تاثیر امنیت اطلاعات بر اقتصاد اطلاعات

* رضا اردلان
دانشجوی دکترای کتابداری و اطلاع رسانی
واحد علوم و تحقیقات دانشگاه آزاد اسلامی
ardalan@yahoo.com
ardalan.reza@gmail.com

مقدمه

الوین تافلر تمدن بشری را به سه مرحله تقسیم می‌کند که شامل مراحل کشاورزی، صنعتی و فراصنعتی یا عصر ارتباطات و اطلاعات می‌شود و معتقد است که در عصر فراصنعتی، قدرت در دست کسانی است که شبکه‌های ارتباطی و اطلاعاتی را در اختیار خود دارند. (www.bmsu.ac.ir) مک‌لوهان صاحبنظر کانادایی، نیز تاریخ بشر را به سه دوره یعنی؛ عصر تمدن شفاهی، عصر تمدن چاپی و عصر تمدن الکترونیک تقسیم می‌کند و معتقد است در عصر الکترونیک، قدرت در دست صاحبان شبکه‌های تلویزیونی و شبکه‌های رایانه‌ای و ماهواره‌هاست. www.bmsu.ac.ir. اطلاعات درکتابخانه ها، دانشگاه ها، مراکز اطلاع رسانی، سازمان‌ها، مؤسسات پیشرفته و جوامع علمی، بسیار حیاتی است. پس از سازماندهی اطلاعات باید با بهره‌گیری از شبکه‌های رایانه‌ای، زمینه استفاده قانونمند و هدفمند از اطلاعات را برای دیگران فراهم کرد و به موازات حرکت به سمت یک مجموعه اطلاعاتی پیشرفته، باید تدابیر لازم در رابطه با حفاظت از اطلاعات نیز اندیشیده شود. با استفاده از فناوری جدید سوابق سازمانی به سادگی قابل نسخه برداری است که این موضوع بر مولّد بودن کارکنان نیز تاثیر گذار می گذارد.

از طرفی هزینه های پایین دادوستد وافزایش دسترس پذیری می تواند مولد بودن سازمان ها را بهبود بخشد و برعکس امکان نسخه برداری و تقلید محصول مشابه می تواند از مولّد بودن بکاهد.

برای تحقق اندیشه دسترسی آزاد به اطلاعات و همچنین تشویق جریان آزاد اطلاعات از ابعاد علمی، اجتماعی، فرهنگی و انسانی و نیز تقویت بنیان های اقتصادی و اقتصاد اطلاعات، صیانت از اطلاعات با جدیت بیشتری باید در دستور کار قرار گیرد و این موضوع با رویکرد توجه به مبانی و کدهای اخلاقی دسترسی به اطلاعات، همگرایی در رعایت قوانین کپی رایت، مالکیت معنوی و تشکیل کنسرسیوم های چند جانبه بین تولیدکنندگان اطلاعات،

ناشران، تولیدکنندگان پایگاه های اطلاعاتی و اطلاعات دیجیتال ، مشارکت دانشگاه ها و مراکز تحقیقاتی در پروژه های تولید اطلاعات و تصویب قوانین مترقی در مجلس قانونگذاری و از همه مهمتر آموزش مستمر قوانین تمامی مقاطع آموزشی می تواند در میان مدت و بلند مدت مؤثر باشد.

اگر بخواهیم در عصر اطلاعات ارایه دهنده اطلاعات و نه مصرف‌کننده صرف باشیم، باید امکان استفاده از اطلاعات بومی را برای مصرف کنندگان محلی و جهانی با هزینه هایی مناسب در سریع‌ترین زمان فراهم نماییم و با ورود به قانون تجارت جهانی و پذیرش نقشی فعال در فرآیند جهانی سازی جایگاه اطلاع رسانی و اطلاعات بومی را در جایگاه مطلوبی قرار دهیم تا با دیگر کشورها در چرخه رقابت و تولید قرار گیریم.

سیاست های حمایتی از اطلاعات یا به عبارتی حفظ امنیت اطلاعات می تواند تکنولوژیکی و یا معنوی باشد. حمایت های معنوی از اطلاعات پیامدهایی را بدنبال دارد، از جمله نارسایی بازار و انحصارگری یا مالکیت صرف که در این مقاله به آن پرداخته شده است.

امنیت اطلاعات (Information security)

«امنیت اطلاعات» به حفاظت از اطلاعات و به حداقل رساندن خطر افشای اطلاعات در بخش های غیرمجاز اشاره دارد. امنیت اطلاعات مجموعه‌ای از ابزارها برای جلوگیری از سرقت، حمله، جنایت، جاسوسی و خرابکاری و علم مطالعه روش‌های حفاظت از داده‌ها در رایانه‌ها و نظام‌های ارتباطی در برابر دسترسی و تغییرات غیرمجاز است. بنابراین می توان سیاست های راهبردی انتخاب شده را بر سه محور حفاظت، تشخیص، و واکنش استوار نمود. حفاظت مطمئن، تشخیص بموقع و واکنش مناسب، از جمله مواردی هستند که باید همواره در ایجاد یک نظام امنیتی رعایت گردد.

فناوری‌های اطلاعاتی و ارتباطی از بدو ایجاد تاکنون، با تغییرات مواجه بوده و برای روند کلی آن ها معمولاً از سه دوره به عنوان دوران تغییر، تحول و تکامل فناوری‌های اطلاعاتی نام برده می‌شود: (صدوقی، ۱۳۸۰، ص٥٦)

۱.عصر سیستم‌محوری (۱۹۸۱ – ۱۹٦٤)، دوره پدیدآمدن سامانه‌ها و فرایندهای سیستمی؛

۲.عصر P.C محوری (۱۹۹٤ – ۱۹۸۱)، دوره ظهور رایانه‌های شخصی.

۳.عصر شبکه‌محوری (۱۹۹٤تاکنون)، دوره یکپارچه‌سازی ارتباطات و اطلاعات.

عکس العمل لازم در برابر یک مشکل امنیتی می تواند کنشی(Proactive) یا واکنشی (Reactive) باشد. منظور از کنش، انجام عملیات پیشگیرانه قبل از وقوع یک مشکل خاص امنیتی است. پیشگیری از وقوع یک مشکل خواه از نوع کنشی یا واکنشی، می‌تواند در سه سطح شبکه(Network Level)، سطح میزبان(Host Level)، سطح برنامه کاربردی(Application Level) پیاده‌سازی گردد.

الف. فناوری‌های امنیت اطلاعات کنشی

۱. رمزنگاری (Cryptography)

به بیان ساده، رمزنگاری به معنای «نوشتن پنهان»، و علم حفاظت، اعتمادپذیری و تأمین تمامیت داده‌ها است . این علم شامل اعمال رمزگذاری، رمزگشایی و تحلیل رمز است. در اصطلاحات رمزنگاری، پیام را «متن آشکار» می‌نامند. کدگذاری مضامین را به شیوه‌ای که آن‌ها را از دید بیگانگان پنهان سازد، «رمزگذاری یا «سِرگذاری» می‌نامند . رمزنگاری با تمام جوانب پیام‌رسانی امن، تعیین اعتبار، امضاهای رقومی، پول الکترونیکی و نرم افزارهای کاربردی دیگر ارتباط دارد.

۲. امضاهای رقومی (Digital signatures)

امضاهای رقومی، معادل «امضای دست‌نوشت» و مبتنی بر همان هدف هستند: نشانه منحصر به فرد یک شخص، با یک بدنه متنی. به این ترتیب، امضای رقومی مانند امضای دست‌نوشت، نباید قابل جعل باشد. این فناوری که با استفاده از الگوریتم رمزنگاری ایجاد می‌شود، تصدیق رمزگذاری‌شده‌ای است که معمولاً به یک پیام پست الکترونیکی یا یک گواهی‌نامه ضمیمه می‌شود تا هویت واقعی تولیدکننده پیام را تأیید کند.

۳. گواهی‌های رقومی(Digital certificates)

گواهی‌های رقومی به حل مسئله «اطمینان» در اینترنت کمک

می‌کنند. متصدی‌های گواهی، مؤسسات تجاری هستند که هویت افراد یا سازمان‌ها را در وب تأیید و تأییدیه‌هایی مبنی بر درستی این هویت‌ها صادر می‌کنند. برای به دست‌آوردن یک گواهی، ممکن است از فرد خواسته شود که یک کارت شناسایی مانند گواهینامه رانندگی را نشان دهد.

بنابراین گواهی‌های رقومی، یک شبکه امن در میان کاربران وب و مکانی برای تأیید صحت و جامعیت یک فایل یا برنامه الکترونیکی ایجاد می‌کنند. این گواهی‌ها حاوی نام فرد، شماره سریال، تاریخ انقضاء، یک نسخه از گواهی نگاهدارنده کلید عمومی (که برای رمزگذاری پیام‌ها و امضاهای رقومی به کار می‌رود) ، می‌باشند (Encyclopedia and learning center، 2004).

٤. شبکه‌های مجازی خصوصی(Virtual private networks)

فناوری شبکه‌های مجازی خصوصی، عبور و مرور شبکه را رمزگذاری می‌کند.

بنابراین این فناوری برای تضمین صحت وامنیت داده‌ها به رمزنگاری وابسته است. این شبکه بسیارامن، برای انتقال داده‌های حساس (از جمله اطلاعات تجاری الکترونیکی) از اینترنت به عنوان رسانه انتقال بهره می‌گیرد.

شبکه‌های مجازی خصوصی، فناوری امنیت اطلاعات از نوع کنشگرایانه هستند، زیرا داده‌ها قبل از آن که در شبکه عمومی منتشر شوند، با رمزگذاری محافظت می‌شوند و این امر باعث می‌گردد که تنها افراد مجاز قادر به خواندن اطلاعات باشند.

۵. نرم‌افزارهای آسیب‌نما (Vulnerability scanners)

نرم‌افزارهای آسیب‌نما برنامه‌هایی برای بررسی نقاط ضعف یک شبکه یا سیستم یا سایت هستند.

بنابراین نرم‌افزارهای آسیب‌نما یک نمونه خاص از نظام آشکارساز نفوذی از فناوری امنیت اطلاعات هستند.

همچنین این نرم‌افزارها به یک پویش فاصله‌مدار اشاره دارند؛ بدین معنا که میزبان‌های روی شبکه را در فواصل خاص و نه بطور پیوسته، پویش می‌کنند. به مجرد این که یک نرم‌افزار آسیب‌نما بررسی یک میزبان را خاتمه داد، داده‌ها در درون یک گزارش، نمونه‌برداری می‌شوند.

٦. پویشگرهای ضد ویروس(Anti- virus scanner)

ویروس رایانه‌ای یک قطعه مخرب نرم‌افزاری است که توانایی تکثیر خودش را در سراسر اینترنت، با یک بار فعال‌شدن دارد. پویشگرهای ضد ویروس، برنامه‌های نرم‌افزاری هستند که برای بررسی و حذف ویروس‌های رایانه‌ای، از حافظه یا دیسک‌ها طراحی شده‌اند.

این برنامه‌ها از طریق جستجوی کدهای ویروس رایانه‌ای، آن‌ها را تشخیص می‌دهند. اگرچه برنامه‌های حفاظت از ویروس نمی‌توانند تمام ویروس‌ها را نابود کنند، اما اعمالی که این برنامه‌ها انجام می‌دهند عبارت‌اند از:۱) ممانعت از فعالیت ویروس،۲) حذف ویروس،۳) تعمیر آسیبی که ویروس عامل آن بوده است، و٤) گرفتن ویروس در زمان کنترل و بعداز فعال‌شدن آن.

۷. پروتکل‌های امنیتی(Security protocols)

پروتکل‌های امنیتی مختلف مانند «پروتکل امنیت اینترنت» (Internet Protocol Security IPsec) و«کربروس» (kerberos) که در فناوری‌های امنیت اطلاعات طبقه‌بندی می‌شوند، وجود دارند.

پروتکل‌ها فناوری‌هایی هستند که از یک روش استاندارد برای انتقال منظم داده‌ها بین رایانه‌ها استفاده می‌کنند، یا مجموعه‌ای از مقررات یا قراردادها هستند که تبادل اطلاعات را میان نظام‌های رایانه‌ای، کنترل و هدایت می‌کنند.

۸ . سخت افزارهای امنیتی(Security hardware)

سخت افزار امنیتی به ابزارهای فیزیکی که کاربرد امنیتی دارند، اشاره می‌کند.

مانند معیارهای رمزگذاری سخت‌افزاری یا مسیریاب‌های سخت افزاری. ابزارهای امنیت فیزیکی شامل امنیت سرورها، امنیت کابل‌ها، سیستم‌های هشدار دهنده امنیتی در زمان دسترسی غیرمجاز یا ذخیره فایل‌ها بعد از استفاده یا گرفتن فایل پشتیبان هستند.

این فناوری یک فناوری امنیت اطلاعات از نوع کنشگرایانه است. مثلاً از رمزگذاری داده‌ها به‌منظور جلوگیری از اعمال خرابکارانه و جرح و تعدیل ابزار سخت‌افزاری استفاده می‌شود. این فناوری در سطح شبکه قابل پیاده‌سازی است.

مثلاً یک قفل سخت‌افزاری می‌تواند در درون درگاه میزبان برای تعیین اعتبار کاربر، قبل از آن که کاربر بتواند به میزبان متصل شود، به کار رود.

۹. جعبه‌های توسعه نرم‌افزار امنیتی
Security software development kits (SD Ks)

جعبه‌های توسعه نرم‌افزار امنیتی، ابزارهای برنامه‌نویسی هستند که در ایجاد برنامه‌های امنیتی مورد استفاده قرار می‌گیرند.

«Java security manager» و «Microsoft.net SDKs» نمونهٔ نرم‌افزارهایی هستند که در ساختن برنامه‌های کاربردی امنیتی (مانند برنامه‌های تعیین اعتبار مبتنی بر وب) به کار می‌روند. این جعبه‌ها شامل سازنده صفحه تصویری، یک ویراستار، یک مترجم، یک پیوند دهنده و امکانات دیگر هستند.

ب. فناوری‌های امنیت اطلاعات واکنشی

۱. دیوار آتش(Firewalls)

در اینترنت یک ابزار نرم‌افزاری، خصوصاً روی یک رایانه پیکربندی‌شده می‌باشد که به عنوان مانع، فیلتر یا گلوگاه بین یک سازمان داخلی یا شبکه امین و شبکه غیرامین یا اینترنت، نصب می‌شود. هدف از دیوار آتش جلوگیری از ارتباطات غیرمجاز در درون یا بیرون شبکه داخلی سازمان یا میزبان است . دیوار آتش بین نظام‌های سازمان و اینترنت قرار می‌گیرد و مهم‌ترین ابزار امنیتی مورد استفاده برای کنترل ارتباطات شبکه‌ای بین دو سازمان که به یکدیگر اعتماد ندارند، می‌باشد.

۲.کلمات عبور(passwords)

کلمه عبور، یک کلمه، عبارت یا حروف متوالی رمزی است که فرد برای به‌دست آوردن جواز دسترسی به اطلاعات مثلاً یک فایل، برنامه کاربردی یا نظام رایانه‌ای باید وارد نماید. این کلمه برای شناسایی و برای اهداف امنیتی در یک نظام رایانه‌ای به کار می‌رود. به هر کاربر مجموعه معینی از الفبا و عدد اختصاص داده می‌شود تا به تمام یا قسمت‌هایی از نظام رایانه‌ای دسترسی داشته باشد.

۳. زیست‌سنجی(Biometrics)

زیست‌سنجی، علم و فناوری سنجش و تحلیل داده‌های زیستی است. در فناوری اطلاعات، زیست‌سنجی معمولاً به فناوری‌هایی برای سنجش و تحلیل ویژگی‌های بدن انسان (مانند:اثرانگشت، قرنیه و شبکیه چشم، الگوهای صدا، الگوهای چهره واندازه‌های دست) خصوصاً به‌منظور تعیین اعتبار اشاره دارد.یکی از ویژگی‌های ذاتی علم زیست‌سنجی این است که کاربر باید با یک الگوی مرجع مقایسه شود.

اثرانگشت، چهره یا داده‌های زیست‌سنجی دیگر را می‌توان جایگزین کارت هوشمند نمود.

٤. نظام‌های آشکارساز نفوذی (Intrusion detection systems (IDS)

نظام‌های آشکارساز نفوذی، یک نظام تدافعی است که فعالیت‌های خصمانه را در یک شبکه تشخیص می‌دهد. بنابراین نکته کلیدی در نظام‌های آشکارساز نفوذی، تشخیص و احتمالاً ممانعت از فعالیت‌هایی است که ممکن است امنیت شبکه را به خطر بیندازند. یکی از ویژگی‌های مهم این نظام‌ها، توانایی آن‌ها در تأمین نمایی از فعالیت‌های غیرعادی، و اعلام هشدار به مدیران نظام‌ها و مسدود نمودن ارتباط مشکوک است.

۵. واقعه‌نگاری(logging)

واقعه‌نگاری به ثبت اعمال یا تراکنش‌های انجام‌شده توسط کاربر یا یک برنامه، تولید سابقه و ثبت نظام‌مند رویدادهای مشخص به ترتیب وقوع آن‌ها برای فراهم‌کردن امکان تعقیب و پیگیری داده‌ها در تحلیل‌های آتی اطلاق می‌شود. واقعه‌نگاری، فناوری امنیت اطلاعات از نوع واکنشی است، زیرا به علت‌جویی حوادث امنیتی بعد از وقوع می‌پردازد.

٦. دسترسی از راه دور(Remot accessing)

«دسترسی از راه دور» به دسترسی به یک سیستم یا برنامه، بدون نیاز به حضور فیزیکی در محل توجه دارد. با این حال معمولاً دسترسی به خدمات از راه دور، کنترل‌شده نیستند، زیرا ممکن است دسترسی به یک خدمت از راه دور به طور ناشناس صورت بگیرد که در این مورد دسترسی به خدمت، خطر جعل هویت را به همراه دارد. در این زمینه با توجه به شرایط و امکانات، باید ایمن‌ترین پروتکل‌ها و فناوری‌ها را به خدمت گرفت.

اقتصاد اطلاعات

اصطلاح اقتصاد اطلاعات در ادبیات اقتصاد دانان در دهه ۱۹٦۰ ظاهر شد که علم مطالعه و بررسی تولید، توزیع، بازاریابی، قیمت گذاری، فروش، مصرف و کلیه درآمدهایی است که به طور مستقیم یا غیر مستقیم از طریق تولید، انتشار، فروش، ذخیره، پردازش و دسترسی به اطلاعات حاصل می شود .اقتصاد دیجیتال و یا اقتصاد اینترنت را می توان به عنوان اولین معیار و وسیله پیشرفت اقتصادی نام برد که ناشی از تحولات اجتماعی و اقتصادی از سال ۱۹٦۰ به بعد می باشد.

هر چند آدام اسمیت (۱۷۷٦) پدر اقتصاد نوین به اهمیت اطلاعات در تولید و گردش امور بازار مطلع بود و طبقه ای از متخصصان که دارای آینده نگری هستند و با تولید دانشی که به لحاظ اقتصادی مفید است و به رشد اقتصادی کمک می کنند را نام می برد(آگوستین،۲۰۰۵).

جریان گذار اقتصاد و سیر تحولات آن، شامل حرکت از حالت اولیه و سنتی بشر یعنی اقتصاد متکی به کشاورزی به اقتصاد صنعت محور و سپس رسیدن به حالت فعلی یعنی اقتصاد اطلاعات محور است.

این تحولات زمینه را برای شکل گیری افکار و اندیشه ها و زمینه های مختلفی در کسب و کار فراهم کرد و حتی در ادبیات اقتصاد جهانی نیز تغییرات قابل ملاحظه ای را با عباراتی همچون: صنعت اطلاعات، بازار اطلاعات، کارکنان اطلاعات موجب شده است.

در بحث نوین «اقتصاد اطلاعات»، واژه ی اطلاعات در گسترده ترین و در عین حال تخصصی ترین شکل خود مورد استفاده قرار می گیرد و آن عبارت است از هر چیزی که بتواند رقمی (دیجیتال) گردد و در قالب هایی از صفر و یک کدبندی شود.

نتایج مسابقات فوتبال، کتاب ها، بانک های اطلاعاتی، مجلات، فیلم ها، موزیک، نرخ سهام در بورس و بالاخره صفحات وب، همه کالاهای اطلاعاتی به حساب می آیند.

کارشناسان اطلاعات همه به این نکته عقیده دارند که مصرف کنندگان مختلف به یک پدیده ی اطلاعاتی، ارزش های بسیار متفاوتی می دهند.

افراد از لحاظ نوع استفاده، قابلیت استفاده، میل به استفاده، ارزیابی هزینه‌های استفاده و توانایی پرداخت بهای استفاده از اطلاعات، با هم تفاوت دارند. به عبارت دیگر همگان آماده یا مایل نیستند هر بهایی را برای یک کالای اطلاعاتی بپردازند.

ناشران کتاب غالباً برای سودآوری، متکی به منابع درآمد فرعی هستند؛ مجلات علمی تا حد زیادی به حق اشتراک متکی هستند؛ انتشارات دانشگاهی تقریباً در تمام جهان از یارانه بهره‌مندند و این سیاست حتی در بین ناشران انتفاعی و ناشران غیر انتفاعی در غرب، همانند آکسفورد و کمبریج و انتشارات دانشگاه شیکاگو، نیز به چشم می خورد؛ روزنامه‌ها و مجلات تقریباً به‌صورت کامل تحت حمایت تبلیغات همه جانبه قرار گرفته اند.

البته موفقیت‌های کتاب های پرفروش مانند هری پاتر، فیلم‌های اسکار و سریال‌های تلویزیونی بین المللی که جوایزی نیزگرفته‌اند، وجود دارد.

تولید کنندگان نرم افزارهای رایانه ای، پایگاه های اطلاعاتی، کتاب های دیجیتال، پایگاه مقالات و انواع مواد دیداری و شنیداری در برابر مصرف کنندگان بالقوه یا بالفعل خود از فرمول های اقتصادی و نظریات عرضه و تقاضا استفاده می کنند، البته گاهی ریسک می کنند و مهمتر اینکه همیشه بازندگانی نیز می‌توان یافت.

با تمام این اوصاف دسترسی به اطلاعات در حال حاضر هم در ایران که قوانین حق مولف را نپذیرفته یا در کشورهایی که مدتهاست به آن پایبندند و در مسیر درست حرکت می کنند، با تهدیدهای مثبت و منفی مواجه است. لازمه درک صحیح و بهره گیری بهینه اطلاعات شناخت حقوق فردی، حقوق گروهی و رعایت کدهای اخلاقی است که ابتدا بایستی با موانع جریان آزاد اطلاعات آشنا شویم.

موانع جریان آزاد اطلاعات

مهمترین موانع جریان آزاد اطلاعات به قرار زیر است:

۱. انفجار اطلاعات: حجم سرسام آور اطلاعات مشکلات متعددی در امر انتخاب، گردآوری، آماده سازی و اشاعه اطلاعات به وجود آورده است.

۲. زبان: قابل انتقال است و از آن جا که زبان عاملی برای تبادل دانش است، می تواند هم دانش فردی و هم دانش گروهی را شکل دهد. انتشار نتایج تحقیقات به زبان های مختلف صورت می پذیرد. حقیقت کاملاً آشکار این است که ملت های جهان هر یک بر زبان ملی خود تأکید می ورزند.

۳. آلودگی اطلاعات: کیفیت اطلاعات بستگی به میزان بصیرت و آگاهی تولید کنندگان و مصرف کنندگان آن دارد. اندازه گیری و کنترل کیفیت اطلاعات و دانش کاری دشوار و البته عملی است. گرچه ایجاد نظام داوری برای تعیین کیفیت و اعتبار اطلاعات امری ضروری است، اما مشکل اصلی حجم زیاد اطلاعات است.

٤. محدودیت های مالی: ارزش اقتصادی اطلاعات و پدیده افزایش قیمت مدارک، حتی کشورهای ثروتمند را با محدودیت هایی در تهیه و تحویل مدارک مواجه ساخته است. فقدان منابع مالی در کشورهای در حال توسعه و توسعه نیافته، برنامه اطلاع رسانی و اشاعه اطلاعات را توسط کتابخانه ها و مراکز اطلاع رسانی تحت تأثیر قرار داده است. هزینه های مستقیم و غیرمستقیم منابع کتابخانه ای، به طور مداوم در حال افزایش است. بنابر این، بسیاری از مدارک سودمند در دسترس جامعه استفاده کننده، قرار نمی گیرند و به همین علت است که امنیت اطلاعات با نیاز شدید مصرف کنندگان اطلاعات از سویی به خطر می افتد و این پدیده هم در کشورهای

توسعه یافته و هم درکشورهای در حال توسعه روی می دهد. البته توان اقتصادی شهروندان نیز از اهمیت بالایی برخوردار است. همه انواع اطلاعات در اشکال متنوع شامل فضاهای دیجیتالی و بسته های نرم افزاری و نمونه های چاپی از این معضل متأثر هستند.

۵. زمان: به دلیل رشد سریع اطلاعات و شکل گیری آن در قالب انواع مدارک، قدرت کنترل کتابشناختی کمتر و یا با دشواری مواجه شده است. بین زمان انتشار، پردازش، جست و جو، دسترسی و بازخورد، خلأ و فاصله زمانی زیادی وجود دارد. در جوامع اطلاعاتی تأخیر زمانی ارزش اطلاعات را کاهش داده و از جریان آزاد اطلاعات جلوگیری می کند.

٦. اطلاعات رایانه ای شده: تمام بهره گیران با شیوه های عرضه اطلاعات رایانه ای شده، آشنا نیستند و این مانعی در راه آزادی اطلاعات محسوب می گردد. اشاعه اطلاعات از طریق اینترنت و همچنین اطلاعات رایانه ای شده، موجب استفاده بدون ضابطه از اطلاعات نویسندگان دیگر گردیده است .

***

علاوه بر اصول فوق، اصول نه گانه اعلامیه جهانی حقوق بشر به سال ۱۹۹۹، معیارهایی برای تدوین قانون حق دسترسی به اطلاعات از سوی دولت ها تدوین و پیش بینی شده است که به شرح زیر است:

اصل ششم. هزینه ها: هزینه های سنگین نباید مانع درخواست دسترسی به اطلاعات شود. از آن جا که هدف قانون آزادی اطلاعات، تقویت دسترسی باز به اطلاعات است، بنابراین هزینه هایی که از سوی نهاد دولتی برای در اختیار نهادن اطلاعات تعیین می شود، نباید چندان زیاد باشد که درخواست کنندگان بالقوه را از رسیدن به این حق باز دارد؛ به ویژه که منافع بلند مدت آزادی اطلاعات برای جامعه از هزینه های تحقیق به مراتب بیشتر است.

با واقعیت های موجود جوامع بشری، اصل مورد نظر بیشتر حالت نمایشی دارد تا عملی و عملگرایانه.

امنیت اطلاعات موضوعی چند بُعدی است که با جنبه‌های غیرفنی متعددی ارتباط دارد. همواره برای تحقق امنیت، ابزارهای فیزیکی، پرسنلی و اجرایی لازم‌اند و ابزارهای فنی به‌تنهایی بی فایده‌اند. اگر چه اغلب سازمان‌ها تمایل به داشتن شبکه‌های ایمن دارند، ارائه تعریفی واحد از امنیت که همه نیازهای شبکه را تأمین نماید، ممکن نیست. در عوض هر سازمان باید ارزش اطلاعات خود را ارزیابی کند و سپس یک خط مشی امنیتی برای مواردی که باید مورد حفاظت قرار گیرند، مشخص نماید. مثلاً روش‌های تعیین اعتبار زیست‌سنجی از نظر قدرت و در دسترس بودن، در حال بهبود هستند، اما در حال حاضر با نوعی تردید با آن‌ها برخورد می‌شود و این تردید ناشی از هزینه‌های نسبتاً بالا و مشکلات مرتبط با دغدغه‌های حفظ حریم خصوصی می‌باشد. البته نظراتی وجود دارند که به موجب آن‌ها می‌توان از ترکیب فناوری‌های متنوع امنیتی، برای تشکیل فناوری‌های امنیتی قوی در زمینه امنیت اطلاعات استفاده نمود. برای یک سازمان، شناختن فناوری‌های امنیت اطلاعات قابل دسترس مهم است تا از آن برای تدوین خط‌مشی‌های امنیتی با توجه

به نوع و حساسیت اطلاعات سازمان خود ، استفاده نمایند. به علاوه، ارائه این طبقه‌بندی از فناوری‌ها، زمینه‌ساز پژوهش جدیدی خواهد بود. البته تهدید امنیت اطلاعات علاوه بر روش های پیش گفته، از طریق دستکاری اطلاعات نیز میسر است.

یکی از مصادیق تهدید امنیت اطلاعات، دستکاری منبع معروف و پرطرفدار دانشنامه‌ی اینترنتی «ویکی پدیا» است. البته نرم‌افزارهایی وجود دارند که تشخیص می‌دهند آیا یک گروه از واژه‌ها از یک متن اینترنتی کپی‌برداری شده‌اند یا خیر. ده ها نسخه از این نرم‌افزارها در دانشگاه های اروپا نصب شده است، اما از نظر کارشناسان کارآیی چندانی ندارند.مثلاً متن‌هایی وجود دارند که از اینترنت ترجمه یا از بانک‌های اطلاعاتی خریداری شده‌اند.

نرم‌افزارهای رایانه‌ای از تشخیص چنین متن‌هایی عاجزند. کارشناسان بهترین راه‌حل برای مبارزه با سرقت‌ادبی را تشکیل کمیسیون‌های ویژه‌ای با همکاری نزدیک دانشگاه‌ها می‌دانند. در برخی کشورها برای مقابله با این مسأله، جریمه و مجازات های قانونی پیش بینی شده است.

نتیجه گیری:

در دنیای امروز، وابستگی ما به سیستم‌های اطلاعاتی طوری است که دستکاری غیرمجاز یا فقدان گسترده‌ی اطلاعات، پیامدهای ناخوشایندی را موجب خواهد شد. در زمینه های الکترونیکی، لازم است که همه‌ی انواع اطلاعات از طریق شبکه دسترس‌پذیر باشند. بنابراین، امنیت اطلاعات شرط ضروری فعالیت های الکترونیکی است.

امنیت و قابلیت استفاده، از اصول متضاد باهم هستند. وقتی که سیستم‌ها را امن‌تر می‌کنیم، طبعاً از قابلیت استفاده‌ی آن‌ها می‌کاهیم. کارالکترونیکی چیزی است که باید در شرایط مربوط به کاربر عادی هم عمل کند، یعنی برای هر کسی قابل استفاده باشد. ترکیب قابلیت استفاده با امنیت، چالش اصلی عصر ما است. اصول فنی برای انجام کارهای الکترونیکی امن، در حال شکل‌گرفتن است و جنبه‌های شبکه‌ای امنیت را می‌توان حل کرد. اما وقتی که با افراد و با جریان‌های پیچیده‌ی اطلاعات سروکار داریم، هیچ راه‌حل استانداردی برای امنیت کل سیستم وجود ندارد.

باید سازوکارهای استاندارد به‌کار گرفته شوند تا اطمینان حاصل شود که سیستم‌های اطلاعاتی مورد استفاده، امنیت جریان‌های اطلاعاتی را به خطر نمی‌اندازند.

هیچ روش شناخته‌شده‌ای برای اثبات امنیت کل فرایندها وجود ندارد. باید بطور مداوم به نظارت و به بازخورد دادن به فرایندهایمان بپردازیم. ضعیف‌ترین نقطه در موضوع امنیت، همچنان افراد و نگرش‌های آن‌ها خواهد بود.

مدت‌ها است که علت اصلی در شکستن امنیت اطلاعات، رفتار غیرمجاز افراد غیرموجه در کارهای روزمره است.

امنیت را باید تعریف، طراحی، و در فرایندهای کاری تعبیه کرد. افراد باید به خوبی راهنمایی شوند، آموزش ببینند و انگیزه‌مند شوند.

کاهش سرانه‌ی قیمت محصولات اطلاعاتی و حمایت رایانه ای دولت ها از دسترسی آزاد به اطلاعات در کشورهای در حال توسعه و ایران، اشاعه، گسترش و تقویت مجلات و مقالات دسترسی آزاد و قرار دادن اطلاعات و مقالات محققان در وب سایت های شخصی برای دسترسی ساده تر با رعایت حقوق مؤلف و ناشر می تواند عملاً بازدهی علمی و پژوهشی را افزایش و به سوی موفقیت سوق دهد.

اگر منابع دسترسی آزاد ، جابجایی‌پذیری ، تنوع زبانی به دسترسی اطلاعات و کیفیت خدمات محور اصلی اقتصاد اطلاعات باشد، در آن صورت یک تفاهم بین المللی بوجود خواهد آمد تا آینده پیشرفت های علمی را بر آن استوار کنیم و با عقلانیت و خرد بیشتری امکان بهره برداری مشترک از اطلاعات بشری بر موفقیت ها و پیشرفت ها بیفزاییم.

منابع و ماخذ:

۱. دایره المعارف کتابداری و اطلاع رسانی. تهران: کتابخانه ملی جمهوری اسلامی ایران، ۱۳۸۱.
۲. شهیدی، محمدمهدی(۱۳۸۳). « آزادی اطلاعات: حق بنیادی بشر در هزاره جدید». وب ، ۵ (۵۱): ۵-۱۰.
۳. نمک دوست تهرانی، حسن (۱۳۸۲). « حق دسترسی به اطلاعات: بنیان ها، روند جهانی و جایگاه ایران». رسانه، ۱٤ (۱): ٦٦-۵۰.
٤. داورپناه، محمدرضا و آرمیده، معصومه .اطلاعات و جامعه. تهران: دبیزش. (۱۳۸٤).
۵. هیل، ملیکل (۱۳۸۱). تاثیر اطلاعات بر جامعه: بررسی ماهیت، ارزش و کاربرد اطلاعات. تهران: چاپار.
٦. علیرضا نوروزی. « آلودگی اطلاعات». فصلنامه اطلاع رسانی. دوره ۱۵، شماره ۱و ۲

7. Catherine Ayre and Adrienne Muir, “Right to Preserve? Copyright and Licensing for Digital Preservation Project Final Report,”(Loughborough: LoughboroughUniversity,2004.(http://www.lboro.ac.uk/departments/dils/disresearch/CLDP/ roject_reports.htm (accessed January 10, 2007).

8. Kate O’Donohue, “The Accessing and Archiving of Electronic Journals: Challenges and Implications within the Library World”The Serials Librarian 49, no. 1–2 (2005): 35–87.

9. http://www.elsevier.nl/ (Accessed January 05, 2007).

10. Galyani Moghaddam, Golnessa. “Scholarly Electronic Journal Publishing: A Study Comparing Commercial and Nonprofit/ University Publishers,” The Serials Librarian 51, no. 3/4 (2006): (177-195) .

11. http://www.persianhack.com/show.aspxid=682(accessed Dec 8 ,2007)