوص المنظمة لذلك في اتفاقية التريبس TRIPS، ثم تلاها التنظيم الوارد في معاهدتا الويبو WIPOاللتان عرفتا باسم معاهدتا الإنترنت الصادرتان عام 1996، تحت مسمى "معاهدة الويبو بشأن حق المؤلف"، و "معاهدة الويبو بشأن الأداء والتسجيل الصوتي"، ولذلك فإن الصعوبات العملية المرتبطة بالتقنيات الحديثة، أو باستخدام شبكة الإنترنت تتجاوز الحلول المطروحة من خلال المعايير الدولية، ومن أمثلة تلك الصعوبات التي تواجه حقوق المؤلف ما يلي:

1. تعدد واختلاف الجهات المختصة بنظر المنازعات المتعلقة بالاعتداء على حق المؤلف.
2. تعدد واختلاف القوانين واجبة التطبيق على تلك النزاعات اعتماداً على الأماكن، أو الدول التي تم فيها الاعتداء من خلال النشر، أو إعادة النشر، أو الاستغلال دون ترخيص، أو دون موافقة المؤلف.
3. القيام بالكثير من الاعتداءات مثل أعمال النسخ، والنشر، والإتاحة، والتوزيع بدون موافقة، أو تصريح صاحب الحق على أجهزة يملكها، أو أشخاص متفرقين لا يوجد بينهم رابط سوى الإنترنت.
4. في الحالة التي يرغب صاحب الحق (المؤلف) في مقاضاة المعتدين على المصنف محل الحماية، وحقوقه المرتبطه به، فإنه سوف يقاضي أشخاص كثيرين ومتفرقين ومختلفين ومن مواطني دول كثيرة، وبالتالي فإنه يواجه صعوبات جامة وكثيرة مثل تعدد القوانين واجبه التطبيق.

2- حق الملكية الفكرية في البيئة الرقمية:

لا توجد مشاكل كبيرة بالنسبة لحقوق النشر أو الملكية الفكرية في مجال المواد المطبوعة، فشراء المكتبة للنسخة المطبوعة يخولها لإعارتها لمن تريد وبأي عدد من المرات بدون الحصول على أي ترخيص من مالك حقوق النشر، كما أن المستفيد من المكتبة التقليدية يقوم باستعارة وعاء المعلومات من أجل القراءة والإطلاع ومن ثم يقوم بإعادته للمكتبة لتقوم هي بعد ذلك بإعارته لشخص آخر.بينما في المكتبة الرقمية فالأمر مختلف تماماً، فلا توجد هناك عملية استعارة أساساً فالمستفيد يقوم بعملية إنزال مصدر المعلومات الرقمي من موقع المكتبة على الشبكة مما يخوله لملكيته الكاملة، كما أن المكتبة تتيح أي عدد مهما بلغ من عمليات إنزال مصدر المعلومات الرقمي. ويخشى كثير من المهتمين بحماية حقوق النشر والملكية الفكرية في هذه الحالة من قيام هذا المستفيد أو غيره بأي عمل غير نظامي ربما ينتج عنه فقد معلومات المؤلف من مصدر المعلومات الرقمي، أو قد توضع بغير أسمه، كما أنه في بعض الأحيان ربما تظهر بيانات المؤلف صحيحة وسليمة ولكن قد يحدث تغيير في محتويات مصدر المعلومات الرقمي وذلك بإضافة أو حذف محتوياته بغير علم المؤلف ورغبته والتي ربما تؤدي إلى ظهور اسم المؤلف على مادة أو أفكار تختلف مع معتقداته وقناعاته

3- حق المؤلف في البيئة الرقمية:

أصحاب حق المؤلف يواجهون في البيئة الرقمية المتشابكة عدد كبير من الصعوبات والقضايا والمشكلات بسبب النشر في هذه البيئة الرقمية أو إتاحة مصنفاتهم عليها، والتي يرجع السبب في وجود غالبيتها إلى السهولة التي يمكن من خلالهااستنساخ المواد المنشورة الكترونياً على الانترنت وقلة التكاليف المالية التي تستلزم ذلك.

أما بالنسبة إلي قوانين حماية حق المؤلف فأنها عموما تعمل على حماية الكتب والكتيبات وغيرها من المواد المكتوبة، والمصنفات الأخرى كالخطب، والمواعظ، والمصنفات المسرحية، والمسرحيات الغنائية، والموسيقية والتمثيل الإيمائي، والمصنفات الموسيقية، والمصنفات السينمائية والإذاعية السمعية البصرية، وأعمال الرسم، والتصوير، والنحت، والحفر، والعمارة والفنون التطبيقية والزخرفية، والصور التوضيحية، والخرائط، والتصميمات والفنون التطبيقية الزخرفية، والخرائط السطحية للأرض، وبرامج الحاسب، وامتدت حسب اتفاقية تربس إلى البرمجيات، سواء كانت بلغة المصدر أو الآلة، إضافية إلى قواعد المعلومات وتحمى برامج الحاسب، وقواعد البيانات وفقا لحق المؤلف طيلة حياته ولمدة خمسين عاما بعد وفاته وتشمل الحماية، الحقوق المعنوية للمؤلف، والحقوق المالية لاستغلال المصنف، وهي حماية استئثارية للمؤلف يمنع من خلالها أي استعمال يضر بمصلحته، وتعطي الحق للمؤلف في استنتاج مصنفة واحدة واستغلالها وفقا لشروط تقترحها القوانين العربية. وتنص القوانين أيضا على إجازة استخدام المصنف دون إذن المؤلف، في معرض تقديم المصنف أو خلال اجتماع عائلي، أوفي مؤسسة تعليمية ثقافية، أو اجتماعية، أو لأغراض شخصية يعمل نسخة واحدة دون تعارض مع الاستغلال العادي، واستعماله في الإيضاح التعليمي والاستشهاد بفقرات منه في إنتاج آخر.

4- إجراءات وطرق الحماية الآلية والقانونية لحقوق المؤلف في بيئة الإنترنت (الرقمية):

قد أثرت التقنية الرقمية الحديثة على هوية وقيمة المعلومات، وأصبح من الممكن تكسير الحواجز الأمنية التي تحميها في شكلها الرقمي الجديد، ويمكن تلخيص عناصر أمن المعلومات في توفير العناصر التالية [6]:

- السرية أو الموثوقية: وهي تعني التأكد من أن المعلومات لا تُكشف ولا يطلع عليها من قبل أشخاص غير مخول لهم ذلك.
- التكاملية وسلامة المحتوى: وهي التأكد من أن المحتوى لم يتم العبث به، أي لم يدمر أي جزء من أجزائه في أي مرحلة عن طريق الدخول غير المشروع فيه من قبل العابثين الذين يقومون بالدخول للمحتوى وتدميره كلياً أو جزئياً.

هذا لا يعنى عدم وجود نتائج سلبية حيث يترتب نشر المصنفات على الإنترنت أن يواجه المؤلف صعوبات في حماية حقه، فالمشكلة الحقيقة تكمن في أن عصر تكنولوجيا المعلومات تعجز القوانين الوطنية عن تنظيم أو تجريم ما يحدث من أفعال الاعتداء على المصنفات عبر الشبكة، لأن تلك الأفعال لا تعرف حدوداً إقليمية إذ تتجاوز تلك الحدود، ونظراً لعجز القوانين الوطنية عن توفير الحماية، نجد قيام الأشخاص أنفسهم بابتداع طرق ألية خاصة لحماية مصنفاتهم، ويطلق عليها الحماية الخاصة، وتنقسم تلك الطرق، أو الوسائل التكنولوجية إلى نوعين:

النوع الأول: التدابير التكنولوجية:

وهي تهدف إلى إعاقة الحصول على المصنف والاستفادة منه إلا لمن يحمل ترخيصاً من صاحب الحق نفسه ومن تلك الأساليب والتقنيات التالي:

أولاً: معرف المواد الرقمية (DOI):

عبارة عن توفر الحماية من خلال رقم ثابت لكل مادة رقمية، وتحديد البيانات الميتاداتا، وبذلك فهو يعتمد على تطبيق كل من نظام handle system، ونظام الميتاداتا، وباستخدام هذا النظام يمكن الوصول إلى الوثائق المتاحة على الشبكة حتى في حالة تغير عنوان الموقع URL، وهو يمنح لكل وثيقة رقم يتكون من جزء ثابت يعبر عن DOIفي قسم منه وعن الناشر في القسم الأخر، وجزء آخر تقوم بإضافته لاحقاً الجهة القائمة بالتسجيل، كما يخصص النظام لكل وثيقة الميتاداتا الخاصة بها، والتي يتم فيها تحديد رقم DOI، وأي رقم محدد للوثيقة، والعنوان، والجهة ودورها سواء أكانت ناشر، منتج، مؤلف، والنوع (ملف رقمي، أو مادة ملموسة مادياً... الخ)، والشكل سواء كان نصي، سمعي، مرئي...

ثانياً: البصمة الإلكترونية (الرقمية)

وهي بصمة رقمية يتم اشتقاقها وفقا لخوارزميات معينة تُدعى دوال أواقتراناتالتموية، إذ تطبق هذه الخوارزميات حسابات رياضية على الرسالة لتوليد بصمة (سلسلة صغيرة) تمثل ملفاً كاملاً، أو رسالة (سلسلة كبيرة) وتدعى البيانات الناتجة عن البصمة الإلكترونية، وتستطيع هذه البصمة تمييز الرسالة الأصلية والتعرف عليها بدقة حتى إن حدث أي تغيير في الرسالة، ولا يمكن فك شفرتها إلا باستخدام مفتاح عام.

ثالثا: تشفير البيانات:

عبارة عن إدخال تعديلات على المعلومات عند إرسالها إلى جهة معينة، أو تحويلها إلى رموز غير ذات معنى؛ حيث عندما تصل إلى أشخاص آخرين لا يستطيعون فهمها أو الاستفادة منها.

النوع الثاني: المعلومات الضرورية لإدارة الحقوق:

وهو ما يعرف بالعلامات المائية الرقمية، وهي معلومات مشفرة يتم إلحاقها بالمادة في صورة رقمية، أو تعديلات أو تحويرات غير مرئية تقترن بالمادة تمكن صاحب الحق من التعرف على تلك المادة وتتبع النسخ غير المرخص بها، والمطالبة بإزالتها من جهاز الكمبيوتر الخادم.

نستخلص من ذلك ظهور وانتشار الإنترنت ظهرت معه قصور القوانين الخاصة بالحماية الفكرية خصوصاً المتاحة على الشبكة، مما يستلزم معه إدخال تعديلات على تلك القوانين للوصول إلى حلول لمواجهة هذا التقدم الهائل في مجال تكنولوجيا الاتصالات.

الفصل السادس

أخلاقيات القوانين والانترنت

ETHICS OF LAWS AND THE INTERNET

يعتبر الانترنت هو نجم التفاعل العالمي وهو النموذج المؤثر للعولمة التي تحدث من خلال الانترنت. وكلمة انترنت لم تكن معروفة قبل نشوء مسماها بل نشأت نتيجة لإدخال كلمة « Inter » التي تشير إلى العلاقة البينية بين شيئين، أو أكثر على كلمة Net التي تعني الشبكة لتعكس أن الانترنت هي شبكة واسعة تربط بين العديد من الشبكات المحدودة.وبدأت الانترنت مند أكثر من ثلاثين عاما، لأغراض عسكرية، سياسية، ثم تعليمه، من خلال شبكة NSFNET التي أنشأتها وكالة **"ناسا"** عبر المؤسسات التعليمية الأمريكية والمجهزة بـ 5 أجهزة حاسوب لتمتد عبر أنحاء العالم. وتنتشر الحواسب الرئيسية المزودة والمكونة للشبكة في الدول المتقدمة خاصة الولايات المتحدة الأمريكية، اليابان، كندا، ألمانيا، وايطاليا، بريطانيا، ايرلندا، واسبانيا، واستراليا، فرنسا، السويد، فنلدا، وسوزيلاند، بولندا، الدنمارك، البرتغال، فنزويلا، كوريا، الشيلي، تشيكوسلوفاكيا، تركيا، المكسيك، الأكوادور، كولومبيا، وإسرائيل. ومع تطور الشبكة بلغ عدد الحواسيب المزودة لخدمة الانترنت ألان 29 مليون جهاز حاسوب، كما بلغ عدد مستخدمي الانترنت في العالم حوالي 500 مليون مبحر، وتزايد بـ 150 مليون كل عام. في حين بلغ عدد مستخدمي الانترنت في العالم العربي حوالي 2 مليون فقط. بالنسبة لعدد المواقع فيزيد عن مليار موقع، 100 منها يزورها 80%من المستخدمين، و20% الباقية تتردد على باقي المواقع".

وإن النشأة الأمريكية للانترنت، وتحديدا في مؤسساتها العسكرية، جعلت من الشبكة أمريكية الطابع، حيث أكثر من 28.770 شبكة مكونة للانترنت تقع بالولايات المتحدة الأمريكية، تليها كندا بـ 4795 شبكة، ثم فرنسا 2003 شبكة. وتشير الإحصائيات إلى أن 80 %من مستخدمي الانترنت يعيشون بالولاية المتحدة الأمريكية. وهو ما جعل هذا البلد

يهيمن على شبكة الشبكات ديمغرافيا وثقافيا، بسيطرة اللغة الإنجليزية، إلى جانب استئثاره بصياغة المواصفات التقنية.

مميزات الانترنت:

الانترنت تحولت إلى ظاهرة اجتماعية عالمية متميزة، اختلفت فيها الآراء، وتناقصت بين مؤيد لإيجابياتها، ورافض لسلبياتها.

ايجابيات الانترنت:

الإنترنت يحمل العديد من الإيجابيات التي أثرت بشكل كبير على مختلف جوانب الحياة. إليك بعض من أهم الإيجابيات:

1. **الوصول إلى المعلومات:**
   - **الإنترنت يوفر كمية هائلة من المعلومات في مختلف المجالات، مما يجعل من السهل الحصول على المعرفة والتعلم عن أي موضوع بشكل سريع ومن أي مكان.**
2. **التواصل الاجتماعي والتواصل العالمي:**
   - **الإنترنت يتيح للأفراد التواصل مع الآخرين في جميع أنحاء العالم، سواء عبر البريد الإلكتروني أو وسائل التواصل الاجتماعي أو مكالمات الفيديو. هذا جعل العالم أكثر تواصلاً وسهولة في الحفاظ على العلاقات الشخصية والمهنية.**
3. **التعلم عبر الإنترنت والتعليم عن بُعد:**
   - **الإنترنت فتح الباب أمام التعلم الإلكتروني والتعليم عن بُعد، مما يتيح للطلاب الوصول إلى الدورات والمواد التعليمية من أي مكان في العالم.**
4. **التجارة الإلكترونية:**
   - **الإنترنت ساهم في نمو التجارة الإلكترونية، مما يتيح للأشخاص شراء وبيع المنتجات والخدمات عبر الإنترنت بسهولة وسرعة.**
5. **الترفيه:**
   - **يوفر الإنترنت مجموعة واسعة من خيارات الترفيه، من مشاهدة الأفلام والمسلسلات إلى الألعاب عبر الإنترنت والاستماع إلى الموسيقى.**
6. **البحث عن الوظائف والعمل عن بُعد:**
   - **أصبح من الممكن البحث عن الوظائف والتقدم لها عبر الإنترنت، بالإضافة إلى العمل عن بُعد من خلال منصات العمل الحر والشركات التي تتيح هذه الفرص.**
7. **التعاون والعمل الجماعي:**

- **الإنترنت يسهل التعاون بين الفرق والأفراد من خلال أدوات التعاون عبر الإنترنت مثل Google Docs وSlack، مما يسهل العمل الجماعي حتى عندما يكون الأعضاء في مواقع جغرافية مختلفة.**

8. **الخدمات الصحية عن بُعد:**

- **يتيح الإنترنت الوصول إلى خدمات الرعاية الصحية عبر الإنترنت، بما في ذلك الاستشارات الطبية عن بُعد، مما يسهل الحصول على الرعاية الصحية في المناطق النائية أو للأشخاص غير القادرين على التنقل.**

9. **الوعي والتعبئة الاجتماعية:**

- **الإنترنت يلعب دورًا كبيرًا في زيادة الوعي بالقضايا الاجتماعية والبيئية والسياسية، ويسمح بالتعبئة والحشد لدعم القضايا والمبادرات العالمية.**

10. **الحفاظ على البيئة:**

- **من خلال تقليل الحاجة إلى السفر والورق، يسهم الإنترنت في الحفاظ على الموارد الطبيعية وتقليل الأثر البيئي.**

سلبيات الانترنت:

على الرغم من الفوائد الكبيرة التي يقدمها الإنترنت، إلا أن له العديد من السلبيات التي يجب أخذها في الاعتبار. إليك بعض من أبرز السلبيات:

1. **الخصوصية والأمان**:

- الإنترنت يعرض الأفراد لخطر انتهاك الخصوصية، حيث يمكن أن تُجمع بياناتهم الشخصية وتستخدم لأغراض غير مشروعة. كما أن الهجمات السيبرانية والاختراقات تشكل تهديدًا كبيرًا لأمان المعلومات.

2. **الإدمان على الإنترنت**:

- الاستخدام المفرط للإنترنت، خاصة وسائل التواصل الاجتماعي والألعاب الإلكترونية، يمكن أن يؤدي إلى الإدمان، مما يؤثر سلبًا على الحياة الاجتماعية، والصحة النفسية، والإنتاجية.

3. **التعرض للمحتوى الضار**:

- يمكن أن يتعرض المستخدمون لمحتوى ضار أو غير مناسب مثل العنف، الكراهية، الإباحية، أو المعلومات المضللة. هذا يمكن أن يكون له تأثيرات سلبية خاصة على الأطفال والمراهقين.

4. **التنمر الإلكتروني**:

- الإنترنت يمكن أن يكون ساحة للتنمر الإلكتروني، حيث يتم استخدام منصات الإنترنت لمضايقة أو تهديد الآخرين، مما يؤدي إلى تأثيرات نفسية سلبية خطيرة.

5. **العزلة الاجتماعية**:

- قد يؤدي الاعتماد المفرط على الإنترنت للتواصل الاجتماعي إلى العزلة في الحياة الواقعية، حيث يفضل البعض التفاعل عبر الإنترنت على التفاعل وجهًا لوجه.

6. **انتشار الأخبار الكاذبة والمعلومات المضللة**:

- الإنترنت يساهم في انتشار الأخبار الكاذبة والمعلومات المضللة بسرعة كبيرة، مما يمكن أن يؤدي إلى خلق البلبلة والإضرار بالرأي العام.

7. **القرصنة والجرائم الإلكترونية**:

- الإنترنت يوفر بيئة خصبة للجرائم الإلكترونية مثل الاحتيال، سرقة الهوية، والقرصنة، مما قد يؤدي إلى خسائر مالية كبيرة وضياع للبيانات الشخصية.

8. **التأثير على الصحة النفسية**:

- الاستخدام المفرط للإنترنت، وخاصة وسائل التواصل الاجتماعي، يمكن أن يؤدي إلى مشاكل مثل الاكتئاب، القلق، والشعور بالعزلة.

9. **الاختراقات الأمنية**:

- الشركات والأفراد على حد سواء عرضة للاختراقات الأمنية التي يمكن أن تؤدي إلى فقدان البيانات الحساسة وسرقة المعلومات المالية.

10. **التأثير على الأطفال**:

- يمكن أن يؤثر الإنترنت سلبًا على الأطفال من خلال التعرض لمحتوى غير لائق، التنمر الإلكتروني، أو الإدمان على الألعاب الإلكترونية.

11. **الاحتيال والخداع**:

- يمكن أن يتعرض المستخدمون لعمليات احتيال وخداع عبر الإنترنت، مثل النصب عبر البريد الإلكتروني أو المواقع المزيفة، مما يؤدي إلى خسائر مالية كبيرة.

12. **الاستخدام غير المشروع**:

- الإنترنت يمكن أن يُستخدم لنشر المواد غير القانونية مثل المخدرات، الأسلحة، أو المواد الإباحية، مما يشكل تهديدًا على المجتمع والأمن.

تلك السلبيات تبرز أهمية استخدام الإنترنت بشكل واعٍ ومسؤول، واتخاذ التدابير اللازمة لحماية الخصوصية والأمان الشخصي، وكذلك توعية الأطفال والشباب حول الاستخدام الآمن للإنترنت.

المنظور العربي لظاهرة الانترنت:

إن التكنولوجيا نتاج ثقافي للمجتمع الذي أنتجها مما يجعل توطينها يتطلب تكيف ثقافيا من جانب المستهلك لإدماجها في البيئة المحلية.والتوسع في تطبيقات ثورة المعلومات في المجتمع العربي، يتطلب شروطا اجتماعية وثقافية أعمق من مجرد استيرادها.فالدول العربية أمام قائمة من المشاكل الاقتصادية، والاجتماعية والثقافية، تتطلب مهارات اللغة الكونية الجديدة، وتضيف مهارات ثورة المعلومات،وخاصة الانترنت في مواجهة مشاكلها، فظاهرة الانترنت تناقصت فيها التوجهات في الواقع العربي مابين :

- ديمقراطية أم مزيد من سيطرة الحكومات ؟
- ألفة جماعات الانترنت أم غربة عن الواقع ؟
- حوار حضارات أم صراع الحضارات ؟
- عمالة أكثر، أم بطالة أكثر ؟
- إبداع جديد أم اجترا ر للقديم؟

وأمام هذا التناقض فقد اختلفت التوجهات المحورية من المنظور الثقافي ألمعلوماتي لظاهرة الانترنت في الدول العربية، من حيث استعمال الانترنت، أين انحصر استعمال الشبكة

كفضاء للدردشة، أو البريد الالكتروني على حساب المعرفة و البحث العلمي، وقد قدرت إحصائيات استخدام الانترنت من قبل العرب كما يلي:

*71 % من المستخدمين يستعملونه في الاتصالات الهاتفية والبريد الالكتروني.
*64 % بحث عن المعلومات.
*42 % في التسلية والترفية.
*38 % في جلب برامج الألعاب.
*23 % العمل في التجارة.
* 18 % في الشراء والتسوق.

وبالنسبة لصناعة الثقافة والمتمثلة في عنصر المحتوى الذي يساهم بشكل كبير في الدخل القومي للبلدان، فيواجه العرب حصارا خانقا على موارد المحتوى بالانترنت حيث يعود احتكار التصنيع الثقافي للولايات المتحدة الأمريكية، خاصة أمام ظهور المحاولات العربية لإنتاج محتوى عربي جديد، إلى جانب قلة وندرة المواقع العربية، وضعف في صناعة البرمجيات، فضلا عن سلبية الرسالة الثقافية العربية عبر الانترنت، وقلة تشعبها.

ونتيجة للمعدل المشاريع لتضخيم حجم المعلومات، تزايد التوجه العالمي إلى الوسائل الاتوماتيكية للبحث والتحليل والتنظيم "كآليات البحث الفائق : التي تمزج بين البحث بمدخل الموضوع والبحث عن لفظ بعينيه. ومنظمات المعلومات الفائقة التي تقوم بفهرسة المعلومات وتبويبها وتخزينها، وروبوتات الأرشفة التي تقوم بأرشفة الشبكة". وأمام هدا الزحف الهائل من روبوتات المعرفة، تبقى الدول العربية معرضة للقرصنة من خلال توظيف تكنولوجيا الوكالة الآلية، إلى جانب كون الدول العربية سوق مستهدفة لمواقع الإباحية على الانترنت.

ومواقع الانترنت عامة، أصبحت تعج بالعديد من التعديات على العديد من الحقوق بالبيئة الرقمية، نتيجة اختلاف التوجهات وتعدد الثقافات، وانعدام الرقابة وهو ما أدى إلى ظهور الجرائم الفضائية.

آداب وأخلاقيات استخدام الإنترنت.

يُعدّ الإنترنت عالماً واسعاً يُستخدم في العديد من المجالات، ولا بد من مراعاة الآداب والأخلاقيات اللازمة أثناء استخدامه، لأن الإنترنت أصبح امتداداً للحياة التي يعيشها أفراد المجتمع على أرض الواقع، وتنطبق عليه جميع القوانين والأخلاقيات التي تُطبّق على أرض الواقع، وتقبّل الآخرين والتسامح معهم على اختلاف ثقافاتهم، وتتمثّل هذه الآداب في جوانب عديدة، فيما يأتي ذكر لبعض منها:

احترام خصوصية المعلومات

يجب الانتباه إلى عدم مشاركة المعلومات الشخصية على شبكة الإنترنت، وتجنب استخدام البيانات الشخصية والحسابات الخاصة أو رفع ملفات خاصة باستخدام شبكات الإنترنت العامة، وذلك لأن الشبكات العامة قد تحتفظ بالمعلومات والملفات حتى بعد الانتهاء من التصفح، وقد تتم مشاركتها مع أشخاص آخرين دون علم المستخدم، وعلى الصعيد الآخر يجب مراعاة خصوصية الآخرين وعدم الدخول إلى حساباتهم أو ملفاتهم الشخصية حتى لو ظهرت لدى المستخدم.

تعزيز الرقابة الذاتية

ينتشر المحتوى المسيء على الإنترنت كما ينتشر المحتوى الجيد، فقد يتعرض المستخدم لمواقع مسيئة أو محتوى سيئ، وللحدّ من تعرض المستخدم لهذا المحتوى هناك عدة طرق للتعامل مع الأمر: أن يكون رقيباً على ذاته ويتجنب هذا المحتوى فور التعرض له، أو أن يستخدم نظام حماية ما يحجب هذا المحتوى تلقائياً، ليجعل تصفح الإنترنت بالنسبة له أكثر سهولة وأقل إيذاء له، بالإضافة إلى تطبيقات حجب الإعلانات لتجنب الإعلانات المسيئة. تُعدّ الأجيال التي وُلدت بعد انتشار التكنولوجيا والإنترنت على دراية كبيرة بالتعامل معه تقنياً، لكن لا بدّ من وجود الرقابة والتوجيه من الآباء والأمهات للأطفال والقاصرين حتى لا يتعرضوا لمشاكل عبر الإنترنت، فيجب الانتباه إلى المحتوى الذي يشاهدونه بحيث لا يكون مسيئاً، ومعرفة اهتماماتهم والأمور التي يبحثون عنها عبر الإنترنت، وإرشادهم بألا يشاركوا معلوماتهم الشخصية، أو عنوان المنزل، أو صورهم الشخصية مع أحد لا يعرفونه عبر الإنترنت، فهذا قد يعرضهم للابتزاز أو التنمر، كما يجب الحذر من إدمانهم على الإنترنت، ومن الجدير بالذكر أنّ هذا ليس بهدف حدّ لحريتهم وإنما بهدف إرشادهم وحمايتهم للتعامل مع الإنترنت بشكل أفضل.

مراعاة آداب التواصل عبر الإنترنت

يمكن التواصل مع الآخرين عبر الإنترنت من خلال البريد الإلكتروني أو مواقع التواصل الاجتماعي، لكن لا بدّ من مراعاة مجموعة من الآداب، منها ما يأتي:

1. استخدام ألفاظ مهذبة ولطيفة أثناء التواصل وعدم استخدام لغة مسيئة.
2. مشاركة المعلومات المفيدة للآخرين وتجنُّب نشر أي محتوى مسيء لشخص، أو عرق، أو دين.
3. عدم إزعاج أشخاص لا يعرفهم المستخدم.
4. احترام اختلاف وجهات النظر.

مراعاة حقوق النشر

من المهم التعامل مع الآخرين عبر الإنترنت كما يتمّ التعامل معهم في الحياة على أرض الواقع، فلا بد من عرض شخصيتك بوضوح ومصداقية وعدم انتحال شخصية أحدهم أو استخدام شخصية مزيفة، وألاّ ينسب المستخدم أي عمل قام به أحد آخر إلى نفسه، سواء كان نصّاً، أو فيلماً، أو موسيقى، أو برمجية ما، فهذه تعدّ سرقة حتى لو كانت عبر الفضاء الإلكتروني.

الأخلاقيات في العمل والمؤسسات التعليمية

يجب أن يتحلى مستخدمو الإنترنت في العمل والمؤسسات التعليمية؛ كالمدارس والجامعات بالشعور بالمسؤولية، فالإنترنت يخدم العمل ويخدم العملية التعليمية، لكن استخدامه لأغراض أخرى غير متعلقة بالعمل أو الدراسة هو تصرف غير أخلاقي ولا يصبّ في مصلحة هذه المؤسسات، فقد يضيع الوقت المخصص للعمل بموجب عقد العمل أثناء تصفح مواقع أخرى ويسبب تشويش وإيقاف العمل، كما قد يضر استخدام الإنترنت في المدارس والجامعات بالأشخاص الذين يستفيدون حقاً منه لأغراضٍ تعليمية.

ضبط أخلاقيات الانترنت:

للمتاعب الأخلاقية السابق ذكرها، التي جلبها التطور الكبير في مجال انسياب المعلومات بشبكة الانترنت، فقد سعت العديد من الهيئات والمنظمات المختصة في المجال إلى فرض التشريعات، والقوانين لتنظيم الكم الهائل والمتدفق من المعلومات على شبكة الانترنت. فظهرت لهدا الغرض العديد من المصطلحات التي لا يزال الاختلاف في ضبط معناها قائم إلى الآن. ورغم اختلف التقنيات والممارسات على الشبكات والانترنت، فإن أشكال ضبط أخلاقيات الانترنت يبقى هدفها جعل الضمير الحي للمستعمل في عقد اجتماعي، لاستخدام الشبكة في صالح المجتمع، ومن أهم هاته الأشكال.

لوائح التنظيم الذاتي:

لا يوجد لهذا المصطلح شرح في قواميس اللغة، وتم اعتباره في القمة العالمية حول التشريع في مجتمع المعلوماتأوسع من مصطلح تقنين والدي يعني تقنين جملة من النصوص القانونية من

طرف المشرع، واتفق جميع المشاركون في هده القمة على أن مصطلح Auto-règlementation "يعني إنشاء واحترام إرادي للقواعد المتفق عليها في مجال معين، بدون إلزام أو رقابة". وهي ترجمة للمصطلح الإنجليزي Self régulation، ويشمل هدا المصطلح أخلاقيات المهنة، فضلا عن اعتبار لوائح التنظيم الذاتي ضمن أنظمة التنظيم والرقابة المستعملة لأمن الشبكة" إلى جانب كونها "عقد اجتماعي" بين جملة من الأشخاص يضمن الحفاظ على مسؤولية جميع الفاعلين على الشبكة لتحقيق امن الانترنت، وكسب ثقة المستهلك، وحماية المحتوى من التلوث والتخريب، وحماية البنية التحتية للشبكة، وحق الملكية الفكرية، وحق الخصوصية.

وقد ظهرت لوائح التنظيم الذاتي" Autorégulation، مع تحول شبكة الانترنت إلى إيديولوجيا ربط الثقافات واللغات، وإلغاء الحدود الزمنية، والمكانية وتحولها أيضا إلى "فضاءات بدون حق" رغم تعدد الحقوق التي تلزمها التشريعات القانونية. وتضم لوائح التنظيم الذاتي:Autorégulation :

* لوائح تنظيم المحتوى بشبكة الانترنت.
* لوائح تنظيم التقنيات بشبكة الانترنت.
* قواعد أخلاقية لمستعملي الانترنت.

***** لوائح تنظيم المحتوى بشبكة الانترنت: وتعني بتنظيم فحوى المواقع والمعلومات التي تنظمنها من أشكال التلوث الثقافي، والعرقي، والأخلاقي والدعاية للتعصب الديني، والعرقي من خلال رسائل المضايقات، ومنتديات النقاش عن بعد.

* لوائح تنظيم التقنيات بشبكة الانترنت: على اعتبار شبكة الانترنت بنية تحتية تقنية أولا، يتطلب حمايتها من كل من يخرب هذه البنية، خاصة من الكعكات "Cookies" التي تعد من مهددات الخصوصية على الانترنت، حيث تسمح هذه المعلومات بتسجيل خطوات البحث، والمواقع التي تمت زيارتها على القرص الصلب، لتكون الكعكات صفحة عن هوايات ومشتريات وخطوات المستخدم للشبكة. الأمر الذي يخرق الخصوصية على الانترنت، ويتطلب وضع تنظيم للتقنيات لتعديل سلوك المستعملين.

* القواعد الأخلاقية لمستعملي الانترنت: هي مجموعة قواعد ممارسة على الانترنت، وحسن سيرة لمستعملي الشبكة العالمية، يتم الاتفاق عليها، لضمان أمن الشبكة من الصراعات والتعديات. وتختلف هذه القواعد من بلد إلى آخر حسب المتغير الثقافي لكل منطقة.

لوائح التنظيم المساعد:

تجمع لوائح التنظيم المساعد بين القانون والأخلاق المهنية، والأخلاق"،وهي أوسع من لوائح التنظيم الذاتي، فضلا عن كونها مؤطرة بالقانون، باعتبارها تنظيم مساعد لتطبيق نصوصه،

وهو ما يجعلها ليست في مستهل الجمعيات والهيئات لوضع قواعدها، إذ تقوم الدولة بهذا الدور على عكس لوائح التنظيم الذاتي. وتعتبر الهيئة لافا (LAFA)، أن لوائح التنظيم المساعدة موضع نقد لاذع من طرف هيئات حماية حقوق الإنسان. وعموما ورغم اختلاف أشكال لوائح التنظيم الضابطة لأخلاق الأنترنت فالغرض منها واحد، هو حماية شبكة الانترنت من كل ما يهدد أمنها و يجعل منها نقمة. ويمكن تلخيص عملية التعامل الأخلاقي مع الانترنت في:

* طلب العلم النافع، والعمل على إيجاد وتنشئة المواطن الانترنت الصالح.
* تحري الصدق والموثوقية، والأمانة في طلب البيانات والمعلومات.
*معلومات الانترنت للبث، والنشر، والإتاحة، وليست للكتم أو الحبس.
* حماية حقوق الملكية الفكرية، وقوانين الفضاء الالكتروني.
* الانترنت وما تقدمه من بيانات ومعلومات للتغير إلى الأفضل في المجالات الاقتصادية والسياسية والاجتماعية.
* بيانات ومعلومات الانترنت من اجل التواصل والتعرف على الأصعدة الوطنية والإقليمية والعلمية.
* كفالة أمن البيانات والمعلومات، وسيرتها، ومراعاة الخصوصية واحترامها.
* اتخاذ التدابير الوقائية لحمية أفراد المجتمع وجماعاته من البيانات والمعلومات الضارة واللوثة.

وهو التعامل الأخلاقي الذي لابد أن تستجيب له الدول العربية، قبل غيرها حفاظًا على هويتها الثقافية، وأنساقها القيمة، لآن أخلاقيات الانترنت وأخلاقيات المعلومات تمثل بنية المعلومات وجوهرها، وتستمد مبادئها وقواعدها وضوابطها من التشريع الإلهي وعادات المجتمع، وتقاليده، وأعرافه خاصة تلك التي لا تتعارض مع التشريعات الإلهية إلى جانب دور التربية الحديثة التي تنمي الالتزام في جوهر الفرد.

آداب وأخلاقيات الإنترنت:

آداب الإنترنت، أو "إتيكيت الإنترنت"، تشير إلى مجموعة من السلوكيات والمعايير التي تهدف إلى استخدام الإنترنت بشكل محترم وآمن. تعكس هذه الآداب القيم الأخلاقية وتساعد في الحفاظ على بيئة إلكترونية صحية ومفيدة. إليك أهمية آداب الإنترنت في السياقات المختلفة:

1. تعزيز التواصل الفعّال

- وضوح الرسائل :آداب الإنترنت تساعد في كتابة رسائل واضحة ومباشرة، مما يقلل من سوء الفهم ويعزز التواصل الفعّال بين الأفراد.
- الاحترام المتبادل :تجنب استخدام اللغة المسيئة أو الهجومية يعزز من احترام الآخرين ويجعل النقاشات أكثر بناءة.

2. الحفاظ على السلامة والأمان

- حماية المعلومات الشخصية :تجنب مشاركة المعلومات الشخصية الحساسة يقلل من مخاطر الاحتيال والسرقة الإلكترونية.
- التحقق من المصادر :التحقق من مصداقية المعلومات قبل نشرها يساهم في تجنب نشر الأخبار الزائفة والمضللة.

3. تعزيز المسؤولية الأخلاقية

- احترام حقوق الملكية الفكرية :الالتزام بقوانين حقوق الطبع والنشر وعدم التعدي على ملكية الآخرين يعزز من احترام الإبداع والابتكار.
- الالتزام بالقوانين :اتباع قوانين الإنترنت المحلية والدولية يعزز من الاستخدام القانوني والمشروع للإنترنت.

4. حماية الصحة النفسية

- تجنب التعليقات السلبية :تجنب التعليقات الجارحة أو التنمر الإلكتروني يحمي الأفراد من التأثيرات النفسية السلبية ويعزز من بيئة الإنترنت الإيجابية.
- التعامل مع المحتوى بحذر :الوعي بتأثير المحتوى الذي يتم مشاركته أو استهلاكه يساعد في الحفاظ على الصحة النفسية.

5. تعزيز الثقة والمصداقية

- بناء سمعة إيجابية :التصرف بمهنية واحترام في التعاملات الإلكترونية يعزز من سمعة الفرد أو المؤسسة ويبني ثقة بين المستخدمين.
- الشفافية :تقديم المعلومات بشفافية وصدق يساعد في بناء علاقات موثوقة ويعزز من مصداقية المحتوى.

6. توفير بيئة تعاونية وآمنة

- تشجيع التعاون :التعامل بأدب واحترام يعزز من فرص التعاون والعمل الجماعي على الإنترنت، مما يؤدي إلى نتائج أفضل.
- إدارة النزاعات بفعالية :اتباع آداب الإنترنت يساعد في حل النزاعات بشكل سلمى وبناء، مما يقلل من التوترات والصراعات.

7. التعليم والتدريب

- تثقيف المستخدمين الجدد :تعليم آداب الإنترنت للمستخدمين الجدد، بما في ذلك الأطفال والمراهقين، يساعد في تطوير سلوكياتهم على الإنترنت بطريقة إيجابية.
- تدريب الموظفين :في بيئات العمل، يمكن أن يحسن تدريب الموظفين على آداب الإنترنت من التفاعل الداخلي والخارجي ويعزز من فعالية العمل الجماعي.

8. حماية الملكية الفكرية

- الاعتراف بالإبداع :احترام حقوق المؤلفين والمبدعين يعزز من تشجيع الإبداع والابتكار ويجنب الانتهاكات القانونية.
- الامتثال للمعايير :اتباع المعايير الأخلاقية في استخدام البرمجيات والمحتوى الرقمي يعزز من الحماية القانونية ويحمي الأصول الفكرية.

9. الامتثال للأخلاقيات المهنية

- التصرف بمهنية :الالتزام بآداب الإنترنت يساعد في الحفاظ على مستوى عالٍ من الأخلاق المهنية، خاصة في البيئات الأكاديمية والتجارية.
- الحفاظ على المعايير :يساهم في الالتزام بالمعايير الأخلاقية للمهنة والحفاظ على مستوى عالٍ من النزاهة والمصداقية.

باختصار، آداب الإنترنت تلعب دورًا حيويًا في ضمان استخدام الإنترنت بشكل محترم وآمن، وتعزز من الفعالية والتعاون والاحترام في بيئة الإنترنت.

الفصل السابع

حقوق المؤلف وحماية البرمجيات

COPYRIGHT PROTECTION FOR SOFTWARE

حقوق المؤلف

حقوق المؤلف هي مجموعة الحقوق الأدبية والمادية التي يتمتع بها أصحاب الحقوق عن استغلال مصنفاتهم الأدبية والفنية والعلمية،،وهي حقوق إستئثارية يتمتع بها صاحب المصنف المبتكر عن استغلال مصنفه أو الترخيص للغير في استغلاله، لا يحق لأي كان أن ينقل أو ينشر أو يستنسخ مصنفا لمؤلف في أي شكل أو صيغة أو طريقة فيها انتهاك للحقوق المادية والمعنوية للمؤلف.من المصنفات الأدبية والفنية والعلمية الكتب، الروايات، القصائد، المسرحيات، المصنفات الموسيقية والسينمائية والإذاعية، الرسوم المتحركة، أعمال التصوير والرسم والنحت والحفر، برامج الحاسوب، الخرائط والمخططات، والأعمال المجسمة.

المصنفات المحمية:

- الكتب والكتيبات وغيرها من المواد المكتوبة.
- المصنفات المسرحية والمسرحيات الغنائية والموسيقية والتمثيل الايمائى.
- المصنفات الموسيقية.
- المصنفات السينمائية والإذاعية السمعية والبصرية.
- أعمال الرسم والتصوير والنحت والحفر والعمارة والفنون التطبيقية والزخرفية.
- الصور التوضيحية والخرائط والتصميمات والمخططات والأعمال المجسمة المتعلقة بالجغرافيا والخرائط السطحية للأرض.
- برامج الحاسب وقواعد البيانات.

شروط إكتساب الحماية:

- مصنف أصلى مبتكر.
- مثبت فى وسط مادى ملموس.
- الايداع ليس شرطاً للحماية.

ما هي حقوق صاحب حق المؤلف:

- الحق فى أن ينسب إليه.
- الحق فى تقرير نشر مصنفه.
- الحق فى إجراء أىّ تعديل على مصنفه.
- الحق فى دفع أىّ اعتداء على مصنفه وفى منع أىّ تشويه أو تحريف أو أىّ تعديل آخر عليه أو أىّ مساس به.
- الحق فى سحب مصنفه من التداول.
- إستنساخ المصنف بأىّ طريقة أو شكل سواء كان بصورة مؤقتة أو دائمة بما فى ذلك التصوير الفوتوغرافي أو السينمائي أو التسجيل الرقمي الإلكتروني.
- ترجمة المصنف إلى لغة أخرى أو إقتباسه أو توزيعه موسيقياً أو إجراء أىّ تحوير عليه.
- التأجير التجارى للنسخة الاصلية من المصنف أو نسخة منه إلى الجمهور.
- توزيع المصنف أو نسخه عن طريق البيع أو أىّ تصرف أخر ناقل للملكية.
- إستيراد نسخ من المصنف بكميات تجارية.
- نقل المصنف إلى الجمهور عن طريق التلاوة أو الإلقاء أو العرض أو التمثيل أو النشر الإذاعى أو التلفزيونى أو السينمائى او أىّ وسيلة أخرى.

إستثناءات من الحماية:

لا تشمل الحماية المصنفات التالية، إلا اذا تميزت مجموعات هذه المصنفات بجهد شخصي ينطوي على الإبتكار أو الترتيب:

- القوانين والأنظمة والأحكام القضائية وقرارات الهيئات الإدارية والإتفاقيات الدولية وسائر الوثائق الرسمية والترجمات الرسمية لهذه المصنفات أو لأىّ جزء منها.
- الأنباء المنشورة أو المذاعة أو المبلغة بصورة علنية.
- الفلكلور الوطنى والمصنفات التى آلت إلى الملكية العامة.

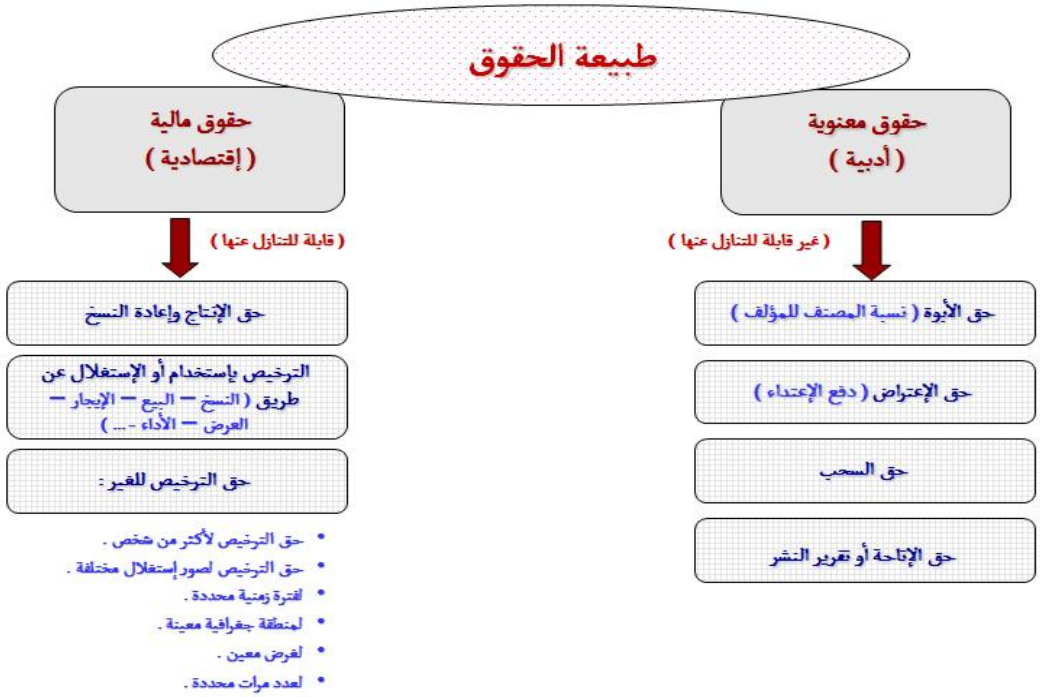
حماية الأفكار أم التعبير عن الأفكار ؟

حق المؤلف يحمي التعبير أو التجسيد المادي للفكرة وليس الفكرة في حد ذاتها... بمعنى أن حق المؤلف يحمي المصنف ذاته.

مدة الحماية : طوال حياة المؤلف + 50 سنة بعد وفاته.

50 عام من تاريخ النشر بالنسبة للأشخاص الإعتبارية.

الأعمال المحمية بقانون الملكية الفكرية تتمتع بالحماية فى مصر وكل دول العالم الأعضاء فى إتفاقية برن.



حقوق المؤلف في البيئه الرقمية

شبكة الانترنت عند تعريفها فهي مجموع شبكات مرتبطة فيما بينها والشبكة اصلا تكون مجموعة حواسيب اذن فالوحدة الاساسية في شبكة الانترنت هي الحاسوب وكما هو معلوم فالحاسوب يتكون من جزء مادي وجزء غير ملموس فالجزء غير الملموس منه كالبرامج والبرمجيات والتي تعتبر الفكر المحرك لجسم الحاسوب كما انه يتكون من اجزاء صغيرة جدا تساهم في عمله وتغذيته تعرف بالدوائر المتكاملة وكل هذه العناصر يطلق عليها اسم مصنف فما المقصود بالمصنف الرقمي ؟ وما هي انواعه على شبكة الانترنت؟.

أنواع المصنفات الرقمية المحمية بحق المؤلف

توجد على الشبكة العالمية العديد من المصنفات الرقمية المختلفة غير انه سنحصر هذه المصنفات في الاصناف الرقمية التي يحميها القانون بموجب حقوق المؤلف، ونشير انه هناك مصنفات محمية بموجب قوانين الملكية الصناعية والتجارية وهذه المصنفات لا منا في بحثنا هذا واجمالا المصنفات المعنية بالحماية هي : برامج الحاسوب، البرمجيات، قواعد البيانات، والدوائر المتكاملة، بالاضافة إلى الملفات الرقمية لمصادر المعلومات التقليدية من الكتب الرقمية والدوريات والموسوعات وغيرها المتاحة عبر الشبكة في شكل رقمي حديث.

برمجيات وبرامج الحاسوب

"تعد اول واهم المصنفات المعلوماتية التي يجب توفير الحماية القانونية لها هي البرمجيات، فهي الكيان المعنوي لنظام الكمبيوتر،كما انها تضم برمجيات التشغيل التى

تعمل مع مكونات النظام معا وتوفير بيئة عمل و البرمجيات التطبيقية" (اذن فبرامج الحاسوب هي أحد هذه المصنفات الرقمية التي تحميها القوانين الدولية والوطنية بموجب قانون حقوق المؤلف، ففي البدايةكان هناك اختلاف في طبيعة القانون الذي يحمي هذا الصنف من الاعمال الرقمية فغلبت الكفة القائلة اا تحمي بموجب حقوق المؤلف وهناك دول مازالت تحميها بموجب قانون الملكية الصناعية وتحديدا براءات الاختراع .فبرامج الحاسب الالي هي عبارة عن: "تعليمات مثبتة على دعامة يمكن قرائتها لاداء واجب معين عن طريق نظام معالجة هذه المعلومات وقرائتها بواسطة الحاسب الالي فالحاسب الالي لوحده لا يمكن ان يؤدي الغرض المرجو منه ولا بد من وجود برامج تحركه "(اما فيما يخص برمجيات الحاسوب" software computer" فهو اصطلاح اعم واشمل من " برنامج كمبيوتر" program computer " " فالبرمجية يمكن ان تحمل في حزمتها العديد من البرامج وتعرف في الاسواق باسم حزم البرامج package software ولا يمكن فصلها عن بعضها واعادة تثبيت كل برنامج على حدى على حاسوب اخر ومثال هذه الحزم الحزمة المشهورة "0.7" office microsoft التي تضم برنامجا للطباعة microsoft power pointوالطباعة للرسومات وبرنامجا microsoft excel 7.0 " للمحاسبة وبرنامجا7.0" .microsoft"word 7.0 "

الاعتداءات الواقعة على حقوق المؤلف على شبكة الانترنت

إن **ما** تتميز به شبكة الانترنت من عالميتها وسهولة بث واسترجاع المعلومات عليها سهل ذلك وقوع اعتداءات على حقوق المؤلفين في هذه البيئة الرقمية الافتراضية حتى في بعض القوانين لاتصنف اعتداءا بل جريمة

1- **مفهوم الاعتداء على حقوق المؤلف**: الاعتداء هو تجاوز الحدود المسموح بها كما انتهاك شيء محمي قانونا او الاستعمال بدون وجه حق لشيء ما دون استاذان صاحبه او مالكه. والاعتداء على حقوق المؤلف هي الاستغلال او الاستعمال غير المشروع لحق من حقوق المؤلف المنصوص عليها دون اذن من صاحبها أي المؤلف أو من آلت إليه الملكية.

2- **أنواع التعديات الواقعة على حق المؤلف**: رغم ان حقوق المؤلف هي احد اقسام الملكية الفكريه ويحميها قانون الملكية الفكرية الادبية والفنية غير انه من جانب التجريم والعقوبات والحماية الجنائية فيحميها قانون العقوبات وفي كثير من الدول فلاتبرأ من الجرائم الواقعة على الاموال لان نتاج المؤلف اي المصنف هو مال منقول لذا تطبق عليه هذه القوانين وعموما اهم هذه الاعتداءات هي الاعتداء على حق من حقوق المؤلف

الادبية او المالية او على اصحاب الحقوق كمنع المؤلف مثلا من نشر مصنفه او نسبته الى غير مؤلفه الحقيقي، او القيام بتعديل وتشويه او تحريف يؤدي بالاضرار بحقوق المؤلف المادية وهز وزعزعة مكانته في المجتمع، وكل هذه الاعتداءات تقع في غياب اذن او ترخيص من المؤلف للمعتدى ويشترط في هذا الاذن او الترخيص ان يكون مكتوب يمكن ان يقوم المعتدي بنشر المؤلف على شبكة الانترنت دون ان يستاذن مؤلفه، وكم هي كثيرة هذه الحوادث خاصة في عصرنا الرقمي هذا فهناك من رقمن كتبا ومؤلفات كثيرة وصنع منها مكتبة رقمية على شبكة الانترنت دون استئذان من اصحابها. كما انه يمكن ان تباع او تاجر مصنفات محمية ويعتبرهذا ايضا اعتداء على حقوق المؤلف.

التصنيع او الاستيراد دون وجه حق لغرض البيع او التاجير او التداول لاي مصنف او نسخ مقلدة او لاى اجهزة او وسائل او ادوات مصممة للتحايل على الحماية التقنية لهذه المصنفات : ويتحقق بتغيير المعطيات الموجودة داخل النظام واستبدالها بمعطيات اخرى بالاضافة الى التعطيل او التعييب دون وجه حق لاي حماية تقنية او معلومات الكترونية تستهدف تنظيم وادارة الحقوق المقررة في بعض القوانين تحميل او تخزين على الحاسب باية نسخة من برامج الحاسب وتطبيقاته او قواعد البيانات دون ترخيص من المؤلف او صاحب الحقوق اوخلفهما.لقد اتعبت هذه الجرائم منتجي المعلومات وكذا التقنيين وكذلك القضاة لكنلم يقف اصحاب هذه الحقوق بمساندة الدولة مكتوفي الايدي بل وجدو حلا تتكاثف فيه جهودكل الاطراف لحماية هذه الحقوق وهي مايعرف بالادارة الجماعية لحقوق المؤلف والحقوق المجاورة.

الطبيعة القانونية لبرامج الحاسب:

على الرغم من إجماع الفقه على أن برامج الحاسب تعد عملاً ذهنياً في المقام الأول، إلا أنه قد انقسم إلى اتجاهين رئيسيين في تحديد الفرع القانوني من فروع الملكية الفكرية الذي يتم حماية هذه البرامج بقواعده، فهناك من يرى بأن ذلك الفرع القانوني هو قانون براءة الاختراع، وهناك من يرى أن حماية البرامج تدخل في نطاق قانون حقوق المؤلف.

أولآ : حماية برامج الحاسب بقانون براءة الاختراع:

ذهب بعض الفقه إلى القول بأن برامج الحاسب تعد من قبيل المبتكرات التي يتمتع صاحبها بحق ملكية الاختراع. وهذا يعني أنه متى توافرت الشروط القانونية الواجب توافرها في الاختراع في هذا البرنامج منح صاحب البرنامج براءة اختراع وبالتالي يكون له حق استئثاري على البرنامج.

على ذلك نتناول الشروط الواجب توافرها لمنح براءة الاختراع، و ماهية الحق الاستئثاري الذي تخوله براءة الاختراع لصاحبها، ومدى تطابق ذلك مع طبيعة برامج الحاسب. وفق ما يلي:

شروط منح البراءة:

تستلزم قوانين براءة الاختراع لمنح براءة الاختراع توافر شروط أربعة وهي:

- وجود الابتكار.
- وجود الجدة.
- قابلية الاختراع للاستغلال الصناعى.
- أن لا يكون ممنوعاً.

الشرط الأول: أن يكون هناك ابتكار

لمنح المخترع براءة اختراع يجب أن يكون العمل الذي قام به متضمناً فكرة أصلية مستنداً إلى نظرية علمية، أي إيجاد شيء لم يكن موجوداً من قبل، أما إذا كان ما قام به طالب البراءة هو عبارة عن تحسين لشيء موجود من قبل بالاقتباس منه أو بالإضافة إليه، فإن ذلك لا يعد اختراعاً بل من قبيل التحسينات التي لا ترقى إلى مستوى الفكرة الابتكارية، وبالتالي لا تصلح أن تكون موضوعاً لبراءة الاختراع، فالمراد في وجود الابتكار الذي يصلح لمنح صاحبه براءة اختراع هو وجود التفنن وإنشاء أو إبتكار الجديد.

إن طبيعة البرامج تتنافى مع شرط الابتكار، كون البرامج أنواع شتى منها البرامج الأصلية ومنها البرامج المجمعة ومنها البرامج المؤلفة ومنها البرامج المفسرة والشارحة.... الخ وبالتالي فإن غالبية البرامج لم تأت بوضع شيء لم يكن موجوداً من قبل، بل إنها إضافات أو تعديلات أو اقتباسات لبرامج أخرى أو مستندة في الأساس على برامج قائمة وإذا تم حماية البرامج بقانون حق براءة الاختراع فهذا يعني أن غالبية البرامج ستكون دون حماية لعدم توافر شرط الابتكار فيها، ولهذا فإن قانون براءة الاختراع ليس القانون الذي يمكن أن يوفر الحماية القانونية لأصحاب برامج الحاسب.

الشرط الثاني: أن يكون الابتكار جديداً

يستلزم في الابتكار أن يتوافر فيه عنصر الجدة، ويقصد بالجدة ألا يكون أحد قد سبق المخترع في التعريف بالاختراع أو بمعنى آخر عدم علم الغير بسر الاختراع قبل طلب البراءة عنه، فإذا شاع سره بعد وضعه وقبل طلب البراءة فلا يمكن منح البراءة لعدم توفر الجدة.

اختلفت التشريعات العربية بشأن الجدة فبعض التشريعات استلزمت الجدة المطلقة، أي أن لا يكون الاختراع معروفاً خلال العصور السابقة، أما البعض الآخر من التشريعات، فتطلبت الجدة النسبية من حيث الزمان، أي أن لا يكون الاختراع معروفاً خلال الخمسين سنة السابقة.

أما من حيث المكان فلقد استلزمت غالبية التشريعات الجدة المطلقة، أي أن لا يكون الاختراع معروفاً داخل البلاد وخارجها.

عملية فحص عنصر الجدة في برامج الحاسب يعتبر من الصعوبات العملية، ومرجع ذلك هو التطور الكبير في مجال البرامج إلى درجة تكون معها التفرقة بين ما هو موجود فعلاً وما هو جديد أمراً عسيراً، فإذا كانت الاختراعات العادية قد تصل المدة التي يستغرقها فحصها والتأكد من مدى توافر عنصر الجدة والابتكار أكثر من ست سنوات لمراجعة كل الوثائق المتعلقة بالاختراعات المماثلة، فكيف يمكن تصور هذا الأمر بالنسبة لبرامج الحاسب المتسمة بالتطور السريع، وحتماً ستكون أمام شبه استحالة في مجاراة هذا التطور، الأمر الذي يترتب عليه استحالة الوصول إلى حقيقة توافر عنصر الجدة من عدمه.

الشرط الثالث: قابلية الاختراع للاستغلال الصناعي

يتوجب حتى يكون الابتكار الجديد اختراعاً أن يتوافر فيه الصفة الصناعية للاختراع، فلا يمكن منح براءة اختراع عن مجرد ابتكار الآراء النظرية، كون هذه الآراء النظرية المجردة لا تؤدي إلى نتائج ملموسة صناعياً، أما إذا تضمن طلب الحصول على البراءة تطبيقاً صناعياً لتلك الأفكار النظرية، في هذه الحالة يمنح صاحب الطلب براءة اختراع على التطبيق الصناعي وليس على الفكرة النظرية ذاتها.

وأن هذا الشرط هو الآخر نادر توافره في برامج الحاسب وهذا ما أكده إحصاء المنظمة العلمية للملكية الفكرية (WIPO) حيث أشار هذا الإحصاء إلى أن واحد في المائة فقط من برامج الحاسب يمكن أن ينطبق عليها شرط الاستغلال الصناعي.

حق الاستئثار في البراءة

لصاحب البراءة حق استئثار على البراءة الممنوحة له فتكون له الأولوية في استغلالها صناعياً، كما يكون له حق استغلالها بطريق غير مباشر وذلك بالتنازل عنها للغير أو بالترخيص باستغلالها، فالعقود الواردة على البراءة وفقاً للقائلين بخضوع البرامج لقانون براءة الاختراع، بوصفها محلاً لحق استئثار تسمح بنقل هذا الحق أو بعض السلطات التي يخولها لصاحبه من خلال عقود التنازل أو الترخيص بالاستغلال وبالتالي قيام خبير البرامج بنقل كافة السلطات التي يخولها له حق ملكية الاختراع إلى متلقي البرنامج، وهذا يعني تنازله منذ لحظة التعاقد عن كافة حقوقه في استغلال البرنامج، وفي الوقت نفسه، وفقاً لما يقتضيه الترخيص أو التنازل في مجال البراءة – فإن المتنازل إليه أو المرخص له يلتزم باستغلال البراءة وهذا الأمر يختلف عما جرى عليه في مجال التعاقد على برامج الحاسب، حيث لا يلتزم العميل باستغلال البرامج بل باستعمالها.

ومما تقدم أن طبيعة حق الاستئثار لصاحب البرنامج تختلف عنه بحق الاختراع وأن هذا الاختلاف إضافة إلى عدم توافر شروط الابتكاروالجدة والقابلية للاستغلال الصناعي يقف

حائلاً بين البرامج وبين القول بحمايتها بتشريع براءة الاختراع. ولهذا ليس بالغريب عدم تجاوب المشرع مع أنصار هذا الرأي واستبعاد غالبية التشريعات الحديثة حماية برامج الحاسب بقانون براءة الاختراع بل إخضاعها للحماية المقررة للمصنفات الأدبية والفنية وفقاً لقانون حقوق المؤلف.

حماية برامج الحاسب بقانون حقوق المؤلف:

يرى أغلب الفقهاء أن برامج الحاسب من المبتكرات الذهنية التي يتم حمايتها عن طريق تشريعات حقوق المؤلف، كون الحماية عبر هذه التشريعات لا تعترضها أية عقبات قانونية، بخلاف الحماية عن طريق قانون براءة الاختراع.

وقد أيدت غالبية التشريعات هذا الرأي منها، الأمريكي والياباني والإنجليزي والفرنسي والإيطالي والألماني والكندي والهندي والمصري في المادة 2 من القانون رقم 38 لسنة 92م والمعدل بالقانون رقم 29 لسنة 1994م، والأردني في المادة 8/3 من قانون حماية المؤلف رقم 22 لسنة 1992م، والتونسي في المادة 1 من قانون الملكية الأدبية والفنية رقم 36 لسنة 1994م، والسعودي في المادة 10/3 من نظام حماية حقوق المؤلف، والقطري في المادة 10/2 من قانون حماية المصنفات الفكرية وحقوق المؤلف، رقم 25 لسنة 1995م، البحريني في المادة 2/ي من قانون حماية حقوق المؤلف رقم 10 لسنة 1993م.

ويعتبر القانون البحريني لسنة 1993م بشأن حماية حقوق المؤلف القانون العربي الوحيد الذي وضع تعريفاً لبرامج الحاسب في المادة 2/ي والتي عرفت البرامج بأنها (**مجموعة العبارات والتعليمات المعبر عنها بأية لغة، أو رمز، أو إشارة والمعدة للاستعمال في الحاسب الآلي بطريق مباشر، أو غير مباشر، بهدف التوصل إلى نتائج محددة**).

لم تتناول غالبية التشريعات تعريفاً محدداً لبرامج الحاسب، بهدف تجنب التدخل المباشر في وضع عملية تكنولوجية يصعب السيطرة على مصطلحاتها ومضمونها في نصوص تشريعية محددة، إضافة إلى أن هذه البرامج في تطور مستمر يستعصى معه وضع تعريف جامع لها، كما أن هذا التطور يجعل من التعريف المحدد لبرامج الحاسب قيداً على استيعاب التطورات الفنية المتلاحقة في ميدان برامج الحاسب، حيث سيجعل البرامج غير المعروفة وقت وضع النص التشريعي الخاص بالتعريف بعيداً عن الحماية القانونية نظراً لعدم تطابق المعايير الواردة في التعريف عليها. ولهذا ترك المشرع في غالبية البلدان أمر تحديد المقصود ببرامج الحاسب المحمية قانوناً للقضاء، الذي يقدره على ضوء المعطيات الفنية وقت رفع الدعوى.

إن تبني غالبية الفقه والتشريع فكرة حماية برامج الحاسب عن طريق تشريعات حقوق المؤلف نظراً لأن هذه البرامج هي نتاج لتفكير أصحابها وبالتالي تعتبر من المصنفات الأدبية

التي يقرر لها القانون الحماية بموجب تشريعات حقوق المؤلف، فالطبيعة الابتكارية لهذه البرامج تتفق مع الطبيعة الابتكارية التي تطلبها قوانين حماية حقوق المؤلف في المصنفات الأدبية و العلمية.

ويقصد بالابتكار الذي تقوم عليه حماية قانون حقوق المؤلف للمصنف، ذلك المجهود الذهني الذي يبذله المؤلف، والذي يسفر عن خلق فكرة تتميز بطابع شخصي خاص، تبدو فيه بصمة شخصيته واضحة عن المصنف سواء تمثل ذلك المجهود في موضوع المصنف أو في أسلوب عرض الفكرة التي انطوى عليها ذلك المصنف أو في الطريقة التي عالج بها الموضوع ترتيباً وتنظيماً، فلا تمتد الحماية للفكرة المجردة بذاتها وإنما لوسيلة التعبير عنها فلا احتكار للفكرة، والتعبير المقصود هنا هو الإخراج المادي الذي تتجسم فيه الفكرة وتبرز إلى حيز الوجود الخارجي كأمر ملموس يدرك بالحواس أي أن تكون شخصية المؤلف واضحة على المصنف، إما من خلال طريقة العرض أو بما قام به من تحليل.

إن الطابع الابتكاري في برنامج الحاسب يكمن في الأسلوب المميز الذي يعالج به خبير البرمجة المشكلة المطروحة أمامه، وفي الاختيار والمزج للعناصر المكونة للبرنامج وأن هذا الأسلوب المتميز يعد ثمرة جهد فكري شخصي لخبير البرمجة وينفرد به، فالخبير كالمترجم لأن كليهما يختار بين عدة وسائل مختلفة للتعبير عن فكرة وهذا الاختيار هو الذي تتجسد فيه شخصية خبير البرمجة إزاء برنامجه ولا يقف التشابه بين دور خبير البرمجة والمترجم عند اختيار الأسلوب والصياغة بل يمتد ليشمل الحكم القانوني أيضاً، فالخبير شأنه شأن المترجم لا تمتد إليه الحماية القانونية إلا إذا قدم ما يدل على وجود حد أدنى من الابتكار في عمله، كما إن عنصر الابتكار للبرنامج، كما هو عليه الحال في المصنفات الأدبية والفنية، قد يوجد في مرحلة إعداد خريطة تدفق المعلومات أو في إحدى عناصر البرنامج اللاحقة لها، أو في عملية الصياغة النهائية.

وخلاصة القول أن تشريعات حقوق المؤلف هي المظلة الواقية لحماية برامج الحاسب لتشابه الطبيعة الخاصة لبرامج الحاسب مع شروط الابتكار الذي تتطلبه هذه التشريعات وبالتالي فإن الصعوبات التي تكتنف الحماية بتشريعات براءة الاختراع والمتمثلة في عدم توافر شروط منح براءة الاختراع على النحو السابق ذكره، فإنها لا وجود لها في تشريعات حقوق المؤلف، وإن انتفاء هذه الصعوبات يجعل من هذه التشريعات محققة لمصالح خبراء البرمجة بشكل كبير مقارنة بتشريعات براءة الاختراع.

مضمون حقوق مؤلف برنامج الحاسب

حيث أن الطبيعة الخاصة لبرامج الحاسب تتفق مع طبيعة الابتكار الذي يتطلبه قانون حقوق المؤلف وبالتالي فإن الحماية الممثلة لهذه البرامج لا يمكن تحقيقها إلا بقانون حقوق المؤلف، وبمقتضى ذلك يكون خبير البرمجة مؤلفاً، ويتمتع بالحقوق التي يمنحها قانون حقوق المؤلف والتي تنقسم إلى حقوق أدبية (معنوية) وحقوق مالية (مادية).

الحق الأدبي لمؤلف برنامج الحاسب :

ترجع أهمية الحق الأدبي لمؤلفه لما يكابده المؤلف في إعداد مصنفه حتى يخرج إلى الناس فكرة إبداعية تسهل استيعابها والاستفادة منها، ولهذا فإن الحق الأدبي هو أساس حماية الشخصية الفكرية للمؤلف نظراً لارتباطه الوثيق بالمؤلف، لذا فإن الحق الأدبي للمؤلف يعرف بأنه مجموعة الامتيازات التي يمنحها القانون للمؤلف والتي لا تقوم بالمال لأنها ترتبط بشخصيته وحرية تفكير وهذه الامتيازات تخول للمؤلف الصلاحيات الكاملة على مصنفه، باعتباره نابعاً منه، وانعكاس لشخصيته، وهذه الامتيازات قاصر على المؤلف، ومانعة للغير، فلا يجوز للغير ممارستها، وهذه الامتيازات القاصرة على المؤلف دعمت بضمانات كافية حيث تعتبر غير قابلة للحجز عليها ولا يسقط حق المطالبة بها أو بحمايتها بالتقادم وإنها حقوق مطلقة في مواجهة الكافة من الأشخاص.

إن المميزات التي منحها القانون للمؤلف والتي تشكل في مجموعها مضمون الحق الأدبي لمؤلف البرامج هي الحق في تقرير النشر والحق في نسبة المصنف إليه، والحق في الاحترام والحق في السحب.

مؤلف برنامج الحاسب له الحق في تقرير نشر برنامجه، ويتمثل هذا الحق في مصلحة مؤلف البرنامج بالاحتفاظ بحق التحكم في نشر برنامجه، ومن المتعارف عليه في المصنفات بوجه عام، أن المصنف يظل من الأسرار الخاصة بالمؤلف إلى أن يختار إفشاء هذا السر، وكذلك فإن الفقه والتشريع يجمعان على أن حق تقرير النشر يتمتع به المؤلف وحده وذلك عندما يقرر إخراج فكرته وابتكاره من أعماق شخصيته إلى عالم الوجود، لأن الأمر هنا يتعلق بالسمعة العلمية أو الأدبية أو الفنية للمؤلف، وحتى قرر صلاحية عمله الإبداعي للنشر فله أن يحدد الوقت المناسب للنشر، كما له أن يختار طريقة النشر التي يراها مناسبة، كما يتمتع مؤلف البرنامج بحق نسبة برنامجه إليه، أي التصريح بأن البرنامج هو نتاج جهده الذهني، ويكون هذا التصريح إما بنشر البرنامج حاملاً اسم مؤلفه من الوهلة الأولى للنشر، وأما بعد نشر البرنامج بفترة من الزمن كما لو نشر البرنامج باسم مستعار أو باسم رمزي، وبعدها يقوم بالتصحيح بالإعلان عن الاسم الحقيقي.

والبرنامج كغيره من المصنفات المحمية بقانون حقوق المؤلف يمكن أن يوضعه شخص طبيعي ولكن بتمويل وإشراف من شخص آخر طبيعي كان أم اعتباري، وهذه الحالة كثيرة الانتشار في الواقع العملي، حيث أن إنتاج البرامج في الغالب يتم عبر شركات البرامج التي تستخدم شخص أو عدة أشخاص بغرض وضع البرامج، ويثور التساؤل حول الشخص

الذي يتمتع بحق تقرير النشر وحق نسبة البرنامج إليه هل المؤلف أو الممول، ونستبين ذلك فيما يلى:

(1) ذهب البعض إلى القول بأنه يمكن تكييف البرنامج بأنه مصنف جماعي، فالوضع الغالب هو تعود المشتركين في إعداد وعمل البرنامج تحت إدارة وإشراف شخص آخر طبيعي أو اعتباري، بغرض تحقيق هدف محدد.

(2) ذهب البعض الآخر بأن يتمتع مؤلف البرنامج بحق أدبي في احترام برنامجه وعدم المساس به والاعتداء عليه حتى لا يتم إلحاق الضرر بالمؤلف أو الإساءة إلى مكانته الشخصية أو الأدبية أو العلمية في المجتمع، فأوصت تشريعات حقوق المؤلف إجراء أي تعديل في المصنف بالحذف أو بالإضافة دون موافقة المؤلف سواء في نفس المصنف أو تسميته ويشمل ذلك المقدمات والشروحات والخواتم والتعليقات. كما لا يجوز للغير أن يقوم بترجمة المصنف دون موافقة المؤلف. وأي فعل من ذلك يعد اعتداء على الحق الأدبي للمؤلف في احترام مصنفه يكون له دفع هذا الاعتداء إذا كان من شأن هذا الاعتداء المساس بسمعة المؤلف وشرفه.

يتمتع مؤلف برنامج الحاسب بحق سحب برنامجه من التداول وهو حق معترف به للمؤلف متى ظهرت أسباب قوية تدفع المؤلف إلى ضرورة سحب مصنفه من التداول إذا كان بقاء هذا المصنف سوف يؤدي إلى الإساءة إلى سمعته الأدبية أو الشخصية لمؤلفه، وأنه يتوجب في هذه الحالة إلزام المؤلف بدفع تعويض عادل لمن آلت إليه حقوق الاستغلال المالي للمصنف.

الحق المالي لمؤلف البرنامج:

لمؤلف البرنامج علاوة على حقه الأدبي، على النحو السابق، حق مالي يتمثل فيما له من سلطة الاستئثار باستغلال هذا البرنامج بما يعود عليه من ربح مالي مقابل لجهده الذهني. فالحق المالي لمؤلف البرنامج من الحقوق الاستئثارية، وهذا يعني أنه وحده هو الذي يملك الترخيص بكل استخدام للبرنامج، ولا يجوز لغيره استعمال البرنامج إلا بعد الحصول على موافقة مؤلفه. ويكون للمؤلف عموماً الحق في استغلال مصنفه عن طريق نقله للجمهور سواء كان ذلك بصورة مباشرة أو بصورة غير مباشرة. وحددت الطرق التي يمكن من خلالها استغلال الحق المالي للمؤلف، هي طبع (نسخ) المصنف والأداء العلني للمصنف، وطرحه للتداول ونقل المصنف إلى لغة أو لغات أخرى.

طبع (نسخ) البرنامج:

يمكن لمؤلف البرنامج القيام بنقل برنامجه إلى الجمهور بصورة غير مباشرة عن طريق صنع نسخ منه. ومتى قام المؤلف بنسخ برنامجه، فهذا يعني أنه حدد اللحظة المناسبة لنشر

برنامجه والكشف فيها عنه، ولذلك يرتبط الحق الأدبي للمؤلف في تقرير نشر مؤلفه بحقه المالي في النسخ كون النسخ هو وسيلة الكشف عن البرنامج، ويكون نسخ البرامج في أية دعامة كالأقراص الجامدة أوالمرنةأو أشرطة الكاسيت وبالعدد الذي يريده المؤلف، بمقابل أو بدون مقابل ولا يجوز لغيره من الأشخاص القيام بنسخ البرنامج دون موافقته، سواء كان هذا النسخ كلياً للبرنامج أو جزئياً ولا يقتصر النسخ المحرم قانوناً على البرنامج وحده بل يمتد إلى المستندات الوصفية له باعتبارها تدخل في مفهوم البرنامج المحمي قانوناً، تطبيقاً لقواعد حماية المؤلف بوجه عام.

الأداء العلني:

يكون نقل المصنف إلى الجمهور بصورة مباشرة عن طريق الأداء العلني وذلك بقيام المؤلف بعرضه مباشرة على الجمهور، إذا كان المصنف من المصنفات التي يمكن عرضها لبرامج الحاسب فإنه لا يتصور عرضها على الجمهور بشكل علني إذ لا توجد فائدة أو قيمة تعود على الجمهور أو من يتصور شراء حق الأداء العلني من مجرد اطلاع الغير على محتوى البرنامج، فالهدف من تصميم وإنتاج البرامج ليس عرضها على الجمهور، وإنما استخدامها لتحقيق أغراض معينة.

طرح البرنامج للتداول:

يكون لمؤلف البرنامج استغلال برنامجه بطرحه للتداول أو توزيعه، وهذا الحق يعتبر في أحيان كثيرة متضمناً في حق الطبع أو النسخ. فعندما يبرم مؤلف البرنامج عقداً يتعلق بنسخ برنامجه، فإنه يملك سلطة تحديد ظروف وشروط توزيع النسخ، وتغطي هذه العقود أمور عدة مثل الكمية والثمن والنطاق الجغرافي للتوزيع المرخص به.

نقل البرنامج من لغة إلى لغة أخرى:

إن نقل البرنامج من لغة المصدر إلى لغة الهدف، تعد ترجمة للبرنامج من لغة إلى أخرى فإذا قام به المؤلف لوحده فإنه يكون قد جسد حقه المالي على البرنامج كما أن حقه الاستئثاري في الترجمة يمكن التنازل عنه للغير مقابل أو بدون مقابل ولا يجوز للغير القيام بهذه الترجمة دون موافقة مؤلف البرنامج وإلا عدّ مقلداً للبرنامج.

تصرف مؤلف برامج الحاسب بالحق المالي:

تعتبر حقوق مؤلف برنامج الحاسب كغيره من مؤلفي المصنفات الأدبية والفنية حقوق ملكية استئثارية لمال معنوي أو حقوقاً شخصية نظراً لأن المصنف ينبع من شخصية مبدعه ومن ثم فإن الحقوق المالية يمكن أن يكون التصرف بها من قبيل منح الحق في استخدام المصنف وبدونه يصبح استخدام الغير للمصنف غير مشروع.

منحت غالبية تشريعات حقوق المؤلف الحق في التصرف بالحقوق التي تشكل مضمون حقه المالي، وكأي مؤلف لمصنف أدبي أو فني فإن لمؤلف برنامج الحاسب أن يتصرف في حقوقه المالية الواردة على البرنامج، من خصائص الحق المالي للمؤلف قابليته للتصرف، سواء كان هذا التصرف بمقابل أو بدون مقابل.

التنظيم القانوني للبرمجيات وقواعد البيانات

لتنظيم القانوني للبرمجيات وقواعد البيانات يشمل مجموعة من القوانين والمعايير التي تهدف إلى حماية حقوق الملكية الفكرية، ضمان الاستخدام القانوني، وتقديم إطار عمل لحل النزاعات التي قد تنشأ. يشمل التنظيم القانوني عدة جوانب رئيسية، تتناول البرمجيات وقواعد البيانات بشكل منفصل وتكامل.

1. حماية البرمجيات

أ .حقوق الطبع والنشر

- **التعريف** :البرمجيات تُعتبر عملاً أدبيًا محميًا بموجب حقوق الطبع والنشر. هذا يعني أن المبرمجين والمؤلفين لديهم حقوق حصرية في نسخ، توزيع، وتعديل البرمجيات.
- **التطبيق** :حقوق الطبع والنشر تمنح الحماية للشفرة المصدرية للبرمجيات، الشفرة الثنائية (المجمعة)، والوثائق المرتبطة بها.

ب .براءات الاختراع

- **التعريف** :في بعض الحالات، يمكن أن تكون البرمجيات أو أجزاء منها مؤهلة للحصول على براءة اختراع، خاصة إذا كانت تقدم تقنية جديدة ومبتكرة.
- **التطبيق** :البراءات توفر حماية للابتكارات التقنية في البرمجيات، لكن تطبيق البراءات على البرمجيات يختلف من بلد لآخر ويعتمد على قوانين البراءات المحلية.

ج .العلامات التجارية

- **التعريف** :يمكن تسجيل أسماء المنتجات، الشعارات، أو العلامات التجارية المتعلقة بالبرمجيات كعلامات تجارية لحمايتها من الاستخدام غير المصرح به.
- **التطبيق** :العلامات التجارية تساهم في حماية سمعة المنتج وتجنب الخلط بين منتجات الشركات المختلفة.

د .اتفاقيات الترخيص

- **التعريف** :اتفاقيات الترخيص تحدد شروط استخدام البرمجيات وتوزيعها. تشمل شروط الترخيص ما يُسمح للمستخدمين بفعله وما يُمنع عليهم.
- **التطبيق** :تُعتبر اتفاقيات الترخيص وثائق قانونية تُلزم المستخدمين بالشروط المحددة من قبل مطوري البرمجيات، مثل عدم توزيع البرمجيات بشكل غير قانوني أو تعديلها.

2. حماية قواعد البيانات

أ .حقوق الطبع والنشر لقواعد البيانات

- **التعريف** :قواعد البيانات يمكن أن تكون محمية بحقوق الطبع والنشر، خصوصًا إذا كانت تحتوي على محتوى أو تنظيم معين يبرز الإبداع والابتكار.
- **التطبيق** :حماية حقوق الطبع والنشر لقواعد البيانات تمنح مالكي قواعد البيانات حقوقًا حصرية على تنظيم وتصنيف البيانات والمواد الخاصة بها.

ب .حقوق قاعدة البيانات الخاصة بالاتحاد الأوروبي

- **التعريف** :في الاتحاد الأوروبي، هناك تشريع خاص لحماية قواعد البيانات يُعرف بـ "قانون حماية قواعد البيانات(Database Directive) "، الذي يمنح حماية قانونية للمصممين والمطورين ضد استغلال أو نسخ قواعد البيانات بدون إذن.
- **التطبيق** :يوفر هذا التشريع حماية خاصة للتصميم والتنظيم من خلال منح حقوق استثمارية للمطورين على استثماراتهم في جمع البيانات وتنظيمها.

3. التنظيم القانوني العالمي والمحلي

أ .الاتفاقيات الدولية

- **اتفاقية برن** :تحمي حقوق الطبع والنشر للأعمال الأدبية والفنية بما في ذلك البرمجيات، وتساعد على حماية البرمجيات عبر الحدود.
- **اتفاقية تريبس** :**(TRIPS)** توفر إطارًا عالميًا لحماية الملكية الفكرية، بما في ذلك حقوق البرمجيات وقواعد البيانات، وتعزز من تطبيق قوانين حماية الملكية الفكرية بشكل موحد بين الدول الأعضاء.

ب .القوانين المحلية

- **قوانين حماية الملكية الفكرية** :كل بلد لديه قوانينه الخاصة بحماية البرمجيات وقواعد البيانات، والتي تتوافق مع أو تتجاوز المتطلبات الدولية.
- **التشريعات الخاصة بالتراخيص والبراءات** :تختلف من بلد لآخر، ويجب على الشركات والمطورين الالتزام بالقوانين المحلية المتعلقة بالترخيص، البراءات، وحقوق الطبع والنشر.

4. الأدوات والتدابير القانونية

أ .اتفاقيات الترخيص والتوزيع

- **المحتوى** :تحدد كيفية استخدام البرمجيات أو قواعد البيانات، بما في ذلك حقوق النسخ والتوزيع والتعديل.
- **التطبيق** :اتفاقيات الترخيص والتوزيع تحدد شروط الاستخدام وتساعد في حماية الحقوق القانونية للمطورين.

ب .إجراءات التظلم والحماية

- **القضايا القانونية** :توفير سبل قانونية لحل النزاعات المتعلقة بالقرصنة أو التعدي على الحقوق. يشمل ذلك رفع دعاوى قضائية ضد الأفراد أو الشركات التي تنتهك حقوق الملكية الفكرية.
- **التعويضات** :تشمل الأضرار المالية والتعويضات القانونية التي يمكن أن تمنح للأطراف المتضررة نتيجة التعدي على حقوق البرمجيات أو قواعد البيانات.

5. الأمن السيبراني والتدابير التقنية

- **حماية البيانات** :استخدام التشفير والتدابير الأمنية لحماية البرمجيات وقواعد البيانات من الوصول غير المصرح به والهجمات السيبرانية.
- **إدارة الحقوق الرقمية** :**(DRM)** تقنيات تمنع النسخ غير المصرح به وتساعد في حماية البرمجيات من التوزيع غير القانوني.

الدور الأمني في حماية البرمجيات

وتجدر الإشارة إلي أن هناك العديد من القوانين التي تحميالمنتجات التي تتعلق بالتكنولوجيا. والتي يمكن إجمالها في التالي:

- تشريعات الخصوصية أو قواعد حماية تجميع ومعالجة وتخزين وتبادل البيانات الشخصية .
- تشريعات جرائم الكمبيوتر.
- تشريعات الملكية الفكرية في حقل حماية البرمجيات .
- تشريعات الأصول الإجرائية الجزائية. وتشريعات الإثبات المتفقة مع عصر المعلومات .
- تشريعات معايير الأمن المعلوماتي .
- تشريعات التجارة الألكترونية "التواقيع الألكترونية. والتعاقد الألكتروني. إلخ ."

والأهمية الاقتصادية لحماية برامج الحاسب الآلي تتمثل في :

الأهمية الاقتصادية لحماية برامج الحاسب الآلي تتجلى في عدة جوانب رئيسية، حيث تلعب الحماية الفعالة للبرمجيات دورًا حيويًا في تعزيز النمو الاقتصادي، الابتكار، واستدامة الأعمال. إليك أبرز الأبعاد الاقتصادية للحماية الفعالة للبرمجيات:

6. تعزيز الابتكار والإبداع

- **تشجيع الاستثمار** :حماية البرمجيات تعزز من قدرة الشركات والمطورين على الاستثمار في البحث والتطوير، حيث يعرفون أن ابتكاراتهم ستكون محمية من الاستغلال غير المشروع.
- **تحفيز الإبداع** :عندما تكون الحقوق محفوظة، يُشجع المطورون على تطوير تقنيات وبرمجيات جديدة دون خوف من السرقة أو التعدي على أفكارهم.

7. زيادة قيمة الشركات

- **حماية الأصول الرقمية** :البرمجيات هي أحد الأصول القيمة للشركات، وحمايتها تساهم في الحفاظ على قيمتها المالية. الشركات التي تحمي برمجياتها بشكل فعال يمكن أن تحسن سمعتها وتعزز قيمة علامتها التجارية.
- **تعزيز الثقة** :العملاء والشركاء يثقون أكثر في الشركات التي تحمي برمجياتها بشكل جيد، مما يمكن أن يؤدي إلى زيادة في الأعمال والعقود.

8. الحد من الخسائر المالية

- **تقليل القرصنة** :حماية البرمجيات تساهم في تقليل الخسائر الناتجة عن القرصنة والنسخ غير المصرح به. الشركات التي تعاني من فقدان الإيرادات بسبب استخدام البرمجيات المقرصنة تواجه أضرارًا مالية كبيرة.
- **الحفاظ على الإيرادات** :عندما يتم حماية البرمجيات بفعالية، يمكن للشركات الحفاظ على مصادر دخلها وزيادة إيراداتها من مبيعات البرمجيات والخدمات المرتبطة بها.

9. تعزيز الأمن السيبراني

- **حماية البيانات** :البرمجيات المحمية تساعد في تأمين البيانات الحساسة وتقلل من مخاطر التسريب والاختراق. هذا يعزز من استقرار الشركات ويقلل من تكاليف التعافي من الهجمات السيبرانية.
- **الامتثال للمعايير** :حماية البرمجيات تساعد الشركات على الامتثال لمتطلبات الأمان والخصوصية، مما قد يكون له تأثير إيجابي على قدرتها على الدخول إلى أسواق جديدة أو الحفاظ على عقود عمل.

10. تعزيز النمو الاقتصادي

- **خلق فرص عمل** :صناعة البرمجيات توفر العديد من فرص العمل في مجالات مختلفة مثل التطوير، الدعم الفني، وأمن المعلومات. حماية البرمجيات تدعم هذه الصناعة وتساعد في خلق المزيد من فرص العمل.
- **تحفيز الاقتصاد الرقمي** :البرمجيات هي أساس الاقتصاد الرقمي الحديث، وحمايتها تساهم في دعم هذا القطاع وتنميته، مما يعزز النمو الاقتصادي العام.

11. تشجيع التعاون الدولي

- **تسهيل التجارة العالمية** :حماية البرمجيات تدعم التجارة الدولية من خلال ضمان أن الشركات التي تصدر برمجياتها إلى أسواق مختلفة تستطيع حماية حقوقها القانونية والحصول على التعويض المناسب.
- **تقليل النزاعات القانونية** :عندما تكون قوانين حماية البرمجيات قوية وموحدة عبر الدول، يتم تقليل النزاعات القانونية المرتبطة بالملكية الفكرية، مما يسهل على الشركات العالمية إدارة عملياتها.

12. حماية الابتكارات الجديدة

- **إعادة استثمار الأرباح** :الشركات التي تحمي برمجياتها يمكنها إعادة استثمار الأرباح في تطوير منتجات وخدمات جديدة، مما يعزز النمو المستدام والابتكار المستمر.

13. تعزيز المنافسة العادلة

- **حماية حقوق المطورين** :حماية البرمجيات تساعد في ضمان أن جميع الشركات تعمل في بيئة تجارية عادلة، مما يعزز المنافسة الصحية ويشجع على تحسين الجودة والخدمات.

14. تجنب الأضرار القانونية

- **تقليل المخاطر القانونية** :حماية البرمجيات تساهم في تجنب القضايا القانونية المرتبطة بالقرصنة أو التعدي على حقوق الملكية الفكرية، مما يقلل من التكاليف المرتبطة بالنزاعات القانونية.

الحماية الفعالة للبرمجيات ليست فقط قضية قانونية، بل هي أيضًا مسألة اقتصادية حيوية تدعم الابتكار، الأمن، والنمو في صناعة تكنولوجيا المعلومات والقطاعات الاقتصادية الأخرى.

.

<u>الدور الأمني في حماية البرمجيات</u>

الدور الأمني في حماية البرمجيات هو جزء حيوي من عملية تطوير البرمجيات وتشغيلها، حيث يتضمن مجموعة من الإجراءات والتدابير التي تهدف إلى حماية البرامج من التهديدات الأمنية المختلفة وضمان سلامتها وسلامة البيانات التي تتعامل معها. إليك بعض الجوانب الرئيسية للدور الأمني في حماية البرمجيات:

1. التشفير

حماية البيانات :التشفير هو عملية تحويل البيانات إلى صيغة غير مفهومة لمنع الوصول غير المصرح به. يُستخدم التشفير لحماية البيانات المخزنة في البرمجيات وكذلك البيانات المرسلة عبر الشبكات.

2. اختبار الأمان(Security Testing)

تحليل الثغرات :يتم اختبار البرمجيات بشكل منتظم للكشف عن الثغرات الأمنية المحتملة. هذا يشمل فحص الشفرات، واختبار البرمجيات في بيئات متعددة للتأكد من عدم وجود نقاط ضعف يمكن استغلالها.

اختبار الاختراق :(Penetration Testing) وهو محاكاة لهجوم إلكتروني على البرمجية لتحديد نقاط الضعف التي يمكن أن يستغلها المهاجمون.

3. إدارة التحديثات والتصحيحات(Patch Management)

التحديثات الأمنية :يُعدّ تحديث البرمجيات بانتظام أمرًا بالغ الأهمية لإصلاح الثغرات الأمنية المكتشفة حديثًا. التحديثات والتصحيحات الأمنية تساعد في حماية البرمجيات من التهديدات الجديدة والمتطورة.

4. التحكم في الوصول(Access Control)

تحديد الصلاحيات :التحكم في من يستطيع الوصول إلى أجزاء معينة من البرمجيات يعتبر جزءًا أساسيًا من الأمان. يمكن استخدام التحقق الثنائي (Two-Factor Authentication) وكلمات المرور المعقدة لتأمين الوصول.

إدارة هويات المستخدمين :تطبيق سياسات قوية للتحقق من هويات المستخدمين وضمان أن كل مستخدم لديه فقط الوصول إلى الأجزاء الضرورية من البرمجيات.

5. التدريب والتوعية الأمنية

التوعية بين المطورين :تدريب المطورين على أفضل الممارسات الأمنية يعتبر خطوة أساسية في حماية البرمجيات. هذا يتضمن التعليم حول كيفية كتابة شفرات آمنة، وكيفية التصدي للهجمات الشائعة مثل حقن SQL (SQL Injection) أو البرمجة عبر المواقع(Cross-Site Scripting).

التوعية للمستخدمين :يجب تثقيف المستخدمين حول كيفية استخدام البرمجيات بشكل آمن، بما في ذلك أهمية كلمات المرور القوية، وتجنب النقر على الروابط المشبوهة، والتأكد من مصادر التطبيقات قبل تنزيلها.

6. إدارة الأحداث الأمنية والاستجابة لها

التحقق والمراقبة :أنظمة إدارة الأحداث الأمنية والمعلومات (SIEM) تراقب البرمجيات باستمرار لاكتشاف أي نشاط غير طبيعي قد يشير إلى محاولة اختراق.

الاستجابة السريعة :يجب أن يكون هناك خطة للاستجابة السريعة في حال اكتشاف أي اختراق أمني، تشمل عزل البرمجيات المتأثرة، وتحليل الهجوم، وتنفيذ الإجراءات التصحيحية.

7. التوثيق والسياسات الأمنية

إعداد السياسات الأمنية :تطوير وتطبيق سياسات أمنية صارمة بشأن كيفية التعامل مع البيانات والبرمجيات. هذه السياسات توفر إرشادات واضحة حول الإجراءات التي يجب اتباعها لضمان أمان البرمجيات.

توثيق التغييرات :توثيق جميع التغييرات والتحديثات التي تطرأ على البرمجيات لضمان إمكانية مراجعة أي خطوة وتحليل أي خرق أمني قد يحدث.

8. التقييم الأمني المستمر

مراجعة دورية :إجراء تقييمات دورية للأمن للتأكد من أن البرمجيات لا تزال آمنة ضد التهديدات الجديدة والمستجدة.

تحليل المخاطر :تقييم المخاطر بشكل منتظم يساعد في تحديد المناطق التي تحتاج إلى تعزيز أمني وتحسين الإجراءات الوقائية.

الدور الأمني في حماية البرمجيات ليس مجرد مجموعة من الإجراءات التقنية، بل هو جزء أساسي من دورة حياة تطوير البرمجيات، ويتطلب تعاونًا وثيقًا بين المطورين، وإدارات تكنولوجيا المعلومات، والأمن السيبراني لضمان أن تكون البرمجيات آمنة ضد التهديدات الحالية والمستقبلية.

معوقات الدورالأمني في محاربة قرصنة البرامج، وتجارب الدول المختلفة لمواجهتها

1. **التطور المستمر في تقنيات القرصنة:**

- القراصنة يستخدمون تقنيات متقدمة ومتجددة باستمرار، مما يجعل من الصعب على الأمن السيبراني مواكبة هذه التطورات. الهجمات مثل "الهندسة العكسية" وتحليل الشفرات أصبحت شائعة لقرصنة البرامج.

2. **نقص الوعي الأمني:**

- نقص الوعي بين المستخدمين والشركات حول أهمية حماية البرمجيات يعزز من انتشار القرصنة. العديد من المستخدمين لا يفهمون تداعيات استخدام البرمجيات المقرصنة، بما في ذلك المخاطر الأمنية المحتملة.

3. **تكاليف الحماية العالية:**

- تأمين البرمجيات بشكل فعال يتطلب استثمارات كبيرة في التكنولوجيا والموارد البشرية. بعض الشركات، وخاصة الصغيرة منها، قد لا تمتلك الموارد الكافية لتنفيذ إجراءات أمنية شاملة.

4. **البنية التحتية القانونية غير المكتملة**:

- في بعض الدول، قوانين حماية الملكية الفكرية ضعيفة أو غير مطبقة بشكل فعال. هذا يؤدي إلى صعوبة مقاضاة القراصنة والموزعين غير الشرعيين للبرامج المقرصنة.

5. **سهولة التوزيع عبر الإنترنت**:

- الإنترنت يُسهل توزيع البرمجيات المقرصنة بشكل واسع، حيث يمكن للقراصنة مشاركة البرامج عبر مواقع الويب، المنتديات، وخدمات مشاركة الملفات. هذا الانتشار السريع يجعل من الصعب تعقب وملاحقة المخالفين.

6. **ضعف التعاون الدولي**:

- قرصنة البرامج غالبًا ما تتجاوز الحدود الوطنية، مما يجعل من الصعب تعقب القراصنة وفرض القوانين بشكل دولي. ضعف التعاون بين الدول يمكن أن يعيق الجهود لمكافحة القرصنة على نطاق عالمي.

7. **الإجراءات القانونية البطيئة**:

- حتى في الدول التي تمتلك قوانين صارمة، قد تكون الإجراءات القانونية بطيئة وغير فعالة في ملاحقة القراصنة أو منعهم من إعادة قرصنة البرامج.

تجارب الدول المختلفة لمواجهة قرصنة البرامج:

1. **الولايات المتحدة**:

- **قوانين صارمة وتطبيق قوي** :الولايات المتحدة لديها بعض من أقوى قوانين حماية الملكية الفكرية في العالم. بالإضافة إلى ذلك، وكالة البرمجيات التجارية (BSA) تلعب دورًا رئيسيًا في مكافحة القرصنة من خلال حملات التوعية والملاحقات القانونية.

- **التحالفات بين القطاعين العام والخاص** :التعاون بين الحكومة والشركات الكبرى مثل مايكروسوفت وأدوبي ساهم في تقليل نسبة القرصنة بشكل ملحوظ.

2. **الاتحاد الأوروبي**:

- **تشريعات موحدة** :الاتحاد الأوروبي يعمل على توحيد قوانين حماية الملكية الفكرية بين دوله الأعضاء، مما يسهل على الشركات اتخاذ إجراءات قانونية ضد القرصنة على مستوى القارة.
- **التعاون العابر للحدود** :برامج مثل "Europol" تساعد في تعزيز التعاون بين الدول الأعضاء لمكافحة الجرائم السيبرانية بما في ذلك قرصنة البرمجيات.

3. **الصين**:

- **التشديد التدريجي على القوانين** :على الرغم من أن الصين كانت تُعرف بأنها بؤرة للقرصنة، إلا أنها بدأت في السنوات الأخيرة تشديد قوانين حماية الملكية الفكرية نتيجة لضغوط دولية ولتحفيز الابتكار المحلي.
- **حملات التوعية** :الحكومة الصينية بدأت في زيادة حملات التوعية بأهمية احترام حقوق الملكية الفكرية، مع تنفيذ عقوبات أشد على المخالفين.

4. **الهند**:

- **تطبيق القوانين وتحديث البنية التحتية القانونية** :الهند تعمل على تحسين قوانين الملكية الفكرية وتطبيقها بفعالية أكبر. مبادرات مثل "Digital India"تشجع على استخدام البرمجيات القانونية من خلال توفير بدائل ميسورة التكلفة.
- **التعاون مع الشركات العالمية** :الهند تتعاون مع شركات البرمجيات العالمية لتعزيز استخدام البرمجيات المرخصة وتوفير حلول بأسعار معقولة لمكافحة القرصنة.

5. **روسيا**:

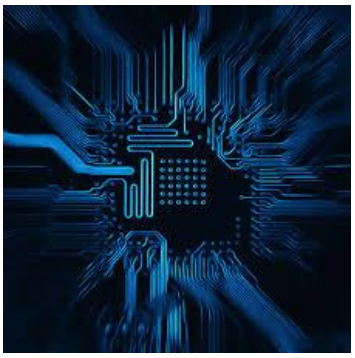
- **تحديات قانونية وثقافية** :على الرغم من وجود قوانين لمكافحة القرصنة، إلا أن التطبيق في روسيا لا يزال تحديًا. هناك جهود حكومية لزيادة وعي

الجمهور والشركات حول مخاطر القرصنة، ولكن الموقف العام تجاه استخدام البرمجيات المقرصنة لا يزال متساهلاً.

الحلول والتوصيات:

- **تعزيز التعاون الدولي** :يجب تعزيز التعاون بين الدول لمكافحة القرصنة عبر الحدود، من خلال معاهدات واتفاقيات تضمن تبادل المعلومات والملاحقة القانونية الفعالة.
- **التوعية والتعليم** :زيادة الوعي حول المخاطر القانونية والأمنية للبرمجيات المقرصنة بين المستخدمين والشركات يمكن أن يقلل من الطلب عليها.
- **التكنولوجيا المضادة للقرصنة** :الاستثمار في تقنيات متقدمة مثل إدارة الحقوق الرقمية (DRM) وتحليل السلوك يمكن أن يساعد في حماية البرمجيات من القرصنة.
- **تشجيع البدائل القانونية** :تقديم برامج بديلة بأسعار مناسبة أو بنماذج اشتراك يمكن أن يقلل من الإقبال على البرمجيات المقرصنة.

مكافحة قرصنة البرمجيات تتطلب جهودًا متكاملة من الحكومات والشركات والأفراد، إضافة إلى تفعيل القوانين وتحديث السياسات لضمان حماية فعالة للملكية الفكرية.



الحماية الدولية لبرامج الحاسب الآلي تعتبر من القضايا الأساسية في مجال حماية الملكية الفكرية، وهي تشمل مجموعة من القوانين والتدابير التي تهدف إلى حماية حقوق المؤلفين والمطورين للبرمجيات من التعدي والقرصنة على مستوى عالمي. إليك أبرز جوانب الحماية الدولية لبرامج الحاسب الآلي:

1. **اتفاقية برن لحماية الأعمال الأدبية والفنية**

- **التعريف** :هي واحدة من أهم الاتفاقيات الدولية التي تهدف إلى حماية حقوق المؤلفين والفنانين عبر الحدود. تتضمن حماية البرمجيات كأعمال أدبية وفنية ضمن نطاقها.
- **النطاق** :تضمن الاتفاقية حماية حقوق المؤلفين في البلدان الأعضاء دون الحاجة لتسجيل حقوقهم في كل بلد على حدة.

2. اتفاقية تريبس(TRIPS)

- **التعريف** :هي جزء من اتفاقيات منظمة التجارة العالمية (WTO) التي تضع معايير دولية لحماية الملكية الفكرية، بما في ذلك حقوق الطبع والنشر والبرمجيات.
- **النطاق** :تفرض الاتفاقية على الدول الأعضاء تبني قوانين محلية تتوافق مع المعايير الدولية لحماية البرمجيات من القرصنة والتعدي.

3. اتفاقية الجوانب المتعلقة بالتجارة من حقوق الملكية الفكرية(TRIPS)

- **التعريف** :تتضمن جوانب حماية البرمجيات كأعمال فكرية، وتوفر إطارًا للتعامل مع انتهاكات حقوق البرمجيات.
- **التطبيق** :توفر اتفاقية TRIPS نظامًا للمراجعة والرقابة والتسوية في النزاعات المتعلقة بحقوق الملكية الفكرية، مما يسهم في تعزيز حماية البرمجيات عالميًا.

4. اتفاقية حق المؤلف في الإنترنت(WIPO Copyright Treaty)

- **التعريف** :هي معاهدة دولية تهدف إلى تحديث قوانين حقوق المؤلف بما يتماشى مع التقدم التكنولوجي وتوفير حماية للبرمجيات والمواد الرقمية عبر الإنترنت.
- **النطاق** :تركز على حماية حقوق المؤلفين من التعديات عبر الإنترنت وضمان حقوقهم في التوزيع والتعديل والاستخدام.

5. قوانين الملكية الفكرية المحلية

- **التطبيق** :الدول الأعضاء في المنظمات الدولية مثل منظمة التجارة العالمية يمكنها اعتماد قوانين محلية تتماشى مع المعايير الدولية للحماية.
- **التنفيذ** :تشمل قوانين الطبع والنشر وبراءات الاختراع التي تحمي البرمجيات من القرصنة والتعديات داخل حدود كل دولة.

6. التعاون الدولي والتبادل المعلوماتي

- **التعاون بين الدول** :تعزيز التعاون بين الدول لمكافحة القرصنة من خلال تبادل المعلومات والموارد والتنسيق في القضايا القانونية والأمنية.
- **المنظمات الدولية** :منظمات مثل المنظمة العالمية للملكية الفكرية (WIPO) تلعب دورًا كبيرًا في التنسيق والتعاون الدولي لحماية حقوق الملكية الفكرية.

7. أدوات الحماية التقنية

- **إدارة الحقوق الرقمية** :**(DRM)** تقنيات تمنع النسخ غير المصرح به والتوزيع غير القانوني للبرمجيات.
- **التشفير** :حماية البيانات والبرمجيات من الوصول غير المصرح به من خلال تقنيات التشفير.

8. المسؤولية القانونية للشركات

- **الالتزام بالقوانين** :الشركات الكبرى التي تطور وتبيع البرمجيات يجب أن تلتزم بالقوانين المحلية والدولية لحماية حقوقها.
- **التقارير والملاحقات القانونية** :الشركات قد تقوم برفع دعاوى قانونية ضد الأطراف التي تنتهك حقوقها أو تسعى لملاحقة القراصنة.

تجارب الدول في الحماية الدولية للبرمجيات:

1. **الولايات المتحدة**:

- **قوانين قوية وتطبيق فعال** :الولايات المتحدة لديها قوانين صارمة لحماية حقوق البرمجيات، مثل قانون حقوق الطبع والنشر للبرمجيات (Software Copyright Act)، وتعمل على تنفيذ هذه القوانين بشكل فعال بالتعاون مع شركات البرمجيات العالمية.

2. **الاتحاد الأوروبي**:

- **تطبيق موحد للقوانين** :الاتحاد الأوروبي يعمل على توحيد قوانين حماية الملكية الفكرية بين الدول الأعضاء، مما يعزز الحماية الدولية للبرمجيات داخل أوروبا.

3. **الصين**:

- **تحسين الحماية** :الصين بدأت في تعزيز قوانين حماية البرمجيات تحت ضغط دولي وزيادة الوعي حول احترام حقوق الملكية الفكرية، مع التركيز على تقليل القرصنة وتحسين آليات التنفيذ.

4. **الهند**:

- **إجراءات جديدة** :الهند تعمل على تحسين إطارها القانوني لحماية البرمجيات، مع زيادة التركيز على تشجيع استخدام البرمجيات القانونية من خلال مبادرات حكومية.

تطبيق الحماية الدولية للبرمجيات يتطلب جهودًا منسقة على مستويات متعددة، بما في ذلك القوانين والتقنيات والتعاون الدولي، لضمان حماية فعالة ضد القرصنة والتعدي على حقوق الملكية الفكرية.

نماذج اسئلة

اولا: اختار الاجابة الصحيحة من اختيارات الاتية:

1.المعايير أو قواعد السلوك المتوقعة من الفرد من قبل مجموعة ينتمي إليها الفرد هي....

A. المبادئ
B. الأخلاق
C. القانون
D. الدين

2. هناك العديد من القوانين التي تحمي المنتجات التي تتعلق بالتكنولوجيا منها

A. تشريعات جرائم الكمبيوتر
B. تشريعات الملكية الفكرية
C. تشريعات معايير الأمن المعلوماتي
D. .كل ما سبق

3.قابلية الاختراع للاستغلال الصناعي هو من شروط

A. منح براءة الاختراع
B. الملكية الفكرية
C. حقوق النشر

D. ليس مما سبق

4.تعد اول واهم المصنفات المعلوماتية اللي يجب توفير الحماية القانونية له

A. المواقع الالكترونية
B. قواعد البيانات
C. البرمجيات
D. الانترنت

5.مجموعة الحقوق الأدبية والمادية التي يتمتع به أصحاب الحقوق عن استغلال مصنفاتهم الأدبية والفنية والعلمية هي

A. حقوق النشر
B. حقوق المؤلف
C. براءة الاختراع
D. .حماية البيانات

6.من لوائح التنظيم الذاتي لضبط أخلاقيات الانترنت التي تقوم بتنظيم فحوى المواقع والمعلومات التي تنظمنها

A. لوائح تنظيم المحتوى بشبكة الانترنت.
B. لوائح تنظيم التقنيات بشبكة الانترنت.
C. قواعد أخلاقيات لمستعملي الانترنت.
D. لوائح التنظيم المساعد

7.هي عبارة عن برامج خاصه مهمتها تعطيل النظام وتعطيل العمليات الخاصة به بالإضافة الى تخريب البيانات والمعلومات المتواجدة على جهاز الحاسوب

A. البرمجيات الخبيثة
B. القرصنة
C. الهاكر
D. لا شى مما سبق

8. هي عبارة عن إدخال تعديلات على المعلومات عند إرسالها إلى جهة معينة

A. البصمة الالكترونية
B. العلامات المائية الرقمية
C. تشفير البيانات
D. كل مما سبق

9 ..... .هو توصيف للمعلومات) نصوص، صور، رسوميات. إلخ (التي تعرض على صفحات الموقع الالكتروني الخاصة بالشركات

A. الموقع الالكتروني

B. البرمجيات
C. قواعد البيانات الالكترونية
D. حماية المعلومات

10.هي وثيقة قانونية تمنح المبتكر أو الشركة المالكة للابتكار حقا احتكاريا على الأفكار أو المعارف التي تتضمنها

A. عقد ترخيص البرنامج
B. العلامة التجارية
C. الاسرار التجارية
D. براءة الاختراع

11 .تعتبر البرمجيات، قواعد البيانات، والمواقع الالكترونية من

A. الملكية الفكرية الرقمية
B. الملكية الفكرية التقليدية
C. النماذج الصناعية
D. حق النشر أو المؤلف

12.ما الذي تحميه العلامة التجارية؟

A. الاختراع
B. عمل فني
C. منظر وشكل وحس المنتج
D. صيغه سريه

13.من خصائص الجرائم الفضائية كل مما يأتي ماعدا-----

A. جريمة غير مقيدة برمان ومكان إذا تمتاز بالتباعد الجغرافي
B. سهوله اخفاء اثار الجريمة والأدلة
C. سهوله الكشف عن مرتكب الجريمة
D. سلوك غير أخلاقي خارج عن المألوف

14.شهادة المخترق الأخلاقي CEH هي تمكن من

A. مكافحة اختراق البيانات للحصول عليها
B. امتلاك المهارات الكافية التي تخولهم احتراف آليات ووسائل حماية المعلومات
C. معرفة الثغرات التي تتواجد في الطرق التي يتبعها المخترقون
D. ليس مما سبق

15.مهندس أو مسؤول تحليل البيانات الأمنية يقوم ب

A. تأمين حفظ المعلومات عبر مختلف المنصات والعمل على تصحيح أي من الأخطاء التي قد تهدد أمنها

B. تتبع محاولات الاختراق وذلك من أجل معرفة مصدر الهجمات الإلكترونية
C. تقييم حالة أنظمة الشر ات وتحديد مواطن الضعف فيها
D. كشف أي ثغرات أمنية قد تجعل المعلومات عرضه للهجمات السيبرانية

16. هو إمكانية رفع المعلومات عبر شبكة الإنترنت لإتاحة الوصول إليها في أي زمان ومكان

A. برامج مكافحة الاختراق
B. التخزين السحابي
C. الجدران النارية
D. التشفير

17.هناك حاجة إلى إرشادات عامة لأخلاقيات الحاسب من أجل

A. التكسير
B. جرائم الحاسوب
C. حماية البيانات الشخصية
D. جميع ما سبق

18.التكسير Cracking يأتي تحت____

A. خدمة الموقع
B. النسخ
C. جرائم الالكترونية
D. أمن البيانات

19 ____.هي مجموعة من القواعد لتحديد المعايير الأخلاقية أو السلوك المقبول اجتماعيا.

A. البروتوكول
B. المعيار
C. .الأخلاق
D. ليس مما سبق

20.كيف تحافظ على جهاز الكمبيوتر الخاص بك آمنًا في مكان العمل .....؟

A. ابق على اطلاع بالتحديثات
B. حافظ على كلمات المرور قوية
C. احذر من شبكات الواي فاي العامة
D. كل مما سبق

21.أي مما يلي ليس من الوصايا لأخلاقيات الحاسب؟

A. لا يجوز لك استخدام أو نسخ البرامج التي لم تدفع مقابلها.
B. يجب أن يفكر الآلاف في العواقب الاجتماعية للبرنامج الذي تكتبه.
C. يجب ألا تتدخل في عمل أجهزة الكمبيوتر للآخرين

D. يجب ألا تستخدم الكمبيوتر للقيام بشيء ممتع.

22.يشمل الأمن السيبراني حماية كلٌ من

A. الحواسيب.
B. السيرفرات.
C. التخزين السحابي
D. كل مما سبق

23.هي حماية البيانات من أي تغيير قد يطرأ عليها من جهة غير مسموح لها بذلك أو تعديلها، ويكون القصد من هذا التغيير التخريب أو الانتهاك للملفات الهامة وإلحاق الضرر بها

A. السرية
B. التكاملية
C. التوافر
D. ليس مما سبق

24. هي تحقيق الحماية للطبقة الأقرب لجهاز الحاسوب

A. أنظمة حماية نظم التشغيل
B. أنظمة حماية لغات البرمجة
C. أنظمة حماية البرامج التطبيقية
D. أنظمة حماية قواعد البيانات

ثانيا: ضع علامة √ امام العبارات الصحيحة وعلامة × امام العبارات الخاطئة :(الدرجة =14)

1. يهدف الأمن السيبرانى بشكل رئيسي إلى تقديم الحماية للمعلومات من الاختراق والتعرض للتخريب المتعمد.
2. من عناصر أمن المعلومات مستشعرات العلامات الحيوية مثل آليات مسح البصمات
3. التشفير هو محاكاة عمليات الاختراق المحتمل وقوعها
4. البرمجيات هي مجموعة عناصر البيانات المنطقيّة المرتبطة مع بعضها البعض بعلاقة رياضيّة، وتتكون من جدول واحد أو أكثر
5. الهندسة الاجتماعية هي برامج توثر على الأداء العادي لجهاز الكمبيوتر مثل البرامج الضارة
6. من مخاطر الجرائم الالكترونية المساس بالاقتصاد والأمن الوطني وتهديده.
7. تتنوع انتشار أسباب الجرائم الإلكترونية ومنها الترفيه والمزاح مع الآخرين
8. تعرف المعلومات بأ نها مجموعة من البيانات التي طرأت عليها عمليّات تغيير ومُعالجة
9. لا تعد البرمجيات software ملكية شخصية ولا يمكنك اعتبارها لها حقوق ملكية فكرية
10. يمكن للمعلمين والطلاب نسخ أي قدر من العمل من مصدر محمي بحقوق النشر بدون طلب الإذن

11. عند إنشاء صفحة ويب، يمكنك استخدام شعار الشركة طالما أن الشعار مرتبط بـ موقع الشركة
12. إخفاء هوية المستخدمين هي وسيلة للحفاظ على هوية المستخدمين من خلال مختلف التطبيقات VPN وغيرهم من التطبيقات.
13. الانتحال هو فعل نسخ ونشر عمل شخص آخر دون اقتباس مناسب
14. المبادئ الأخلاقية هي أدوات تستخدم للتفكير في المواقف الصعبة.

أهم المراجع

http://www.rsc-northwest.ac.uk/technical/dns/The%20DNS.asp
/http://www.sanog.org-sanog1-dnstrain.pdf
http://www.fistconference.org/data/presentaciones/dnssecurity.pdf
http://www.ep.net/training/tld-rio-day2.pdf
http://security.polito.it/doc/pub/dnssec.pdf

البرمجيات وبراءة الاختراع د. نزار الحافظ .

David Brainbridge, "Introduction to computer law", forth edition, Longman, 2000.

د. نزار الحافظ، م. جلال فارس الحداد، "تطبيق حماية الملكية الفكرية على برامج الحاسوب"، مكتبة الأسد، كانون الثاني ٢٠٠٠.

التجارة الإلكترونية – إبراهيم بختي.

العقود الإلكترونية – منتدى طلبة جامعة البحرين ـ كلية الحقوق.

الملكية الفكرية في مجتمع المعلومات – محمد حجازي.

حقوق الملكية الفكرية – محمد السيد عرفة – مجلة البحوث الأمنية العدد (٢٤).

القانون والإنترنت -- تنظيم الفضاء الإلكتروني – إدوارد ليليان.