

قوانین حقوقی و امنیتی در حوزه فناوری اطلاعات

قوانین حقوقی و امنیتی در حوزه فناوری اطلاعات

چه بخواهیم و چه نخواهیم، فناوری های نونی اطلاعاتی به زندگی فردی و اجتماعی ما راه پیدا کرده اند. هرروزه ما شاهد ظهور فناوری هایی هستیم که قبلا آن ها را در رویاهای خود تصور می کردیم. فناوری های که در طی چند دهه توانسته اند رفتار و کردار بشر را تغییر داده و متحول نمایند. یکی از دستاوردهای مهم انقلاب فناوری اطلاعات، ذخیره سازی و نگهداری اطلاعات جمع آوری شده از سوی فرد، سازمان و یا حتی دولت بوده تا بتوانند در سازمان مورد نیاز از این اطلاعات استفاده بجا نمایند. ولی از سوی دیگر یکی از معضلات بزرگ این عصر، استفاده های غیرمجاز از اطلاعات ذخیره شده است.

شبکه های کامپیوتری و اینترنت، از جمله فناوری هایی هستند که باعث به وجود آمدن انقلابی در سیر پیشرفت بیشتر بوده ولی در کنار این توسعه، مشکلاتی را نیز به وجود آورده اند که از عمده این مشکلات امنیت اطلاعاتی می باشد. اطلاعاتی را که قصد داریم از یک نقطه به نقطه دیگری از طریق اینترنت انتقال دهیم، از چندین کامپیوتر موجود در ISP ها عبور کرده تا به مقصد منتقل شود. در این نقل و انتقالات اطلاعاتی ممکن است سوء استفاده ای صورت گیرد و دسترسی غیرمجازی به اطلاعات شما انجام پذیرد.

خیلی از نرم افزارهایی که در داخل کشورمان استفاده می نماییم، تحت قانون کپی رایت هستند. قانونی که اجازه استفاده رایگان به شخص را از نرم افزار نمی دهد ولی ما به راحتی این نرم افزارها را کپی و تکثیر می نماییم. حتی نرم افزارهایی که در داخل کشور و توسط شرکت های ایرانی تولید گشته اند. این موضوع و موضوعات مشابه آن باعث شده است که خسارات و لطمه های بزرگی به صنعت فناوری اطلاعات وارد آمده و جوامع را به سمت این تفکر سوق دهد که برای کنترل حوزه های مختلف فناوری اطلاعات و بالا بردن امنیت آن، قوانین و مقرراتی را وضع نمایند.

فراهم شدن فناوری های نوین اطلاعاتی تنها باعث پیدایش محصولات نوین و راه های بهتر و کارآمدتر برای انجام امور نشده، بلکه در کنار آن سوء استفاده از فناوری را نیز افزایش داده است. فناوری اطلاعات نیز همانند سایر فناوری ها حالت ابزاری دارد و می توان آن را به گونه ای مورد استفاده قرار داد که برای همگان مفید واقع شود و یا به نحوی از آن استفاده کرد که نتایج خطرناکی به بار آورد. عامل سرعت، یکی از عوامل مهم و تاثیرگذار در صنعت فناوری اطلاعات است که باعث می شود اطلاعات غیر قابل مشاهده و با چشم غیر مسلح، تحت کنترل نرم افزار تهیه شده و توسط افراد جابجا گردد. در چنین فضایی، اعمال غیر قانونی و مخرب آنقدر سریع صورت می گیرد که سوء استفاده گر آن می تواند غیر قابل شناسایی باشد.

اینجاست که قانون و بالاتر از آن اخلاق و فرهنگ صحیح استفاده از صنعت فناوری اطلاعات باعث جلوگیری از سوء استفاده های اطلاعاتی می شود. اگر خوب دقت کنیم متوجه می شویم که قانونمندی و قانون مداری در صنعت فناوری اطلاعات را می توان از سه حوزه مورد بررسی قرار داد.

□ حوزه اخلاقی و فردی

□ حوزه اجتماعی و سازمانی

□ حوزه دولتی و حقوقی

همان طور که می دانید، دسترسی غیر مجاز به اطلاعات دیگران، امروزه به عنوان یک سرگرمی محسوب می شود. حتی تازه واردین به دنیای فناوری اطلاعات دوست دارند که با روش های هک کردن آشنا شده و به اطلاعات فردی و حریم خصوصی افراد وارد شوند. تنها عاملی که می تواند به طور موثر مانع از این عمل گردد، اخلاق و اصول اخلاقی است. عموماً اصول اخلاقی و ایجاد فرهنگ استفاده صحیح از فناوری های مدرن است که می تواند این نوع سوء استفاده های فردی را کنترل نماید تا دیگران به خود اجازه ندهند که از اطلاعات فردی دیگران استفاده نمایند.

در یک سطح بالاتر حوزه اجتماعی در استفاده از فناوری های نوین اطلاعاتی مطرح می باشد. این حوزه می بایست ارزش های که در سطح جامعه حاکم می باشد را مطرح نموده تا بدین طریق حفظ حقوق اطلاعات فردی، رعایت شود. در سازمان های کوچک، شرایط تامین امنیت اطلاعات ممکن است ساده باشد و هر کس مسیولیت رایانه ها و فایل های خود را برعهده داشته باشد. در صورتی که گروه های بزرگ تر مثل سازمان های موجود در یک اجتماع که با عملیات تجاری سروکار دارند و یا گروه هایی که از داده های محرمانه شهروندان و مشتریان نگهداری می کنند، نیاز به ایجاد سیاست ها و روال های رسمی امنیتی بیشتر اهمیت پیدا می کند. هنگامی که مدیران و کارمندان موضوع امنیت فناوری اطلاعات را مد نظر قرار می دهند - چه در شرکت های تجاری، چه در سازمان های غیر انتفاعی و چه در موسسات دولتی - همواره با مسایل مشابهی در زمینه امنیت اطلاعاتی مواجه خواهند بود. هر یک از این گروه ها برای حفظ داده های خود نیاز به سطح معینی از امنیت دستورات عملی و قوانین شفاف و ساده برای به اجرا در آمدن توسط کارکنان دارند. مدیران در این بعد از امنیت، برای نیل به اهداف تعیین شده باید به سیاست ها و تدوین قوانین امنیتی اطلاعاتی، توجه فراوان داشته باشند. همچنین درک هزینه های پیاده سازی سیاست های امنیتی کارآ، از اهمیت ویژه ای برخوردار است. قوانین امنیتی در فناوری های اطلاعاتی، نوعی سرمایه گذاری در حوزه اجتماعی این بحث که خدمت شما عنوان کردم. به حساب می آیند که می بایست با توجه به هزینه های ضایعات متحمل مورد ارزیابی قرار گیرند. به عنوان مثال تدوین قوانین هم چون مسایلی که در مقاله « قرار داده های نرم افزاری » مطرح کرده ام می تواند در این حوزه باعث شفاف سازی و تعیین چارچوب هایی جهت جلوگیری از معضلات موجود در حوزه پروژه های فناوری اطلاعات گردد.

از بعد حوزه دولتی و حقوقی نیز، سیاست ها و قوانین وضع شده دولت در زمینه فناوری اطلاعات و نظارت به اجرای دقیق این قوانین می تواند باعث حفظ حریم خصوصی افراد گردد. البته دولت نیز به عنوان قانون گذاری در این زمینه می بایست بسیار با احتیاط عمل نماید، چرا که یک چارچوب عمومی سیاست می تواند امنیت این صنعت را تقویت کند، اما مشکلاتی را در اثر وضع این قوانین به وجود آورد که ضررهای آن بیش از مزایای آن باشد دولت در وضع قوانین باید به این موضوع توجه نماید که فناوری های این صنعت سرعت در حال تغییر است و تهدیدات شبکه های اطلاعاتی جدید با چنان سرعتی انتشار می یابند که مقررات دولتی به راحتی می توانند تبدیل به موانعی برای ارایه سریع پاسخ های مبتکرانه شوند. بنابراین بهترین راه این است که میان معیارهای قانونی و غیر قانونی یک نقطه تعادل پیدا نماید. برای دسترسی به چنین تعادلی، سیاست گذاران باید به برخی ویژگی های ذاتی و منحصر به فرد این صنعت توجه نمایند.

پس سعی کنیم که با رفتن به سوی قوانین صحیح و اجرایی حوزه فناوری اطلاعات، چتری امنیتی بر بالای سر آینده کشورمان باز نماییم. و این امر جز با راهبری دولت و ترویج فرهنگ استفاده صحیح از فناوری های نوین اطلاعاتی، میسر نمی گردد.



منبع: ITE