المحاضرة رقم 07:

المبادئ الأخلاقية المرتبطة بمجتمع المعلومات.

-أخلاقيات مجتمع المعلومات.

يذكر موقع اليونيسكو أنه قد:

انبثقت المبادئ الأخلاقية لمجتمعات المعرفة من الإعلان العالمي لحقوق الإنسان وهي تشمل الحق في حرية التعبير وتعميم الانتفاع بالمعلومات، ولا سيما المعلومات المدرجة في النطاق العام، والحق في التعليم، والحق في الخصوصية، والحق في المشاركة في الحياة الثقافية. ويتمحور النقاش الدولي المرتبط بأخلاقيات المعلومات حول الجوانب الأخلاقية والقانونية والاجتماعية للتطبيقات الخاصة بتكنولوجيات المعلومات والاتصالات.

وتتعاون اليونسكو على نحو وثيق مع الدول الأعضاء فيها لدعم الأبعاد الأخلاقية لمجتمع المعلومات وتعزيزها. ويمثل ذلك إحدى أولويات المنظمة في الجهود الشاملة التي تبذلها لتنفيذ قرارات مؤتمر القمة العالمي لمجتمع المعلومات.

ولا يزال الانتفاع الحر والميسّر بالمعلومات المتاحة في الشبكات التفاعلية هدفاً رئيسياً، وهو موضوع يطرح قضايا أخلاقية متعددة تستلزم الكثير من الاهتمام من جانب المجتمع الدولي.

وتوفر التغييرات الناتجة عن التطور السريع لتكنولوجيات المعلومات والاتصالات فرصاً هائلة للبشرية، ولكنها تطرح في الوقت عينه تحديات أخلاقية غير مسبوقة. ويُعد السعي إلى بناء مجتمع المعلومات على أسس الاحترام المتبادل والالتزام بحقوق الإنسان وإنفاذها من أكبر التحديات الأخلاقية في القرن الحادي والعشرين. وفي حين تقدّم التكنولوجيات الرقمية التي أتاحت ترابط أجزاء العالم الكثير من الفوائد، فإنها تنطوي أيضاً على مخاطر سوء الاستعمال والاستغلال.

وبدأت البلدان بوضع آليات لحماية مواطنيها من هذه المخاطر ترمي على سبيل المثال إلى ضمان سلامة الأطفال على شبكة الإنترنت. ومع ذلك، لا يزال الكثير مما ينبغي فعله لمعالجة الآثار الأخلاقية لمجتمع المعلومات.

وتسعى اليونسكو من خلال تعاونها مع شركائها من المؤسسات، وكذلك من خلال برنامج المعلومات للجميع الخاص بها، إلى التصدي لهذه التحديات من أجل بناء مجتمع معلومات يرتكز على مبدأي العدالة والتعدد الثقافي.

المحاضرة رقم 08:

مجتمع المعلومات والثقة الإلكترونية.

أولا/ الأمن المعلوماتي.

إن الثقة الإلكترونية مسألة جد هامة بالنسبة للفرد في المجتمع، بصفته مستفيدا أو مستهلكا أو مستخدما، ذلك أن الإستخدام الدائم يتطلب نوعا من الثقة بالنسبة للفرد، حيث يطرح مسألة الثقة في الشبكة المعلوماتية، يتعلق الأمر بالأمن المعلوماتي. لذلك سنتطرق أولا لماهية الأمن المعلوماتي.

تتعدد تعريفات أمن المعلومات وتتنوع حسب زاوية الرؤية، فنحن إذا نظرنا من زاوية أكاديمية سنجد أنه العلم الذي يبحث في نظريات وإستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها.

ولو نظرنا من زاوية تكنولوجية وفنية بحتة يمكننا تعريفه على أنه (الوسائل والأدوات والإجراءات المطلوب توفيرها

لضمان حماية المعلومات من الأخطار الداخلية والخارجية)، ومن الزاوية القانونية نجد التعريف قد أخذ منحى آخر لكونه يركز على التدابير والإجراءات التى من شأنها حماية سرية وسلامة وخصوصية محتوى وتوفر المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها فى ارتكاب الجريمة المعلوماتية.

وبشكل عام يمكن القول إن أمن المعلومات هو تلك الرؤى والسياسات والإجراءات التى تصمم وتنفذ على مستويات مختلفة، فردية ومؤسسية ومجتمعية، وتستهدف تحقيق عناصر الحماية والصيانة المختلفة التي تضمن أن تتحقق للمعلومات السرية أو الموثوقية، أى التأكد من أن المعلومات لا تُكشف ولا يُطَّلع عليها من قبل أشخاص غير مخولين بذلك. والتكاملية وسلامة المحتوى أى التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله أو العبث به، وبشكل خاص لن يتم تدمير المحتوى أو تغييره أو العبث به فى أية مرحلة من مراحل المعالجة أو التبادل، سواء في مرحلة التعامل الداخلي مع المعلومات، أو عن طريق تدخل غير مشروع. أما الاستمرارية فتعني توفر وإتاحة المعلومات أو الخدمات المبنية عليها لمستخدميها والمستفيدين منها والتأكد من استمرار توفرها والنظم التي تخدمها واستمرار القدرة على التفاعل معها والتأكيد كذلك على أن مستخدمها لن يتعرض إلى منع الاستخدام أو الحيلولة بينه وبين الدخول إليها، كما تعني أيضا ضمان عدم إنكار الشخص الذي قام بتصرف ما متصل بالمعلومات أو مواقعها أنه هو الذي قام بهذا التصرف.

ثانيا/ خصوصية البيانات.

تشكل انتهاكات الخصوصية على الإنترنت مخاطر حقيقية. على سبيل المثال، يمكن مشاركة حالاتك الطبية دون موافقتك، أو يمكن إتاحة بياناتك المصرفية لجهات خارجية. قد تتعرض رسائل بريدك الإلكتروني للاختراق. ومن الممكن سرقة هويتك.

وتوجد مخاطر بعيدة المدى أكثر مما يدرك معظم الناس بسبب ما قد يحدث لبياناتك بعد ذلك. إن تطوير البيانات الضخمة يعني أنه يمكن تحليل سجل التصفح للتوصل إلى استنتاجات لا ترغب في معرفتها. على سبيل المثال، قد لا تتوقع امرأة تشتري بعض العناصر مثل مكملات حمض الفوليك والمرطبات غير المعطرة أن إحدى جهات الاستشارات التسويقية تدرس عمليتها الشرائية أو سجل البحث الخاص بها لتستنتج أنها اكتشفت للتو أنها حامل.

وإذا كانت تعيش مع والدها ووالدتها، أو لم تخبر شريكها، فقد لا تكون سعيدة لتلقي مواد تسويقية عبر البريد بعنوان مثل "تهانينا على طفلك!".

هذا مجرد مثال واحد على كيفية تجاوز مشكلات خصوصية الإنترنت إلى أبعد بكثير وأعمق من مجرد حماية بيانات حسابك المصرفي أو حسابك على مواقع التواصل الاجتماعي. عندما تزور موقعًا إلكترونيًا أو تقوم بتنزيل تطبيق، يتم تخزين البيانات المتعلقة بك، وربما يتم ذلك دون موافقتك وحتى دون علمك. قد ترغب في معرفة مكان ذهاب هذه البيانات وكيفية استخدامها، أو قد تقرر أنك تريد تجنب جمعها تمامًا.

ثالثا/ الثقة الرقمية.

يحقق التحول الرقمي والاتصال فوائد لا جدال فيها، بما في ذلك تحسين الإنتاجية والابتكار والتحديث والنمو الاقتصادي المتسارع والتنمية البشرية المتقدمة.

ونتيجة لذلك أصبح التحول الرقمي أيضًا من أولويات التنمية المستدامة. أصبح الاتصال - كأساس للتحول الرقمي -

سريعًا مطلبًا أساسيًا للجميع. سيحتاج الاتصال الرقمي في النهاية إلى أن يكون موجودًا في كل مكان، وأن يتم تمكينه بواسطة شبكات يمكنها استشعار التغييرات والاحتياجات، مما يوفر مستقبلًا ذكيًا للجميع.

ومع ذلك فإن المزيد من الرقمنة يجلب تحديات جديدة للأمن السيبراني. الأمن والثقة ضروريان أيضًا لضمان الوصول عبر الإنترنت والتبادلات الموثوقة للبيانات والمعلومات. لجني الفوائد الاجتماعية والاقتصادية الهائلة للاتصال، يجب اتخاذ التدابير المناسبة لتعظيم الإمكانات، ويجب بناء الثقة الرقمية، بما في ذلك الثقة في استخدام تكنولوجيا المعلومات والاتصالات وكذلك الثقة بين أصحاب المصلحة للتعاون مع الآخرين.

في الأسواق الناشئة، تكون الثقة الكاملة في الخدمات الرقمية منخفضة في بعض الأحيان لعدة أسباب، بما في ذلك الافتقار إلى المعرفة الرقمية، وثقافة الصحة الإلكترونية في المؤسسات، وانتشار الجرائم الإلكترونية وعمليات الاحتيال. يمكن تحقيق الثقة الرقمية في هذه الأسواق على أفضل وجه من خلال مجموعة متنوعة من التدابير ، بما في ذلك تنفيذ تخزين البيانات وشبكات الاتصال الآمنة، واستخدام أساليب المصادقة القوية وتعزيز محو الأمية الرقمية.