همـــایش علـــمی پـــژوهشی فقـــه و حقـــوق اســـلامی

نهاد برگزار کننده همایش: موسسه قانون یار

((با حمایت معنوی مرکز علمی کاربردی سازمان همیاری شهرداری های استان اصفهان))

سردبیر علمی و مسئول برگزاری همایش: دکتر بهنام اسدی شماره مجوز: ۹۸/۷۸۸۶۴-۲۳۵۱

سال برگزاری همایش: ۱۳۹۸ شماره مقاله: ۱۱۰۵/۱۷۶ رده بندی کنگره: الف ۱۰۱/۸۲

حمایت کیفری از امنیت داده ها در حریم خصوصی و مصادیق نقض آن

دکتر کریم صالحی[۱]

عضو هیات علمی گروه حقوق دانشگاه آزاد اسلامی شهرکرد

دکتر امین امیریان فارسانی

دکتری حقوق کیفری و جرم شناسی ، مدرس دانشگاه آزاد اسلامی شهرکرد

چکیده

در سیستم‌های رایانه‌ای، اطلاعات مهم‌ترین و پرارزش‌ترین عنصر هستند و گاهی ارزشمندترین محصول یک شرکت می‌باشند. از آنجا که در عصر نوین، داده ها و سامانه‌ها دارای ارزشی بالاتر از گندم و حتی فن‌آوری هستند لذا ضرورت دارد که تمام انسان‌ها، در هر زمان و مکان، از آنها در برابر حملات و مخاطرات حفاظت کرده و امنیت کافی را در سیستم‌های خود بر قرار کنند. در فضای سایبر مرز و محدودیتی وجود ندارد، بنابراین حریم خصوصی افراد در بیشتر موارد با جرایمی نظیر دسترسی غیرمجاز(هک) به خطر می‌افتد. این در حالی است که افراد گاهی از این خطرات آگاهی دارند ولی به علت نداشتن مهارت کافی یا عدم آموزش مناسب توانایی مقابله با حملات سایبری را ندارند. در تحقیق حاضر در پی آن هستیم که با آموزش همگانی و بالا بردن قابلیت و توانایی افراد از طریق صدا و سیما و همایش‌های مختلف، جایگاه ایران را در حوزه امنیت سایبری ارتقا دهیم، محیطی امن و قابل اطمینان برای افراد در حوزه حریم خصوصی

---

[۱] نویسنده مسئول

و اطلاعات محرمانه شخصی ایجاد کنیم و با این تدابیر، راه حملات سایبری را سد کرده و جلوی پیشروی آن را بگیریم.

واژه‌های کلیدی: حریم خصوصی، امنیت سایبری، اطلاعات، داده، فضای سایبر

مقدمه

با اختراع رایانه و پیشرفت آن، دنیای رایانه‌ها و به تعبیر صحیح‌تر، فضای سایبر شکل گرفت. با گذشت زمان پیشرفت هر کدام از آنها از دیگری متاثر بوده و هر دوی آنها بر زندگی بشر تاثیرگزار بودند. فضای سایبر و رایانه زندگی بشری را با قوانین خود هماهنگ ساخته و جامعه‌ای نوین را بر پا کرده است؛ جامعه‌ای که پول الکترونیک در قراردادهای الکترونیکی و تنها از طریق سامانه بانک‌های الکترونیکی رد و بدل می‌گردد و تجارت الکترونیکی را سرعت می‌بخشد. اطلاعات و داده‌ها موثرترین عنصری هستند که در این فضا ایفای نقش می‌کنند. در واقع، داده‌ها و اطلاعات جان فضای سایبر محسوب می‌گردند که بدون آنها فضای سایبر جسمی بدون روح خواهد بود. این مهم‌ترین تفاوت فضای سایبر از دنیای واقعی به شمار می آید؛ فضایی که در آن زمان و مکان اهمیت خود را از دست می دهند و به قولی، بی‌معنی می گردند؛ فضایی که حضور فیزیکی در آن بی‌ارزش می‌شود. این عوامل موجب می‌گردد که فضای سایبر ماهیتی مستقل و متفاوت از فضای واقعی به خود بگیرد. به تناسب این، ارزش‌هایی متفاوت از ارزش‌های حاکم بر دنیای واقعی، بر فضای سایبر و عناصر تشکیل دهنده آن حکمفرماست. فضای سایبر از لحاظ حقوق کیفری فن‌آوری اطلاعات، از جمله فضاهایی است که می توانند موجبات بزه‌دیده‌شدن افراد می‌شود. به سخن دیگر، می‌توان امکان ارتکاب راحت بزه را برای مجرمین سایبر در این فضا متصور بود. از آنجا که افراد به نوعی با این فضا آشنایی کافی ندارند لذا گاهی تدابیر امنیتی مناسبی را هم اتخاذ نمی‌کنند. همین امر این می‌تواند موجبات نقض حریم خصوصی افراد و به تبع آن، بزه‌دیده‌شدن آنها را در پی داشته باشد. امنیت سایبری یا به تعبیر دقیق‌تر، اخذ تدابیر امنیتی مناسب نیاز به

آموزش و همگانی‌شدن آن توسط نهادهای مربوطه دارد تا شاهد کمترین مخاطرات در این فضای حیرت‌انگیز باشیم و بتوانیم با امنیت خاطر بیشتری به انجام فعالیت‌های روزمره خود، بدون استرس از ترس نقض حریم خصوصی در تمام شقوق آن، باشیم. این مهم جز با شناسایی مبانی امنیت سایبری و استفاده آنها در تمام حوزه‌های مرتبط با سیستم‌ها و سامانه‌های رایانه‌ای میسّر نمی‌شود.

فصل اول: مفهوم‌شناسی

دلالت الفاظ بر معنایشان ذاتی نیست بلکه قراردادی و اعتباری می‌باشد و از راه جعل یک لفظ و تخصیص آن برای معنایی خاص ایجاد می‌شود. همین اعتباری‌بودن مفاهیم باعث ایجاد تفاوت‌های زیاد در تعریف آنها از سوی افراد مختلف و به تبع آن، تفاوت در درک معنا می‌شود. امروزه برای حل این مشکل، پژوهشگران در اولین قسمت از نوشته خود و برای ایجا اشتراک ذهنی با مخاطب در تصور معنا، به تعریف مفاهیم پایه‌ای موضوع اقدام می‌کنند(زرگر، ۱۳۸۲: ۲۵).

بند یکم: امنیت سایبری[1]

امنیت از مفاهیمی است که از دیرباز همراه بشر بوده است و شاید بتوان قدمت آن را همتای کهنسالی خود انسان دانست. نخستین سرچشمه‌های امنیت در تلاش انسان برای بقا و محافظت از خویشتن در برابر جهان خارج آغاز شد؛ تلاشی که نتیجه غریزه درونی او برای ادامه حیات است. پناه‌گرفتن در غار یا ساختن خانه را می‌توان نمونه‌هایی از این کوشش اولیه به شمار آورد. افزون بر خود انسان، دارایی‌های او نیز در شمول همین مفهوم قرار می‌گیرد. انسان نه‌تنها حفاظت از خود که حفاظت از آنچه به او وابسته است را نیز عهده‌دار است. بدین ترتیب، می‌توان دریافت که حصار کشیدن در اطراف مزرعه یا دیوار کشیدن در اطراف خانه، اگر چه برای حفظ جان خود انسان صورت نمی‌گیرد اما باز هم تلاشی برای رسیدن به امنیت است؛ زیرا محصولات مزرعه یا لوازم زندگی نیز به دلیل انتساب به انسان ارزش

[1] cyber security

محافظت پیدا کرده‌اند(الهی‌منش و سدره‌نشین، ۱۳۹۱: ۶۲).اکنون و با جمع بین این دو ((مطلب)) می‌توان گفت هر آنچه از نظر انسان دارای ارزش باشد مانند حیات، بدن، اموال و ...، لاجرم صحت و سلامت آن نیز برای او اهمیت دارد. از همین‌جاست که رکنی مهم در مفهوم امنیت رخ می‌نماید و آن، صحت و سلامت چیزی است که ارزشمند می‌باشد و باید محفوظ بماند. در همین راستا، افراد برای جلوگیری از دسترسی دیگران به داده و سامانه‌های خود - که ممکن است منجر به حذف، تخریب یا استفاده‌ناپذیر کردن آنها شود- محافظت می‌کنند(عالی پور و کارگری، ۱۳۸۹: ۲۷). بین امنیت سایبری و امنیت ملی مرز بسیار ناچیز و باریکی است. تا زمانی که امنیت سایبری مورد تهدید یا حمله سایبری واقع نشده، امنیت ملی هم مورد مخاطره و خطر قرار نگرفته است و هیچ تهدیدی متوجه آن نیست. به سخن دیگر، پیوند میان امنیت ملی و فضای سایبر با آغاز قرن بیست و یکم و با رایانه‌ای‌تر شدن امور شفاف‌تر شده است. امنیت ملی در فضای سایبر منوط به امنیت داده‌ها و اطلاعات است و تا زمانی که امنیت اطلاعات مخدوش نگردد، امنیت ملی نیز تهدید نمی‌شود. امنیت اطلاعات با سه معیار اصلی تبلور می‌یابد. نخست، قابلیت اعتماد و رازداری[1]تا به واسطه آن اطلاعات به صورت غیرمجاز افشا نشوند. دوم، صحت و تمامیت[2]تا از تغییر یا حذف غیرمجاز اطلاعات پیشگیری شود. سوم، قابلیت دسترسی[3]تا با تحقق این معیار، ممانعت غیرمجاز از دسترسی به اطلاعات و منابع آن پیش نیاید(عالی‌پور، ۱۳۹۰: ۴۵).

در همین راستا، شایان ذکر است که هر چند دسترسی‌پذیری یکی از اصول بنیادین امنیت رایانه‌ای است ولی گاه این ممانعت از دسترسی نه به صورت غیرمجاز که به صورت مجاز، آن هم از طریق دسترسی که یا با اجازهٔ دارنده است یا این که رمز یا پسورد روی صفحه مانیتور نوشته شده است، رخ می دهد. در اینجا باید گفت در بحث ممانعت از دسترسی دیگر بحث هک‌کردن مطرح نمی‌شود و فقط بحث این که مطرح است که شخصی غیر از دارندهٔ داده‌ها که مجاز به دسترسی نباشد، دسترسی پیدا کند و موجب ممانعت گردد .غیر از این سه

[1] Confidentiality

[2] In tegrity

[3] Aralability

معیار ماهوی، باید پارامترهای قابلیت استناد[1](شناسایی قبلی طرفینی که به مبادله داده می‌پردازند)، قابلیت پاسخگویی[2](تعریف و اجرای مسئولیت‌های طرفین) و رد ناپذیری[3] (اثبات اینکه اطلاعات به دریافت‌کننده ارسال شده و ارسال‌کننده نیز مدنظر قرار بگیرد تا از حیث شکلی نیز پشتوانه امنیت اطلاعات تعیین گردد.[4](Chalender,2003: 80) پیوند فضای سایبر و امنیت ملی از جهت مثبت و منفی قابل توجه است. ارتباط امنیت بین این دو در نتیجه طبیعی کارکرد فن‌آوری اطلاعات است. فن‌آوری اطلاعات با نزدیک ساختن مکان‌ها و کوتاه کردن زمان‌ها و با امکانات خارق‌العاده‌ای که به دولت‌ها تقدیم کرده، روش‌های نوین پاسداری از امنیت ملی را از طریق خبرگیری، هم در سطح بین‌المللی و هم در سطح داخلی، مد نظر قرار داده است. دولت‌ها هر چند هنوز از نزدیک‌ساختن اطلاعات سرّی به ساحت اینترنت احتراز می‌کنند اما ناگزیر از رایانه‌ای‌کردن آنها هستند. این موضوع، علی‌رغم تهدیدات بسیار، زمینه مناسب پردازش سریع اطلاعات و تبادل آها را فراهم، و کسب اطلاعات از دیگران و یا اطلاع‌رسانی به دیگران را تقویت می‌کند.فن‌آوری اطلاعات برای تامین امنیت ملی، کارکردهایی فراتر از اطلاع‌رسانی دارد. برخی از دولت‌ها با استفاده از تکنیک پنهان‌نگاری[5]در محیط رایانه سعی در حفظ اطلاعات مرتبط با امنیت ملی نموده‌اند. رمزنگاری تکنیک کدگذاری اطلاعات حین انتقال آنهاست تا احتیاط‌های لازم برای عدم دسترسی به آنها فراهم شود. در ابتدا، این شیوه توسط آژانس امنیت ملی آمریکا برای محافظت از اطلاعات ملی فراهم گردید اما در ادامه، طبق دستورالعمل تصمیم‌گیری در

---

[1] Authenticity

[2] Accountability

[3] Non-Repudiation

[4] – امنیت اطلاعات با امنیت رایانه فرق دارد. در امنیت رایانه‌ای مسائل مربوط به نیل به امور عینی که از آنها به عنوان معیارها و پارامترهای(موارد ذکر شده در متن) یادشده مطرح می‌گردد و شامل محیط پردازش داده و اطلاعات نمی‌شود. اما امنیت اطلاعات غیر از مسائل پیش‌گفته شامل سیستم یا شبکه می‌شود. به عنوان مثال، امنیت رایانه دغدغه پرداختن به ارسال اطلاعات یا مدارک رایانه‌ای یا ذخیره آنها را ندارد، حال آنکه امنیت اطلاعات به این مهم می‌پردازد. باید اشاره کرد که امنیت فن‌آوری اطلاعات تقریباً قرین و هم‌معنی امنیت رایانه‌ای است.

[5] cryptography

مورد امنیت ملی مشهور به اناس‌دی‌دی ۱۴۵[1]، آژانسی با نام امنیت ملی یا حفاظت از داده‌های حساس مبادرت به کنترل رمزنگاری داده‌های اشخاص نمود، بدون آنکه طبقه‌بندی خاصی از داده‌های مورد کنترل ارائه دهد(عالی‌پور، ۱۳۸۹: ۴۷).

بند دوم: داده‌های رایانه‌ای[2]

می توان همه مفروضات، داشته ها، دانسته ها، سوابق و اطلاعات را داده نامید. انسان برای ثبت و درک مشترک هر واقعیت و پدیده از نشانه‌های مختص آن استفاده نمود. ابتدا به صورت تصویر و در ادامهٔ سیر تکاملی آن از حروف، اعداد و علائم کمک گرفت. بنابراین، هر واقعیت یا داده‌ای با حروف، اعداد و علائم و یا ترکیبی از آنها قابل ثبت است. به اعداد، حروف و علامت‌هایی که برای درک و فهم مشترک از انسان ها یا رایانه سرچشمه می گیرند، داده می گویند(جلالی، ۱۳۸۲: ۳۳).داده ممکن است فی‌نفسه ماهیتی نداشته باشد زیرا داده عبارت از توالی هایی از صفر و یک است که به صورت نمادی از وقایع، اطلاعات یا مفاهیم ظاهر می‌شود؛ به گونه‌ای که قابلیت پردازش در یک سیستم رایانه‌ای را داشته باشد. البته آن سیستم هم باید برنامه‌ای در اختیار داشته باشد که بتواند این داده ها را به نحو صحیح و درست پردازش نماید و از این طریق، عملکرد شایسته ای برای آن سیستم رقم بزند و به مرحله اجرا بگذارد(البوعلی،۱۳۹۲: ۲۳).در قانون تجارت الکترونیکی، علی‌رغم کاربرد کلمهٔ داده در عباراتی چون «حمایت از داده»[3]و «پایگاه‌های داده»[4] تعریفی از این واژه ارائه نشده است. داده را می توان دارای اقسام: «داده مخابراتی»، «داده موجود روی کارت‌های اعتباری»، «داده موجود روی تراشه های مغناطیسی» و... دانست. اما به طور کلی باید گفت که داده رایانه‌ای عبارت از اطلاعاتی است که در قالبی خاص ایجاد، ذخیره و نگهداری

[1] NSDD 145 (National security decision directive)

[2] Computer Data

[3] Data Protection

[4] Data Base

می‌شود(نوری، ۱۳۸۳: ۵۹).غالباً داده‌های رایانه‌ای موضوع جرایم رایانه‌ای واقع می‌شوند. البته دیگر اقسام نام‌برده از داده را می‌توان به نوعی داده رایانه‌ای دانست زیرا امروزه با در هم آمیختن تجهیزات مخابراتی و سیستم‌های رایانه‌ای عملاً تفکیک این فضاها از یکدیگر میسر نیست. داده‌های موجود روی کارت‌ها و تراشه‌ها نیز به وسیله رایانه قابل ایجاد، ذخیره و پردازش هستند. بنابراین، داده رایانه‌ای دارای مفهوم عامی است که سایر انواع یادشده زیرمجموعه‌های آن هستند(خرم‌آبادی، ۱۳۸۴: ۲۸).

بند سوم: اطلاعات[۱]

واژه «انفورماسیون» (اطلاعات) دارای ریشه لاتین است. معنای اولیه آن «مفهوم» و «عبارت» بود و بعدها به «آگاهی» و «انتقال داده‌ها» تغییر یافت و مفهوم آن، برداشت ما از واقعیات اطرافمان می‌باشد. واژه‌نامه ای.ال.ای، اطلاعات را عبارت از تمام ایده‌ها، واقعیت‌ها و کارهای خلاقانه ذهن تعریف نموده که به صورت رسمی یا غیررسمی به هر حالتی ثبت، منتشر و توزیع گردیده است. اطلاعات می‌تواند شامل کتاب، نشریه ادواری، نقشه، فایل کامپیوتری، مواد شنیداری و دیداری و حالات ترکیبی آنها باشد. همچنین، بر مبنای محتوا می‌توان اطلاعات را به انواع علمی، مالی، فنی و... تقسیم‌بندی کرد. در حوزه فن‌آوری اطلاعات، اطلاعات خام جابه‌جا نمی‌شود و آنچه که واقعاً منتقل می‌شود، داده است (باستانی، ۱۳۸۸: ۴۹)

بند چهارم: حریم خصوصی اطلاعات[۲]

حریم خصوصی اطلاعاتی یا داده‌ای(حفاظت داده‌ها) رابطه‌ای است بین جمع‌آوری و توزیع داده‌ها، تکنولوژی و انتظار عمومی از حریم خصوصی با مسائل قانونی و سیاسی مرتبط با آنها. نگرانی‌ها در حریم خصوصی در هنگام جمع‌آوری و نگهداری به صورت دیجیتال یا غیردیجیتال داده‌ها و اطلاعاتی که فردی را به صورت خاص بازشناساند، خود را نشان

[۱] Howng, the ALA Giossary of library and information science, (Chicago, Amrican library)

[۲] Privacy Information

می‌دهد. ریشه و اساس مشکل حریم خصوصی مربوط به افشاگری نامناسب و بدون کنترل داده‌های شخصی است. مشکلات حریم خصوصی اطلاعاتی در حقیقت مربوط به منابع مختلف و متنوع داده‌ها واطلاعات می‌باشد. از جملهٔ آن منابع می‌توان به موارد زیر اشاره کرد:

- بایگانی پزشکی (بایگانی اطلاعات مربوط به سلامت اشخاص)
- بایگانی جرایم
- خانه و بایگانی جغرافیایی
- نژاد و قومیت‌ها
- سرویس‌های مربوط به موقعیت مکانی

چالش اصلی در حفظ حریم خصوصی آنجایی مطرح است که در توزیع و به‌اشتراک‌گذاری داده‌های مختلف، بتوان اطلاعاتی که شخص خاصی را باز می‌شناساند، حفظ کرد.

بند پنجم: فضای سایبر[1]

از لحاظ لغوی در فرهنگ‌های مختلف، فضای سایبر به معنای فضای مجازی و غیرملموس به کار رفته است. فضای سایبر محیطی مجازی است که به صورت غیرملموس در پهنه شبکه‌های بین‌المللی، که از طریق شاهراه‌های اطلاعاتی مثل اینترنت به هم وصل هستند، وجود دارد. در این محیط تمامی اطلاعات درباره رابطه افراد، فرهنگ‌ها، ملت‌ها، کشورها و به طور کلی هر آنچه در کره خاکی به صورت فیزیکی و ملموس وجود دارد (به صورت اسناد، نوشته، تصویر، صوت)، در یک فضای مجازی به شکل دیجیتالی نیز وجود دارد و قابل استفاده و در دسترس کاربران است. فضای سایبر در واقع محیطی مجازی برای فعالیت‌های اجتماعی می‌باشد. مهم‌ترین ویژگی این فضا، استقلال از زمان و مکان است.

[1] cyber space

سرعت بالا، ارزان بودن، کیفیت مناسب و در دسترس بودن اطلاعات از ویژگی‌های فضای سایبر است. در این فضا همان‌گونه که فعالیت‌ها سریع‌تر و راحت‌تر انجام می‌شوند جرایم نیز سریع‌تر و کم‌هزینه‌تر صورت می‌گیرند(محمدی‌فر، ۱۳۸۲: ۴۵).

فصل دوم: جایگاه امنیت سایبری در حریم خصوصی

فاصله زیادی بین مصرف کنندگان اینترنت و حریم خصوصی آنلاین آنها وجود دارد. مشاهدات گوناگون نشان می‌دهد که دغدغه بزرگ کاربران اینترنت، حفظ امنیت و حریم خصوصی آنهاست. هنگامی که چگونگی حفظ اطلاعات شخصی به میان می‌آید، این فاصله بیش تر می شود. عده زیادی از کاربران، به غلط، بر این عقیده اند که راهکارهای حفظ حریم خصوصی سایت‌های مختلف کاربران را از ایجاد پروفایل مربوط به فعالیت‌های یک نفر- که این امر در بین بازاریاب‌های آنلاین رایج است- باز می‌دارد. کاربران باید به این درک برسند که هر کلیک و حرکت در دنیای آنلاین یک ردپای الکترونیکی از آنها بر جای می گذارد و می‌تواند گردآوری، ذخیره، شمارش و پیگیری شود و در نتیجه، فهرست دقیقی از فعالیت‌ها، علاقه‌ها و الگوهای رفتاری آنها ثبت گردد. این پروسه با عنوان «مسیریابی رفتاری» نیز شناخته می‌شود. مسیریابی رفتاری کاربران بیش از هر چیزی در داده‌هایی به نام «کوکی‌ها»[1]ثبت می شود. کوکی‌ها فایل‌های اطلاعاتی کوچکی هستند که در کامپیوتر کاربران ذخیره می‌شوند و توسط خود سایت و آگهی‌دهندگان انتشار می‌یابد و در نتیجه، به ثبت می‌رسد. (باستانی ، ۱۳۸۸، ص۲۷)کوکی‌ها چیز جدیدی نیستند و معمولاً کاربری آنلاین را آسان‌تر می‌کنند. برای مثال، کوکی‌ها رمز عبور و برخی از اطلاعات شخصی کاربر در اینترنت را ذخیره می‌کنند. در نتیجه دیگر لازم نیست که کاربران آن اطلاعات را دوباره وارد کنند و از این جهت، تقریباً مفید هستند. تمام مرورگرهای اینترنتی مثل اینترنت اکسپلورر یا فایرفاکس ابزاری را در اختیار کاربران قرار می‌دهند که به آنها اجازه می‌دهد کوکی‌ها را به شیوه‌های گوناگون مدیریت کنند. مثلاً می‌توان از ورود و ثبت کوکی‌هایی که به شبکه‌های تبلیغاتی اجازه می‌دهند الگوی رفتاری کاربران را در سایت‌های مختلف

[1] Cookies

مسیریابی و ثبت کنند، جلوگیری کرد.مدیریت کوکی‌ها، به تنهایی، نمی‌تواند جلوی مسیریابی آنلاین را بگیرد. بعضی از کوکی‌ها ظاهراً نفوذناپذیر هستند و تلاش برای محو آنها فایده‌ای ندارد. برخی از مدل های تجاری جدید از تمام کوکی‌ها عبور می کنند و اطلاعات مربوط به کلیک کاربران را به طور مستقیم از ارایه‌کنندگان سرویس‌های اینترنت دریافت می‌دارند. در حالی که کل صنعت فن‌آوری به سوی مسیریابی الگوی رفتاری آنلاین کاربران پیش می‌رود و پروفایل‌های مخصوص این امر با اطلاعات تمام و کمال ساخته می شود، اما ساختار حفظ محرمانگی منافع کاربران به طرز اسفباری ضعیف است. کاربران باید حق انتخاب داشته باشند و به آنها اجازه داده شود که بر اطلاعات شخصی خود نظارت داشته و از حقوق خود دفاع کنند.مطالب فوق به خوبی جایگاه امنیت سایبر و نقش مهم آن در حریم خصوصی را نمایش می‌دهد؛ تا آنجا که فرد شاید نتواند با اطمینان از عدم نفوذ دیگران به حریم خصوصی خود صحبت کند ولی تا حد زیادی توانسته است در برابر حملات سایبری با امنیت سایبری کافی مقابله نشان دهد و حریم خصوصی خود را تا به میزان بالایی از نفوذ هکرها و افراد ناشناس در امان نگه دار

فصل سوم: شیوه‌های حملات سایبری در نقض امنیت داده ها

بند یکم: ویروس‌های رایانه‌ای[1]

ویروس ها اغلب تاثیرهای جانبی ویرانگری دارند(البته گاهی نیز بی ضرر هستند). برای نمونه، برخی از ویروس‌ها می‌توانند به داده‌های موجود در دیسک سخت کامپیوتر ضرر برسانند یا حافظه‌ای را که برای منظورهای دیگر مورد نیاز برنامه‌هاست، اشغال کنند. ویروس‌ها بدین علت خطرناک می‌شوند که پیش از آنکه بتوان آنها را متوقف کرد، با سرعت بسیار منتشر می‌شوند. از این رو، چون نمی توان جلوی پیشرفت آنها را گرفت، خسارت های هنگفتی به داده‌ها و سامانه‌های رایانه‌ای کاریران وارد می‌آورند و بعضاً مانع دسترسی کاربران می‌شوند. در مدتی که شبکه‌های رایانه‌ای مورد استفاده واقع می‌شوند، هزاران ویروس

[1] Computer viruses

رایانه‌ای اطلاعات و داده‌های افراد را از میان برده یا سبب اختلال در کارکرد سیستم رایانه‌ای آنان می‌گردند. از جملهٔ آنها می‌توان به «مغز پاکستانی»، «ویروس ملیسا»، «اکسپلورزیپ»، «چرنوبیل» و «دوستت دارم» اشاره کرد که مانع دسترسی کاربران می‌شوند (فضلی، ۱۳۸۳: ۱۷۰).

بند دوم: تراواها[۱]

در علوم رایانه‌ای نیز اسب تراوا – مشابه اسب معروف در افسانه مزبور– برنامه‌ای است که ظاهراً خوب و سودمند به نظر می‌رسد ولی در حقیقت شامل برنامه‌های ویرانگر و مختل‌کننده است.[۲]اسب‌های تراوای رایانه‌ای انواع و اقسام بسیاری دارند که از جمله می‌توان به اسب‌های تراوای اداره از راه دور[۳]، تراواهای گذرواژه[۴]و تراواهای ویرانگر[۵]اشاره کرد.(جلالی ، ۱۳۸۲، ص۱۴)

بند سوم: کرم‌های کامپیوتری[۶]

اغلب مردم کرم‌های کامپیوتری را با ویروس‌ها اشتباه می‌گیرند زیرا هر دو، کامپیوتر یا سامانه را آلوده می‌کنند و می‌توانند آثار مخربی مانند حذف فایل‌ها و پاک‌کردن کل دیسک سخت، داشته باشند. متخصصان کرم‌ها را زیرمجموعه‌ای از ویروس‌ها در نظر گرفته و گاهی از اصطلاح ویروس برای اشاره به آنها استفاده می‌کنند (Mantin,1991: 54). تفاوت مهم بین ویروس و کرم رایانه‌ای در آن است که کرم‌ها روی شبکه فعالیت دارند اما فعالیت ویروس وابسته به تکثیر یا نسخه‌برداری فیزیکی است. به عبارت دیگر، ویروس‌ها به این

---

۱ Trojans

۲ Cyber Terrorism in the Context of globalization

۳ Remote AdimnistrationTrojans

۴ Password Trojans

۵ Destructive Trojans

۶ Computer worms

قانع‌اند که در یک کامپیوتر بمانند و فایلی را پس از فایل دیگر آلوده کنند اما کرم‌ها همیشه در جستجوی مرزهای جدید هستند.

فصل چهارم: مصادیق نقض حریم خصوصی در فضای مجازی

جنبهٔ دیگر موضوع – همانطور که گفته شد– مربوط به ناقضان حریم خصوصی در فضای مجازی است. این بزهکاران زمانی که وارد فضای مجازی یا همان اینترنت می‌شوند، آن را مِلک طِلق خود دانسته و به خود اجازه هرگونه فعالیت و ورود به حریم خصوصی دیگران را می‌دهند. در زیر به برخی مصادیق نقض حریم خصوصی در فضای مجازی که در قانون جرایم رایانه ای جرم انگاری شده است، می‌پردازیم:

۱. دسترسی غیرمجاز به داده‌های رایانه‌ای یا مخابراتی نظیر هک ایمیل یا اکانت افراد

۲. شنود غیرمجاز محتوای در حال انتقال در سیستم‌های رایانه‌ای یا مخابراتی نظیر استفاده از نرم‌افزارهای شنود چت‌های اینترنتی.

۳. دسترسی غیرمجاز به داده‌های سرّیِ در حال انتقال در سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده و تحصیل و شنود آن.

۴. در دسترس قرار دادن داده‌های سرّیِ در حال انتقال در سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده برای اشخاص فاقد صلاحیت.

۵. نقض تدابیر امنیتی سیستم‌های رایانه‌ای یا مخابراتی به قصد دسترسی به داده‌های سرّیِ در حال انتقال در سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده.

۶. حذف یا تخریب یا مختل یا غیرقابل پردازش نمودن داده‌های دیگری از سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده، به طور غیرمجاز.

۷. از کار انداختن یا مختل نمودن سیستم‌های رایانه‌ای یا مخابراتی به طور غیرمجاز، نظیر غیرفعال‌سازی دیتابیس تارنماها و ممانعت از دسترسی افراد به سایت‌های شخصی.

۸. ممانعت از دسترسی اشخاص مجاز به داده‌ها یا سیستمهای رایانه‌ای یا مخابراتی، به طور غیرمجاز.

۹. ربودن داده‌های متعلق به دیگری.

۱۰. هتک حیثیت از طریق انتشار صوت و فیلم تحریف‌شدهٔ افراد دیگر به وسیله سیستم‌های رایانه‌ای یا مخابراتی.

۱۱. نشر اکاذیب از طریق سیستم‌های رایانه‌ای یا مخابراتی به قصد ضرر رساندن به غیر یا تشویش اذهان عمومی.

۱۲. فروش یا انتشار یا در دسترس قرار دادن گذرواژه یا هر داده‌ای که امکان دسترسی غیرمجاز به داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتیِ متعلق به دیگری را فراهم می‌کند.

۱۳. آموزش نحوه ارتکاب جرایم دسترسی غیرمجاز، شنود غیرمجاز، جاسوسی رایانه‌ای و تخریب و اخلال در داده‌ها یا سیستم‌های رایانه‌ای و مخابراتی.

ناقضین حریم خصوصی در فضای مجازی به دلایلی نظیر: افسردگی، عصبانیت، حسادت، انتقام‌جوئی، حس تنفر، تفریح و سرگرمی، خود کم‌بینی و حقارت، حس رقابت و عدم توجه به اصول اخلاقی و ارزش‌های جامعه خود را مجاز به ورود به حریم خصوصی قربانیان دانسته و خسارات جبران‌ناپذیری را به حیثیت و مال و حتی جان افراد وارد می‌سازند.

بند یکم: شیوه‌های مقابله با نقض حریم خصوصی و امنیت داده ها

هر فردی دوست دارد محیط و فضایی داشته باشد که دیگران بدون اجازه‌اش قادر نباشند به آن وارد شوند. اما این خواست مشروع و قانونی بارها از سوی افراد حقیقی و حقوقی مورد حمله قرار می‌گیرد. در سال‌های اخیر نیز با گسترش چشمگیر استفاده از شبکه‌های اینترنتی و افزایش کاربران فضای مجازی این حمله‌ها بیشتر و جدی‌تر شده است؛ مشکلی که با سد قانون می‌توان از آسیب‌ها و مشکلاتِ ناشی از آن کاست.باید در ابتدا و برای آشنایی بیشتر با موضوع «حریم خصوصی» آن را تعریف کنیم. در تعریفی ساده، حریم خصوصی یعنی هر فرد این حق را داشته باشد که بدون ترس و در خلوتی که دوست دارد اطلاعات مربوط به زندگی خود را مخفی کند. در اینجا فرد تصمیم می‌گیرد که چه زمانی و تا چه اندازه‌ای این اطلاعات را با دیگران تقسیم کند. باید دانست که در تعالیم دینی نیز بر رعایت حریم خصوصی تاکید و از مردم خواسته شده است که از افشای اطلاعات زندگی خود خودداری کنند. با این حال، در دنیای مدرن افراد وارد فضایی می‌شوند که اطلاعاتشان از هیچ دستبرد یا تعدی‌ای در امان نیست. قرارداشتن در چنین شرایطی نقض حریم خصوصی در فضای مجازی را به یکی از مهم‌ترین مسائل جوامع تبدیل می‌کند. این موضوع از دو منظر قربانیان نقض و ناقضین حریم خصوصی قابل طرح و بررسی است.

بند دوم: نقش قربانی را بازی نکنید

در منظر اول، قربانیان نقض حریم خصوصی قرار دارند. در این باره باید به این اصل توجه شود که در فضای مجازی تا نگارنده یا همان کاربر وجود نداشته باشد، جرمِ نقض یا تعدی به حریم خصوصی نیز رخ نمی‌دهد. به عبارتی دیگر، نگارنده می‌تواند با رعایت مجموعه‌ای از موارد پیشگیرانه قربانی نباشد. باید این را بدانید که بسیاری از بزه‌دیدگان جرایم سایبری استعدادی زیادی برای قربانی‌بودن دارند یعنی این افراد به راحتی طعمه بزهکاران سایبری می‌شوند.(محسنی، ۱۳۸۹: ۳۲) با نگاهی به صفحه حوادث و سایت پلیس فتا (فضای تبادل اطلاعات) می‌توان دریافت که بسیاری از مال‌باختگان و افرادی که در فضای مجازی مورد سوءاستفاده قرار گرفته‌اند، به آسانی اطلاعات خود را در اختیار بزهکار قرار داده‌اند.

کارشناسان ضعف شخصیتی، فقدان اطلاعات کافی درباره محیط مجازی و بی‌دقتی در محافظت از داده‌ها را از مهمترین دلایل قربانی‌شدن افراد در فضای مجازی می‌دانند. در بیانی ساده، مردم باید بدانند همانطور که با نصب قفل‌های محکم و رعایت نکات ایمنی خانه یا خودروی خود را در برابر سرقت ایمن می‌کنند، باید در حوزه اطلاعات در فضای مجازی نیز جانب مسایل امنیتی را نگه دارند. نگهداری اطلاعات خصوصی در فلش و کارت‌های حافظه، تلفن همراه و سی.دی و مواردی از این دست، پای مجرمان سایبری را به زندگی شما باز می‌کند. با آموزش افراد از سوی دولت، هم در جهت ارتقای امنیت سایبری در ایران و هم جلوگیری از نقض حریم خصوصی با استفاده از این تدابیر امکان پذیر است و می توانند از قربانی شدن افراد در این فضای غیر قابل انکار پذیر جلوگیری کند و موجبات رفع دغدغه کاربران را بتوان با اموزش صحیح امنیت سایبری نایل آمد.

نتیجه گیری و پیشنهادات

انسان به حکم طبیعت و سرشت باید دارای حریم خصوصی برای خود باشد و از آن محافظت نماید. در مقابل، افراد می‌بایست نسبت به صیانت و رعایت حریم خصوصی سایرین اقدام نمایند.نقض حریم خصوصی در فضای مجازی یکی از مهم‌ترین مسائل روز جامعه ماست که از دو منظر: ۱) قربانیان نقض حریم خصوصی در فضای مجازی و ۲) ناقضین حریم خصوصی در فضای مجازی قابل بررسی است. بزه‌دیدگان در فضای مجازی نقش مهمی را در بروز جرایم ناقض حریم خصوصی ایفا می‌کنند. آنها، در عین حال، می‌توانند در اقدامات پیشگیرانه علیه جرایم سایبری نقش‌آفرین باشند. بسیاری از بزه‌دیدگان جرایم سایبری و کسانی که حریم خصوصی آنان در فضای مجازی نقض می‌شود، استعداد قابل توجهی برای قربانی‌شدن بروز می‌دهند و به راحتی طعمه بزهکاران سایبری می‌گردند. بعضی از کلاهبرداری‌های اینترنتی به وسیله کسب اطلاعات به روش‌های بسیار ساده و سوء استفاده از عکس‌ها و اسرار شخصی، نمونه‌هایی از این موضوع می‌باشند. ضعف شخصیتی، فقدان اطلاعات کافی در رابطه با محیط مجازی و عدم دقت در محافظت از داده‌ها و... مواردی است که قربانیِ بزه سایبری را در قربانی‌شدنش مساعدت می‌کند. افراد باید نسبت به صیانت

از حریم خصوصی خود همت نمایند. بسیاری از اشخاص، بدون رعایت مسائل امنیتی، خصوصی‌ترین اطلاعات خود را روی سیستم رایانه‌ای و یا حامل‌های داده نظیر فلش، کارت‌های حافظه، تلفن همراه و سی‌دی و ... ذخیره می‌کنند. آنها با این کار دست بزهکار سایبری را در تعرض به حریم خصوصی باز می‌گذارند و اینچنین استعداد خود در قربانی‌شدن در فضای مجازی را نشان می‌دهند. در حالی که با کمی تدبیر و با کمک از نهادهایی نظیر صدا و سیما می‌توان افراد را با این فضا آشنا و امنیت سایبری را برای آنها تشریح کرده، راه را برای مقابله با نقض حریم خصوصی بسته و موجبات از بین رفتن دغدغه کاربران را ایجاد نمود.

پیشنهادات:

- همکاری پلیس فتا با صدا و سیما برای هشدار و ارائه نکات آموزشی و مخاطرات امنیتی در حوزه فضای سایبر به صورت فیلم مستند یا بروشورهای مخصوص
- همکاری پلیس فتا با آموزش و پرورش برای بالابردن سطح دانش‌آموزان و خانواده‌ها در حوزه امنیت سایبری و شناسایی راه‌های مقابله و برون‌رفت از بحران از طرف مختصصان حوزه جرایم سایبری، از طریق تدریس به عنوان واحد درسی یا کلاس فوق برنامه
- استفاده پلیس فتا از مجرمین سایبری و هکرها به منظور شناسایی ضعف سیستم‌ها و ارتقای امنیت آنها برای جلوگیری از ورود غیرمجاز اشخاص به داده‌ها و سامانه‌های رایانه‌ای انجام پذیرد.
- استفاده از نرم‌افزارهای شناسایی ویروس و نصب نرم‌افزارهای ضد ویروس روی سیستم‌های رایانه‌ای در جهت حذف یا حداقل کردن حملات به آنها از طرف پلیس فتا

- مجهز کردن تمام مرکز نگهداری داده‌ها و اطلاعات مهم به سیستم اعلام خطر یا هشدار از سوی پلیس فتا. با این کار هر گونه ورود غیرمجاز یا حملات برای حذف یا استفاده ناپذیر کردن داده‌ها به مرکز، گزارش و به سرعت اقدامات لازم صورت می‌گیرد.

- آموزش افسران و ضابطین در پلیس فتا ویژۀ جرایم رایانه‌ای و تفکیک آن با جرایم سایبری، و امکان آموزش مهارت‌های مرتبط برای آنها جهت انجام‌دادن بهتر کار

منابع و مآخذ

۱. البوعلی، امیر (۱۳۹۲)، صلاحیت محاکم در جرایم سایبری، تهران: جنگل، چاپ اول.

۲. الهی‌منش، محمدرضا و ابوالفضل سدره‌نشین (۱۳۹۱)، محشای قانون جرایم رایانه‌ای، تهران: مجد، چاپ اول.

۳. باستانی، برومند (۱۳۸۸)، جرایم کامپیوتری و اینترنتی جلوه‌ای نوین از بزهکاری، تهران: بهنامی، چاپ دوم.

۴. جلالی، علی‌اکبر، (۱۳۸۲) شهر الکترونیک، تهران: دانشگاه علم و صنعت ایران، چاپ اول.

۵. خرم‌آبادی، عبدالصمد (۱۳۸۴)، «تاریخچه، تعریف و طبقه بندی جرایم رایانه‌ای»، چاپ‌شده در: مجموعه مقالات همایش بررسی ابعاد حقوق فناوری اطلاعات، تهران: معاونت حقوقی و توسعه قضایی قوه قضاییه.چاپ اول

۶. زرگر، محمود (۱۳۸۲)، اصول و مفاهیم فناوری اطلاعات، تهران: بهینه، چاپ اول.

۷. عالی‌پور، حسن و نوروز کارگری (۱۳۸۹)، جرایم ضد امنیت ملی، تهران: خرسندی، چاپ اول.

۸. عالی‌پور، حسن (۱۳۹۰)، حقوق کیفری فناوری اطلاعات، تهران: خرسندی، چاپ اول.

۹. فضلی، مهدی (۱۳۸۳)، «تخریب و اخلال در داده‌ها و سیستم‌های رایانه‌ای»، چاپ‌شده در: مجموعه مقالات همایش جنبه‌های حقوقی فناوری اطلاعات، قم: سلسبیل، چاپ اول.صص۱۲-۱۸

۱۰. محسنی، فرید (۱۳۸۹)، حریم خصوصی اطلاعات، تهران: دانشگاه امام صادق(ع)، چاپ اول.

۱۱. محمدی‌فر، علیرضا (۱۳۸۲)، وب را بشناسیم، تهران: ریز پردازنده، چاپ دوم.

۱۲. نوری، محمدعلی (۱۳۸۳)، حقوق حمایت از داده‌ها، تهران: گنج دانش، چاپ اول.