فصلنامه علمی (مقاله علمی-پژوهشی) جامعه‌شناسی سیاسی ایران، سال سوم،شماره دوم(پیاپی۱۰)تابستان ۱۳۹۹،صص۱۰۸۸-۱۰۷۲

امنیت محتوا ی داده‌ها در حریم خصوصی ومطالعه تطبیقی آن

همایون علی حسینی[۱]

حمیدرضا علی کرمی[۲]

رسول احمدی فر[۳]

تاریخ دریافت :۱۴ /۱۳۹۸/۱۲

تاریخ پذیرش: ۱۳۹۹/۲/۲۹

چکیده

در نظام های حقوقی آزادی های فردی مورد توجه بوده است امروزه اشخاص اعم از حقیقی و حقوقی در فضایی مجازی فعالیت های گسترده ای را انجام می دهند محتوای و داد های مبادله شده توسط اشخاص و ذینفعان در این فضا تولیدو حمل می شود باید دارای حرمت ،امنیت و حریم خاص باشند که نقض آنها تبعاتی برای کنشگران آن بوجود می آورد لازم است مسولیت مدنی اشخاص در این فضا بررسی و با مقررات و مصوبات حاکم بر مجامع بین المللی تطبیق داده شده و برای حفظ و کرامت این جایگاه و حرمت آن راهکارهایی اتخاذگردد.تعاریف مختلفی از داده ،امنیت ،حریم اشخاص و محتوا درمقررات و عرف جامعه وجود دارد. امور مذکور از جمله حقوقی به شمار می‌رود که لازم است تمامی انسان‌ها در هر حکومتی با آن آشنا باشند زیرا با آگاهی از آنها ، امنیت شهروندان رعایت خواهد شد، ضمن این‌که دولت‌ها نیز در این زمینه سهم عمده‌ای بر عهده دارند. ازجمله تکالیف دولتها و نظامهای حقوقی، به روز کردن قوانینی است که در حوزه حریم شخصی شهروندان وضع شده اند، مواردی از جمله پرهیز از شنود مکالمات تلفنی با تامین امنیت فضای مجازی، همگی جزو مصادیق حریم خصوصی شهروندان است و قانونگذار مکلف است نظام حقوقی ویژه ای را درباره آنها تدوین نماید .امنیت داد ه ها گاه توسط دولت و سازمانهای دولتی نقض میگردد وگاه افراد خود ممکن است اقدام به نقض امنیت آنها نمایند با این تفاوت که هرگاه حریم خصوصی یک شهروند مورد تجاوز شهروند دیگری قرار گیرد می توان به قوانین موجود و نظم اجتماعی پناه برد و از دولت و قوه قضاییه استمداد جست و فرد متجاوز را مجازات نمود اما این امر در مورد دولت به سادگی صورت نمیگیرد و هرگز نمیتوان دولت را به خاطر نقض حریم خصوصی مجازات کرد بلکه در مطلوبترین حالت خود میتوان دولت را به جبران خسارت ملزم نمود که آن نیز با قید و بندها و شرایط فراوان روبروست ضمن آنکه در بسیاری موارد اقدامات دولت ظاهری قانونی و مدیریت مآبانه دارد .حریم اشخاص در فضای سایبر به دلیل امکان ردیابی و ثبت و نشر اطلاعات شخصی کاربران دچار تضییقات بیشتری است و وضع قوانین جدی برای حمایت از این حق در نظامهای حقوقی ضروری می باشند. مباحث فنی و مهندسی در فضای سایبر و قوانین کشورهای مختلف در این خصوص نشان دهنده دیدگاههای متفاوت به این مقوله هست که در کشور ما هم بر اساس ساختار آن و همچنین نگاه اسلام به این مقوله چارچوبهایی تعیین گردیده است.اتحادیه جهانی اروپا در زمینه حمایت از تولید و حمل محتوای اینترنتی به وضع مقرراتی پرداخته که رگولاتوری های کشورهای عضو در حال تغییر در فرایند تولید و تنظیم گری روش های نوینی هستند تا خود را به روش تنظیم گری بین المللی منطبق نمایند اجرای صحیح و درست این مصوبات نیازمند آنست تا در بخش های گوناگون تنظیم گری ازجمله تولید و حفاظت از محتوا تعادل و تبادل نظر جدی صورت پذیرد اتحادیه تاکید دارد مهمترین و چالش انگیزترین موضوع حریم خصوصی و امنیت محتوا می باشد؛لذا بایسته است با تلفیق علوم فنی و مهندسی و نظام های حقوقی دکترین جدیدی همگام با رشد تکنولوژی پدید آید.

واژگان کلیدی: امنیت ،داده ، مسئولیت مدنی، نقض حریم شخصی،فرآیند تولید، حمل محتوای اینترنتی، حقوق بشر، مقررات اتحادیه اروپا.

---

[۱]گروه حقوق،واحد اراک،دانشگاه آزاد اسلامی، اراک،ایران.

[۲]گروه حقوق،واحد اراک،دانشگاه آزاد اسلامی، اراک،ایران.

[۳]گروه حقوق،واحد اراک،دانشگاه آزاد اسلامی، اراک،ایران. گروه حقوق،دانشگاه ملایر، ملایر،ایران.

مقدمه

حریم خصوصی اشخاص گاه توسط دولت و سازمان¬های دولتی نقض میگردد وگاه افراد خود ممکن است اقدام به نقض حریم شخصی یکدیگر نمایند با این تفاوت که هرگاه حریم خصوصی یک شهروند مورد تجاوز شهروند دیگری قرار گیرد می توان به قوانین موجود و نظم اجتماعی پناه برد و از دولت و قوه قضاییه استمداد جست و فرد متجاوز را مجازات نمود اما این امر در مورد دولت به سادگی صورت نمیگیرد و هرگز نمی توان دولت را به خاطر نقض حریم خصوصی مجازات کرد بلکه در مطلوبترین حالت خود میتوان دولت را به جبران خسارت ملزم نمود که آن نیز با قید و بندها و شرایط فراوان روبروست ضمن آنکه در بسیاری موارد اقدامات دولت ظاهری قانونی و مدیریت مآبانه دارد .

حریم اشخاص در فضای سایبر به دلیل امکان ردیابی و ثبت و نشر اطلاعات شخصی کاربران دچار تضییقات بیشتری است و وضع قوانین جدی برای حمایت از این حق در نظامهای حقوقی ضروری می باشند. قوانین کشورهای مختلف در این خصوص نشان دهنده دیدگاههای متفاوت به این مقوله هست که در کشور ما هم بر اساس ساختار آن و همچنین نگاه اسلام به این مقوله چارچوبهایی تعیین گردیده است .

لذا در قوانین هر کشوری تدابیری جهت حمایت از حریم خصوصی افراد در فضای مجازی درمقابل اقدامات افراد و دولت اتخاذ شده است. در نظام حقوقی ایران نیز قوانینی و مصوباتی در زمینه تولید و حمل محتوای اینترنتی وجود دارد که در این پژوهش مورد بررسی قرار میگیرند.

پیشنه تحقیق

۱- محسنی نسترن ،آریائیان احسان،رجبی امید، ویسی مهرداد و بحرین تکاوش - کتاب رگولاتوری داده ها ۱۳۹۷- انتشارات راه

نتیجه : فناوری کلان داده ها به عنوان یکی از فناوری های نوین و موضوعات محوری توسعه فناوری و کسب و کارها، نظام حقوقی جدیدی را به وجود می آورد . در هریک از طبقات و لایه های فناوری کلان داده ها بازیگران و فعالانی وجود دارند که بر چگونگی تولید محصول یا ارئه خدمت کمک می کند

۲-کروبی محمد تقی - کتاب اتحاد اروپا و بحث حمایت از داده های شخصی و حریم خصوصی ارتباطات ۱۳۸۴- ناشر بقعه

نتیجه : بحث حریم خصوصی در تکنولوژی اطلاعاتی و ارتباطی در اتحادیه اروپا، با عنایت به ظرفیت خاص آن به طور جدی مورد بحث و بررسی و نهایتا اعمال راهکارهای عملی در جهت تضمین و حراست از این حق واقع

شده است.دستورالعمل های ۴۶،۹۵،۶۶،۹۷،۵۸،۲ معیارهای قانونی جدیدی برای پردازش داده های شخصی و حق حریم خصوصی در بحث ارتباطات الکترونیکی معرفی و از تمامی اعضا تبعیت از آن معیارها را خواستار شده

۳- محمدی، قاسم، جرم انتشار اسرار شخصی وخانوادگی درفضای مجازی، دانشگاه علامه طباطبایی، استاد راهنما: علی محمدی، ۱۳۹۱

قانونگذار توجه خاصی را به بحث اسرار شخصی و خانوادگی دارد و بر پایه حریم خصوصی به حمایت از آن همت گمارده تا از این طریق مانع لطمه و آسیب به کیان خانواده گردد. واژگان کلیدی: فضای مجازی، انتشار، اسرار شخصی، اسرار خانوادگی

روش تحقیق

نوع تحقیق توصیفی ـ تحلیلی می باشد به بیان دیگر روش تحقیق این طرح، توصیفی وغیرتجربی واز نوع همبستگی و همخوانی است به این دلیل که آنچه را که هست توصیف می کند، شامل جمع آوری، ثبت ، تجزیه وتحلیل وتفسیر شرایط موجود است و گردآوری اطلاعات، به شیوه ی کتابخانه ای و مراجعه مستقیم به منابع و مآخذ با استفاده از فیش برداری است.

فصل ۱؛ امنیت محتوا و حریم شخصی

اطمینان از حفظ حریم خصوصی داده ها به بیش از مجموعه خاصی از فنون یا فناوری نیاز دارد. همچنین شامل آموزش هر کارمند با دسترسی به داده های حساس در مورد فرایندهای تأیید شده حفاظت از داده است. همانطور که یک خلبان هواپیما از چک لیست استفاده می کند تا اطمینان حاصل شود که موارد مهم قبل از پرواز بررسی می شود و در طول پرواز نظارت می‌شود، فناوری اطلاعات حرفه ای نیز باید بتواند و مایل است از سیاست های حفظ حریم خصوصی امنیت داده ها و سایر منابع برای اطمینان از حریم خصوصPii و سایر اطلاعات حساس استفاده کند.

به طور خاص، برای اطمینان از حریم خصوصی داده ها، متخصصان فناوری اطلاعات باید مجموعه ای از دستورالعمل ها، فرآیندها و رویه هایی امنیتی را اجرا کنند که به طور مفصل درباره چگونگی جمع آوری، ذخیره سازی و استفاده از اطلاعات حساس توسط شرکت و کارمندان آن در تمام سیستم های آن توضیح دهد. هدف از این سیاست حفظ حریم خصوصی این است که اطمینان حاصل شود همه کارمندان به اهمیت امنیت و حریم خصوصی داده ها پی برده، از قرار گرفتن در معرض نامناسب داده ها جلوگیری کرده و می دانند که چگونه با مسائل مربوط به امنیت و نقض خط مشی برخورد کنند.

بند ۱؛ امنیت محتوا

نقض حریم خصوصی داده ها دیگر فقط برای سازمانها خجالت آور و ناراحت کننده نیست. اکنون، قوانین امنیت وحریم خصوصی مانند HIPAA (قوانین حفظ حریم خصوصی ایالات متحده) و GDPR در اتحادیه اروپا مجازاتی را برای عدم حفظ حریم خصوصی piiو سایر اطلاعات شخصی بسیار حساس مجازات می کنند. این استانداردهای انطباق می تواند تحریم های مالی و حتی اتهامات کیفری را برای قرار گرفتن عمدی و حتی گاهی غیر عمدی PII اعمال کند. HIPAA بر محافظت از اطلاعات شخصی مربوط به مراقبت های بهداشتی در ایالات متحده متمرکز است، در حالی که GDPR مجموعه گسترده ای از استانداردهای حریم خصوصی و الزامات انطباق نظارتی را به هر شرکتی که piiساکنان اتحادیه اروپا را ذخیره یا پردازش می کند، تحمیل می کندودر صورت نقض مجازاتی برای آن وضع کرده است.

در حالی که حریم خصوصی داده ها از طریق مجموعه ای از سیاست ها و رویه هایی که برای حفاظت از حریم خصوصی دادهها طراحی شدهاند اجرا می شود، امنیت دادهها شامل استفاده از استراتژی های فیزیکی و منطقی برای محافظت از اطلاعات در برابر نقض داده ها، حملات سایبری و از بین رفتن تصادفی یا عمدی داده ها است.

به طور خاص امنیت داده ها ، فناوری ها و تکنیک هایی است که شرکت ها برای جلوگیری از موارد ذیل اجرا می کنند:

- دسترسی غیرمجاز
- از دست دادن عمدی داده های حساس
- از دست دادن تصادفی یا تخریب داده های حساس

تکنیک های خاص برای امنیت داده ها شامل احراز هویت چند عاملی، چندین لایه کنترل دسترسی در شبکه و لایه برنامه و تشخیص و جداسازی دستگاه های غیرمجاز به محض اتصال به شبکه است. پشتیبان گیری منظم و برنامه های آزمایش شده برای بازیابی نیز قسمت بزرگی از امنیت داده ها است.

بند ۲ ; محتوای اطلاعات و پردازش اطلاعات

داده به تنهایی به درد نمی خورد. باید قابل ارائه و برای گیرنده دارای ارزش باشد. وقتی که چنین شد و معنای مشخص پیدا کرد، به اطلاعات تبدیل می‌شود. به طور مثال مجموعه‌ای از صداها که یک ویژگی خاص دارند (مثل شدت صوت، فرکانس و ...) داده هستند اما اینکه بدانیم این صدا، صدای یک اتومبیل است در حیطه اطلاعات تعریف می‌شود. به بیان دیگر می‌توان گفت اطلاعات، داده هایی گروه بندی شده، ذخیره و حتی پالایش و حتی سازماندهی شده هستند تا برای استفاده فرد یا افرادی خاص، ارزشمند بشوند.

فصلنامه علمی (مقاله علمی-پژوهشی) جامعه‌شناسی سیاسی ایران، سال سوم، شماره دوم (پیاپی ۱۰)، تابستان ۱۳۹۹

بند ۳ ; محتوا

دیتاها شامل مواردی چون دانسته ها، آگاهی ها، داشته ها، آمارها، شناسه ها، پیشینه ها و پنداشته ها، نشانه ها، معانی یا مقادیر یا ویژگی های قابل اندازه گیری می‌باشند. این نشانه ها می‌توانند شکلهای متفاوتی داشته باشند؛ از علایم گرفته تا اشکال نقاشی شده و کلمات چاپ شده. حتی امواج صدا را میتوان داده در نظر گرفت. گاهی در قلمرو ذهنی، «داده»ها را محرکهای حسّی معرفی کرده اند که از راه حواس، دریافت (یا درک) می‌شوند. برای مثال، صداهایی که می‌شنویم، داده هستند.

در تعریف کلی، محتوا به هر واحد اطلاعاتی اطلاق می‌شود که به‌صورت دیجیتالی ارائه شود و به صورت الکترونیکی قابل مدیریت باشد. این محتوا می‌تواند به‌صورت هر یک از موارد: صفحات‌وب، تصاویر، ویدئو، انیمیشن، مستندات، فایل‌هایPDF، و اطلاعات ذخیره شده در بانک‌های اطلاعاتی در دسترس عموم قرار گیرد.

محتوا در اصل هر واحد اطلاعاتی است که به‌صورت دیجیتال عرضه شده و شامل متن، عکس، گرافیک، فیلم، صوت، سند یا هر چیز مشابه دیگر است. به‌عبارت دیگر محتوا واحد اطلاعاتی است که به‌صورت الکترونیکی قابل مدیریت باشد.

فصل ۲ ; ساخت محتوا

محتوا هر بسته اطلاعاتی با هر فرمت و قالبی است که بر روی اینترنت منتشر شده باشد و دسترسی به‌آن نیاز به مقررات ویژه‌ای نداشته باشد. در واقع هر نوع اطلاعات که در اشکال مختلف صوتی، تصویری، متنی، صفحات وب، انیمیشن و فیلم که در قالب‌های دیجیتالی در محیط وب قرار می‌گیرد، به‌عنوان محتوا در اینترنت تعبیر می‌شود. اصولاً فلسفه شبکه‌های اطلاعاتی انتشار و انتقال اطلاعات برروی شبکه است. بدون اطلاعات و محتوا، شبکه معنا و مفهومی ندارد. ارزش هر شبکه‌ای به‌حجم اطلاعات موجود در بستر آن است نه لزوما به تکنولوژی انتقال آنها.

سابقه ورود اینترنت به‌ایران به‌سال ۱۳۷۲ بر می‌گردد سالی که مرکز فیزیک نظری با یک لینک ارتباطی به‌یکی از دانشگاه‌های اروپا وصل شد اما عمومی‌شدن اینترنت در ایران از سال ۱۳۷۶ آغاز شد مهمترین رخداد در این زمینه برگزاری اجلاس سران کشورهای عضو کنفرانس اسلامی در تهران بود، که یکی از مقررات پروتکل‌های آن ایجاد ایستگاه‌های اتصال به‌اینترنت در پانل‌های سالن اجلاس بود. وب ایرانی از آن سال به بعد شروع به رشد کرد

بند ۲ انواع امنیت مجازی

امنیت سایبری یک مؤلفه مهم زیرساخت های شرکت یا سازمان است. این موضوع در خصوص سازمان های حاکمیتی و امنیتی انتظامی که جایگاهی نظارتی دارند ، می‌تواند خطیر ارزیابی گردد. موفقیت در توانایی یک سازمان به محافظت از اطلاعات اختصاصی و داده های مشتری در مقابل افرادی که سوء استفاده می کنند بستگی دارد.

معنی امنیت سایبری برابراست با: برنامه ریزی و اقدام برای حفاظت سیستم ها، شبکه ها، دیتابیس ها و برنامه ها از حملات دیجیتال و سازماندهی یک استراتژی دفاعی علیه مجرمان اینترنتی و اقدامات مخرب آنها. این حملات سایبری معمولا به منظور دستیابی، تغییر و از بین بردن اطلاعات حساس، اخاذی و دزدی پول از کاربران یا متوقف کردن فرآیندهای معمول کاری است. یک رویکرد امنیت سایبری موفق، دارای چندین لایه حفاظت در سراسر کامپیوترها، شبکه ها، برنامه ها یا دیتابیس هایی است که شخص قصد دارد از آنها حفاظت کند. در یک سازمان، افراد، فرآیندها و تکنولوژی باید همگی یکدیگر را کامل کنند تا یک دفاع موثر از حملات سایبری را به وجود آورند.

امنیت سایبری شامل یک سری پروتکل یا دستورالعمل است که یک شرکت یا یک فرد برای اطمینان از اطلاعات از "ICA" خود پیروی می کند. ICA مخفف کلمات یکپارچگی، محرمانه بودن و در دسترس بودن می باشد. اگر سازمانها از امنیت مناسبی برخوردار باشد، می توان خیلی سریع در مواقع قطعی برق، خطاها یا خرابی های هارد را بازیابی کرد. زیرا این نوع حوادث باعث می شود که کارایی سازمانها در برابر حملات خارجی و هکرها آسیب پذیرتر شود.

چالش های امنیت سایبری

بهترین استراتژی های امنیت سایبری فراتر از اصول ذکر شده در بالا است. هر هکر پیشرفته می تواند از این دفاع ساده عبور کند. با گسترش یک مجموعه ، امنیت سایبری نیز دشوارتر می شود. به عنوان مثال، "سطح حمله" یک شرکت Fortune ۱۰۰۰ بسیار بزرگتر از یک تجارت کوچک و متوسط است.

گسترش فرصت های حمله برای هکرها

چالش دیگر امنیت سایبری، مقابله با همپوشانی فزاینده بین دنیای فیزیکی و مجازی مبادله اطلاعات است. هرچه اتومبیل‌های بدون راننده و سایر دستگاه های خود تنظیم شده رایج شوند، اینترنت اشیاء (IoT) و سیاست های تجاری BYOD به مجرمان دسترسی بیشتری به سیستم های فیزیکی سایبر می دهد. این امر شامل ماشین ها،

فصلنامه علمی (مقاله علمی-پژوهشی) جامعه‌شناسی سیاسی ایران، سال سوم، شماره دوم (پیاپی ۱۰)، تابستان ۱۳۹۹

کارخانه ها، یخچال هوشمند و توستر در آشپزخانه شما، حتی برای یک دستگاه ضربان ساز پزشکی می باشد. در آینده، نفوذ به یکی از این سیستم ها ممکن است به معنای نفوذ به همه آن ها باشد.

مقررات پیچیده

یک چالش مهم در امنیت سایبری عدم وجود متخصصان واجد شرایط برای انجام کار است. افراد زیادی در سطح پایین طیف امنیت سایبری با مهارت های عمومی قرار دارند. کارشناسان امنیتی که می دانند چگونه از شرکت ها در برابر هکرهای پیشرفته محافظت کنند، نادر هستند. کسانی که می دانند چگونه کارها را انجام دهند می دانند که چقدر این امر اهمیت دارد.

در نظام حقوقی و حاکمیتی ایران هیچ نهاد یا دستگاه اجرایی مسولیت تدوین باید ها و نباید های فضای مجازی را نمی پذیرد کنترل و نظارت بر محتوا بین سازمانها ،نهادها و وزارتخانه ها سرگردان و هیچ پاسخگوی قانونی وجود ندارد.

فصل ۳ ; امنیت شبکه

امنیت یک شبکه از یک شرکت در برابر دسترسی و نفوذ غیرمجاز محافظت می‌کند. امنیت مناسب بر روی یک شبکه همچنین می‌تواند تهدیدات داخلی برای سیستم را پیدا کرده و از بین ببرد.

اجرای مؤثر امنیت شبکه غالباً نیاز به برخی سازش‌ها بین امنیت و بهره‌وری دارد. به عنوان مثال، ورود به سیستمی که دارای محافظت از اطلاعات است، از دسترسی غیرمجاز به اطلاعات جلوگیری می کند، اما همچنین باعث کاهش بهره وری شرکت می شود. یکی از مشکلات قابل توجه امنیت شبکه این است که از منابع زیادی استفاده می کند.

ابزارهای امنیتی شبکه مقادیر عظیمی از داده ها را تولید می کنند. حتی اگر یک سیستم امنیتی شبکه تهدیدی پیدا کند، ممکن است به دلیل حجم بالای داده هایی که تولید می شود، شکاف را از بین نبرد. تیم های فناوری اطلاعات اکنون در حال استفاده از یادگیری ماشین برای شناسایی خودکار تهدیدات امنیتی هستند که از این طریق خطای انسانی را کاهش می دهند.

بند ۱ ; انواع تهدیدهای امنیت سایبری

تخلفات سایبری می تواند اشکال مختلفی از جمله موارد زیر را به خود اختصاص دهد:

- **بدافزارها (Malware) :** نوعی نرم افزار مخرب است که در آن می توان از هر فایل یا برنامه ای برای آسیب رساندن به کاربر رایانه مانند کرم ها، ویروس های رایانه ای، Trojanها و نرم افزارهای جاسوسی(Spyware) استفاده کرد.

- **باج افزارها (Ransomware) :** نوعی بدافزار است که شامل یک مهاجم است که فایلهای سیستم رایانه قربانی را قفل می کند. این کار معمولاً از طریق رمزگذاری صورت می گیرد و خواستار پرداخت پول برای رمزگشایی و باز کردن قفل آنها است.

- **مهندسی اجتماعی (Social Engineering) :** سوء استفاده زیرکانه از تمایل طبیعی انسان به اعتماد کردن است، که به کمک مجموعه‌ای از تکنیک‌ها، فرد را به فاش کردن اطلاعات یا انجام کارهایی خاص متقاعد می‌کند.

- **فیشینگ (Phishing) :** نوعی کلاهبرداری که در آن ایمیل های جعلی ارسال می شود که شبیه ایمیل از منابع معتبر است .با این حال، هدف از این ایمیلها سرقت داده های حساس مانند کارت اعتباری یا اطلاعات ورود به سیستم است

بند ۲ ; تعریف حریم خصوصی

هر چند که قانونگذاران هرگز به انتظار تعریف باقی نمانده و با وضع قوانین متعدد ابعاد گوناگون حریم خصوصی را مورد حمایت قرار می دهد. موارد ذیل نمونه هایی از تعاریف ارائه شده غربی است:

- شخصی که تنها به حال خود رها شود.
- تمایل اشخاص به اینکه آزادانه تصمیم بگیرند که تحت چه شرایطی و تا چه میزانی خود، وضعیت و رفتارشان را برای دیگران فاش کنند.
- حق اشخاص دایر بر اینکه در مقابل هر گونه مداخله در زندگی یا امور شخصی یا امور خانوادگی از طریق ابزارهای فیزیکی ای افشاء اطلاعات مصون بمانند.
- حریم خصوصی متشکل از سه رکن می باشد: محرمانگی، گمنامی، و تنهایی

هر یک از تعاریف سعی دارند تا عناصر مهم و ارکان مهم حریم خصوصی را به تصویر بکشند. در اینجا بدون آنکه قصد داوری و ارزیابی تک تک این تعاریف را داشته باشیم. بایستی بیان نمود که عنصر اساسی حریم خصوصی میزان وقوف و مداخله سایرین نسبت به زندگی شخصی ایشان است. [۱]

حریم خصوصی در سراسر جهان در مناطق و فرهنگ های مختلف به رسمیت شناخته شده است. این حق در اعلامیه جهانی حقوق بشر، پیمان بین المللی حقوق مدنی و سیاسی، پیمان حقوق بشر اروپا و بسیاری دیگر از معاهده های بین المللی و منطقه ای حقوق بشر حفاظت شده است. تقریباً تمام کشورهای جهان در قانون اساسی خود حق حریم خصوصی را پیش بینی کرده اند. این قوانین به طور حداقلی شامل محرمانگی ارتباطات میشوند.

شورای اروپا طی قطعنامه ۱۹۷۰/۴۲۸حریم خصوصی را چنین تعریف نمود:

حریم خصوصی مربوط می‌شود به حیطه خصوصی، خانوادگی و مسکن، تمامیت روحی و جسمی، آبرو، اعتبار، شهرت و حیثیت افراد، اجتناب از اینکه چهره‌ای کاذب از خود ساخته شود، افشا نکردن حقایق و وقایع نامربوط و آزار دهنده، عدم افشای غیرمجاز تصاویر خصوصی، حمایت از عدم افشای اطلاعات که بر اثر اعتماد اشخاص دریافت کرده‌اند یا در اختیار آن‌ها قرار داده شده است.

تعریف فضای مجازی

- براساس جلسه بیست و دوم دی ۱۳۹۳شورای عالی فضای مجازی
- فضایی است متشکل از شبکه های ارتباطی که در آن محتوا و خدمات مفید در چارچوب مبانی و ارزش های اسلامی و قوانین و مقررات کشور ارایه می شود و کاربران می توانند بر اساس ویژگی های جمعیتی از محتوا و خدمات مورد نیاز بهرمند شوند و حتی الامکان در برابر محتوا و رفتارهای آسیب زا محفوظ بنماید

بند ۳ ; چشم انداز اتحادیه جهانی مخابرات به امنیت ICT

در حوزه استانداردسازی اتحادیه جهانی ارتباطات (ITU-T)، گروه مطالعاتی ۱۷ (SG۱۷) امور مربوط به امنیت را در تمام گروه‌های مطالعاتی ITU-T هماهنگ می‌کند. گروه مذکور که اغلب در همکاری با سایر سازمان‌های توسعه استاندارد (SDO) و کنسرسیوم‌های مختلف صنعت ICT کار می‌کند، با طیف گسترده‌ای از مسائل استانداردسازی سروکار دارد.

---

[۱] اصلانی، حمید رضا، «حقوق فناوری اطلاعات»، تهران، انتشارات میزان، چاپ اول، (۱۳۸۴) ص۱۸-۲۰

به عنوان مثال، SG۱۷ در حال حاضر درخصوص امنیت سایبری، مدیریت امنیت، چارچوب‌ها و معماری‌های امنیت، مقابله با هرزنامه، مدیریت هویت، حفاظت از اطلاعات قابل شناسایی شخصی، امنیت برنامه‌ها و سرویس‌ها برای اینترنت اشیا (IoT)، شبکه هوشمند، تلفن‌های هوشمند، شبکه نرم افزار-محور (SDN)، خدمات وب، تجزیه و تحلیل کلان‌داده، شبکه‌های اجتماعی، رایانش ابری، سیستم‌های مالی تلفن همراه، IPTV و تله بیومتریک به انجام مطالعات و واکاوی مباحث مشغول است.

یکی از مرجع‌های کلیدی استانداردهای امنیتی که امروزه از آن استفاده می شود، توصیه‌نامه ITU-T X.۵۰۹ برای احراز هویت الکترونیکی از طریق شبکه‌های عمومی است. این توصیه‌نامه سنگ بنایی در طراحی برنامه های مربوط به زیرساخت های کلید عمومی (PKI) است و در طیف وسیعی از برنامه ها استفاده می شود. در واقع این توصیه‌نامه از ایمن سازی ارتباط بین یک مرورگر و یک سرور در وب، تا ارائه امضاهای دیجیتال بهره می‌برد که امکان انجام معاملات تجارت الکترونیکی را با اطمینان به همان سیستم سنتی فراهم می کند. بدون پذیرش گسترده استاندارد مذکور، ظهور تجارت الکترونیکی غیرممکن بود.

امنیت سایبری همچنان در دستور کار SG۱۷ قرار دارد. علاوه بر این، SG۱۷ در حال هماهنگی کارهای استانداردسازی امنیتی است که شامل مبارزه با سرقت دستگاه های تقلبی و موبایل، IMT-۲۰۲۰، فناوری داده های رویداد مبتنی برابر، سلامت الکترونیکی، چارچوب اعتماد هویت باز، شناسه فرکانس رادیویی (RFID) و محافظت آنلاین از کودکان است.

در ادامه، قطعنامه‌های مرتبط با مسائل امنیت در مجموعه قطعنامه‌های حوزه استانداردسازی اتحادیه جهانی ارتباطات (ITU-T) عنوان گردیده است[۲].

قطعنامه ۵۰: امنیت سایبری

قطعنامه ۵۲: مقابله و مبارزه با هرزنامه (اسپم)

قطعنامه ۵۸: تشویق برای ایجاد تیم های ملی پاسخگویی به حوادث رایانه ای ، به ویژه برای کشورهای در حال توسعه

قطعنامه ۶۱: مقابله و مبارزه با سوءاستفاده از منابع شماره‌گذاری بین المللی ارتباطات

قطعنامه ۸۴: مطالعات مربوط به حمایت از کاربران خدمات مخابراتی / فناوری اطلاعات و ارتباطات

[۲] https://www.itu.int/pub/T-RES

قطعنامه ۹۶: مطالعات در زمینه مبارزه با دستگاه های تقلبی مخابراتی / فناوری اطلاعات و ارتباطات

قطعنامه ۹۷: مبارزه با سرقت دستگاه‌های تلفن همراه

امنیت سایبری در کنفرانس سران مختار

در قطعنامه نهایی کنفرانس سران مختار سال ۲۰۱۸ (Plenipotentiary Conference - ۲۰۱۸)، مسئله امنیت سایبر در قالب یکی از بندهای هدف راهبردی پایداری (Sustainability) در نظر گرفته شده است:

هدف ۳-۱: تا سال ۲۰۲۳، آمادگی امنیت سایبری کشورها با قابلیت های کلیدی: برخوردار بودن از برنامه راهبردی، تیم‌های ملی واکنش به حوادث/سوانح رایانه‌ای و قوانین و مقررات لازم بهبود یابد.

همچنین قطعنامه ۱۳۰ با عنوان "" تقویت نقش ITU در ایجاد اطمینان و امنیت در استفاده از فناوری‌های اطلاعاتی و ارتباطی" به موضوع امنیت پرداخته است. در بخش resolve این قطعنامه به مواردی از جمله لزوم ارتقای درک مشترک دولت‌ها و ذینفعان در خصوص مفهوم اطمینان و امنیت، لزوم همکاری با سایر نهادهای بین‌المللی ضمن پرهیز از موازی‌کاری، پرهیز از ورود ITU به مسائل داخلی دولت‌ها در خصوص مقررات‌گذاری و امنیت ملی، تقویت چارچوب‌های امنیت و اطمینان و ... پرداخته شده است.

فصل ۴

قطعنامه مصوب مجمع عمومی ۱۸ دسامبر ۲۰۱۳ سازمان ملل ۶۸/۱۶۷ حق خصوصی در عصر دیجیتال

۱-حق حریم خصوصی را مورد تائید قرار میدهد که بر اساس آن هیچ شخصی مورد نقض خود سرانه و غیر قانونی حریم خصوصی، خانوادگی، خانگی و مکاتبات و حق حمایت قانون در برابر این موارد نقض بر اساس ماده ۱۲ اعلامیه جهانی حقوق بشر و ماده ۱۷ معاهده جهانی حقوق مدنی و سیاسی قرار نخواهد گرفت.

۲-ماهیت جهانی و آزاد اینترنت و پیشرفت سریع فناوری های ارتباطات و اطلاعات را به عنوان عامل محرک تسریع پیشرفت توسعه در قالب برای مختلف آن به رسمیت میشناسد؛

۳-تائید میکند حقوقی که افراد بر فضای خارج از اینترنت دارند، در فضای بر خط (آنلاین) نیز وجود دارد که شامل حریم خصوصی نیز میشود.

۴-از تمامی دولت ها میخواهد :

الف) احترام و حمایت از حق حریم خصوصی از جمله در قالب ارتباطات دیجیتال مد نظر داشته باشند .

ب) انجام اقداماتی برای خاتمه نقض این حقوق و ایجاد شرایطی برای پیشگیری از نقض حقوق از جمله با تضمین اینکه قوانین ملی با تعهدات دولت ها بر اساس قوانین بین المللی حقوق بشر همخوانی داشته باشد؛

پ)بررسی روندها، رویه ها و مقررات مربوط به نظارت بر مکاتبات، استراق آنها و جمع آوری اطلاعات از جمله نظارت، استراق و جمع آوری با توجه به حفظ حق خصوصی با تضمین اجرای کامل و موثر تمامی تعهدات بر اساس قوانین حقوق بشر بین المللی؛

ت) ایجاد و حفظ مکانیسم های مستقل نظارت موثر داخلی که شفافیت، تناسب و مسئولیت پذیری نظارت دولت بر مکاتبات، استراق و جمع آوری داده ها را تضمین نماید؛

۵-از کمیسیونر عالی حقوق بشر سازمان ملل در خواست میکند گزارشی در مورد حمایت و ترویج حق حریم خصوصی در قالب نظارت داخلی و فرا منطقه ای و استراق مکاتبات دیجیتال و جمع آوری داده های شخصی به بیست و هفتمین نشست شورای حقوق بشر و شصت و نهمین نشست مجمع عمومی به منظور ارائه توصیه هایی که مورد توجه کشورهای عضو قرار گیرد، تسلیم نماید.

۶-تصمیم به بررسی این مسئله در نشست شصت و نهم تحت عنوان فرعی ((ابهامات حقوق بشر از جمله راهبردهای جایگزین برای بهبود بهره مندی موثر از حقوق بشر و آزادی های اساسی)) تحت عنوان اصلی ((ترویج و حمایت از حقوق بشر)) گرفته شد

بند ۱ ; حق حریم خصوصی در عصر دیجیتال – ۹ آوریل ۲۰۱۸

شورای حقوق بشر در تاریخ ۲۳ مارس ۲۰۱۷، قطعنامه شماره ۳۴/۷ را در مورد ((حق حریم خصوصی عصر دیجیتال)) تصویب نمود. بند ۱۰ قطعنامه از کمیسیونر عالی حقوق بشر سازمان ملل متحد در خواست میکند تا قبل از نشست سی و هفتم شورای حقوق بشر، اقدام به سازماندهی کارگاه کارشناسی با هدف شناسایی و تشریح اصول، استانداردها و بهترین روش های ترویج و حفاظت از حق حریم خصوصی در عصر دیجیتال و از جمله مسئولیت شرکت های تجاری در این رابطه کرده و گزارشی در مورد آن تهیه نموده و به نشست سی و نهم شورا ارائه نماید.

برای کسب اطلاعات بیشتر به نشانی زیر مراجعه فرمایید :

\http://www.ohchr.org/EN/issues/Digital/Ago/Pages/ReportPrivacy.aspx

بند ۲ ;حفاظت از داده ها

از میان تمامی حقوق موجود برای بشر در چارچوب بین المللی، حریم خصوصی شاید دشوارترین موضوع برای تعریف حریم خصوصی بر اساس قالب و محیط تفاوت گسترده ای دارند. در بسیار از کشورها این مفهوم با حفاظت از داده ها تعویض شده است که حریم خصوصی را بر حسب مدیریت اطلاعات شخصی تفسیر میکند.

خارج از این قالب نسبتاً سختگیرانه، حفاظت از حریم خصوصی به عنوان راهی برای مرزکشی جامعه انسانی برای امور شخصی فرد نگرسته میشود. عدم وجود تعریفی یکسان نباید سبب بی اهمیت انگاشتن این موضوع شود. چنانکه نویسنده ای مشاهده کرد « از یک لحاظ تمامی حقوق بشر جنبه هایی از حق حریم خصوصی وی هستند».

حفاظت از داده ها نیز به عنوان حریم خصوصی اطلاعات تلقی شده و شامل ایجاد قوانینی حاکم بر جمع آوری و رسیدگی به اطلاعات شخصی از جمله اطلاعات اعتباری، پزشکی و سوابق دولتی میشود.

حفاظت از داده ها به نوبه خود مفهومی جدید محسوب نمیشود اما بدل به مسئله ای بسیار مهم در عصر دیجیتال شده است. حفاظت از داده ها به طوری فزاینده بخشی از جریان مباحث حقوقی شده است که بخشی از به دلیل رشد روزافزون تجارت الکترونیک است. حفاظت از داده ها را میتوان به عنوان اقداماتی حفاظتی برای مراقبت از یکپارچگی، حریم خصوصی و امنیت داده ها تلقی کرد. نکته اساسی در بحث حفاظت از داده ها اختیار شخص یا توانایی فرد برای دسترسی به اطلاعات شخصی خودش است. اما جمع آوری، دستکاری و استفاده از اطلاعات شخصی به طور روزافزونی برای شرکت ها ساده شده است.

Lawrencet.Greenberg.seymourE.Goodman.Kevinj.soo

Hoo، National Defense university press ۱۹۹۸

مسئله اصلی اقداماتی است که برای کنترل و سرکوب اعمال تروریستی صورت گرفته است. در حالی که این اقدامات به شدت ضروری هستند، باید با توجه به حق حریم خصوصی افراد نیز متناسب باشند.

نیازی فوری به توسعه حداقل استانداردها در سطح بین المللی برای کنترل مالکیت و استفاده از داده های شخصی وجود دارد.

حفاظت از اطلاعات مربوط به افراد که در کامپیوترها نگهداری و ذخیره میشود مستلزم آن است که پایگاه داده ها حاوی اطلاعات شخصی به ثبت رسیده و سپس اصول زیر در آن پیاده شود :

- پردازش منصفانه و قانونی
- پردازش برای اهداف محدود
- کفایت، ارتباط و عدم تطویل

- صحت
- عدم ثبت بیش از مدت مورد نیاز
- پردازش در راستای حقوق فردی
- امنیت
- عدم انتقال به اشخاص ثالث بدون حفاظت کافی

بند ۳ ; اتحادیه اروپا

در سال ۱۹۹۵ شورای اروپا دستورالعمل حفاظت از داده ها را به منظور هماهنگی قوانین کشورهای عضو در ارائه سطوح سازگار حفاظت برای شهروندان و تضمین جریان آزاد اطلاعات شخصی در اتحادیه اروپا تصویب کرد. این دستورالعمل مبنایی در سطح مشترک برای حریم خصوصی ایجاد میکند که نه تنها موجب تقویت قانون حفاظت از داده ها میشود بلکه دامنه از حقوق جدید را نیز ایجاد مینماید. این دستورالعمل برای پردازش اطلاعات شخصی در فایل های الکترونیک و دستی استفاده میشود.

یکی از مفاهیم کلیدی در الگوی حفاظت از داده ها در اروپا، قابلیت اجرایی است. داده ها دارای حقوق تثبیت شده در قوانین هستند. هر کشور عضو اتحادیه اروپا دارای کمیسیونر یا آژانس حفاظت از داده ها میباشد که این قوانین را اجراء میکند. انتظار میرود کشورهایی که اروپا با آنها تجارت میکند نیز نیاز به ایجاد سطحی مشابه از نظارت و اجراء پیدا کنند.

براساس دستور العمل حفاظت از داده های اتحادیه اروپا، تمامی کشورهای عضو باید دارای نهادهای اجرایی مستقل باشند. این آژانس ها دارای اختیاراتی قابل توجه خواهند بود. دولت ها باید در زمان تنظیم مقررات مربوط به پردازش اطلاعات با آنها مشورت نمایند؛ این نهادها دارای اختیار انجام بررسی و دسترسی به اطلاعات مربوط به بررسی ها و انجام اقداماتی نظیر معدوم سازی اطلاعات یا ممانعت از پردازش آنها، طرح شکایت قانونی و استماع و صدور گزارش هستند.

این دستورالعمل وظیفه تضمین اینکه اطلاعات مربوط به شهروندان اروپا در کشورهای خارج از اتحادیه اروپا از همان سطح حفاظت در زمان انتقال و پردازش برخوردار یاشند را به دوش کشورهای عضو میگذارد. این الزام و تعهد منجر به فشار فزاینده ای بر کشور های خارج از اتحادیه برای اعمال قوانین حریم خصوصی شده است. کشورهایی که از اجرای این قوانین سر باز بزنند ممکن است قادر به دسترسی به برخی جریان های اطلاعات و به خصوص اطلاعات حساس نباشند.

شورای اتحادیه اروپا در ژوئن ۲۰۰۲ دستورالعمل جدید حریم خصوصی و مکاتبات الکترونیک را صادر نمود. بر اساس شرایط دستور العمل جدید، کشورهای عضو میتوانند قوانین مربوط به حفظ داده های ترافیک و موقعیت کلیه مکاتبات انجام شده بر روی گوشی های، تلفن های ثابت، فکس، ایمیل، چت روم، اینترنت و دیگر ابزار ارتباط الکترونیک را تصویب نمایند. این قوانین برای مقاصدی از جمله امنیت ملی تا پیشگیری، بررسی و تعقیب جرایم کیفری را شامل میشوند.

www.privacy international.org/survey/phr۲۰۰۳/overview.htm

نتیجه گیری

ساماندهی اینچنین فضایی از حساسیت و اهمیت بسیار بالایی برخوردار است و هرگونه خطا و اشتباه در خط-مشی‌گذاری و برنامه‌ریزی می‌تواند پیامدهای ناگواری را متوجه عرصه‌های کلان کشور کند. ممکن است یک خطا در برآورد نیازهای فناورانه، پیامدهای سیاسی در پی داشته باشد یا تنظیم نادرست مناسبات اقتصادی کنشگران فضای مجازی، چالش‌های فرهنگی به بار آورد یا بی‌توجهی به رشد نامناسب شاخص های،به ناکارآیی خدمات عمومی الکترونیکی بیانجامد.

۱- بی‌گمان تشکیل کمیسیون تنظیم مقررات ارتباطی به موجب ماده ۵ قانون وظایف و اختیارات وزارت ارتباطات و فناوری اطلاعات، برای تحقق چنین رسالتی صورت گرفته است. این مرجع موظف است با رصد بالادستی همهٔ برنامه‌ها و مأموریت‌های اجرایی مرتبط با ساختار بخش ارتباطی و فناوری اطلاعات، نبودها، کاستی‌ها و نارسایی‌های هر حوزه را شناسایی و رأسا با پاسخگو نگاه‌داشتن مراجع ذی‌ربط، نسبت به رفع آنها اقدام کند.

و لازم است قوه مقننه ضمانت اجرای قوی برای مصوبات کمیسیون مصوب نماید

- ۲- جنبه های سیاسی –امنیتی ،اقتصادی ،فرهنگی ،اجتماعی و فناوری الزام می نماید تشکل های پنج گانه با عنواوین ذکر شده تشکیل گردد
- شورای عالی و مرکز ملی فضای مجازی بازآفرینی نهادی، ساختاری و تشکیلاتی را در پرتو الگوی پیشنهادی در دستور کار خود قرار دهند و پیرو آن، هریک از قوای سه‌گانه نیز برپایهٔ سیاست‌های مدون شورای عالی فضای مجازی، اقدامات لازم را در دستور کار قرار دهند. برای مثال، مجلس شورای اسلامی با تشکیل کمیسیون فضای مجازی، نسبت به فعال‌سازی کمیته‌های پنج‌گانه و تعامل سازندهٔ آنها با سایر ارکان متناظر آنها در سایر قوا، زیرنظر شورا و مرکز ملی فضای مجازی اقدام کند. همچنین، قوهٔ قضائیه برای برخورد کارآتر و اثربخش با جرایم مرتبط با فضای مجازی، چه در عرصهٔ پیشگیری از وقوع و چه برخورد کیفری با آنها، کمیته‌های تخصصی پنج-

گانه را تشکیل دهد و مقدمات اصلاح حداقل دو ساله قوانین بخش ict را مهیا کند. و قوهٔ مجریه نیز با تشکیل تشکل های پنج گانه فضای مجازی، سازوکار مشابه را برای ساماندهی دستگاه‌های اجرایی ذی‌ربط و وظایف و اختیارات آنها به انجام رساند.تا از تکنولوژی‌های نوین فضای مجازی که امروزه داده‌های خصوصی اقتصادی مانند بیت کوین‌ها و موارد مشابه به‌وجود می‌آیند امنیت داده‌های اقتصادی را تضمین کنند.

- در صورت شکل گیری چنین الگویی فراگیر می توان امید داشت وقتی هکری اقدام به طراحی برای تخریب ،جعل یا ربودن یا... داده های دیگری می نماید همانطور که در فرضیه تحقیق بیان شد حریم اشخاص مورد تجاوز قرار گرفته و با جمع آوری ،سرقت ،شنود ،رهگیری مکالمات و مراسلات مصادیق تجاوز به حریم خصوصی آشکار می شود و حقوقدانان و فقهای مطلع به امور فنی و مهندسی باید و نباید های مسئولیت مدنی در فضای سایبر را روشن تر نمایند .

منابع و ماخذ:

کتابها

۱. ابن منظور، «لسان العرب»، بیروت، داراحیاء التراث العربی و موسسه التاریخ العرب، (۱۴۱۶)
۲. احمد، سلیمان محمد،« ضمان المتلفات فی الفقه الاسلامی»، قاهره، مطبعه السعاده، (۱۴۰۵ ه. ق)
۳. احمدلو، مونا، «حریم خصوصی در فقه و حقوق ایران»، تهران: انتشارات مجد، (۱۳۹۲)
٤. اصلانی، حمیدرضا، «حقوق فناوری اطلاعات»، تهران، انتشارات میزان، (۱۳۸۹)
٥. انصاری، باقر، «حقوق حریم خصوصی»، تهران، انتشارات سمت، (۱۳۹۰)
٦. انصاری، شیخ مرتضی، «فرائد الاصول (الرسایل)، قم، انتشارات مصطفوی، (۱۳۷۴)
۷. انصاری، شیخ مرتضی، «کتاب المکاسب»، جلد ۲، قم، انتشارات دهاقانی ،(۱۳۷۴)
۸. انوری، حسن، «فرهنگ بزرگ سخن»، تهران، انتشارات سخن، (۱۳۸۱)

۹. باستانی، برومند، «جرایم کامپیوتری و اینترنتی ، جلوه ای نوین از بزهکاری»، چاپ ۳، تهران، انتشارات مجد، (۱۳۹۰)

۱۰. باریکلو، علی رضا، «مسئولیت مدنی»، چاپ هشتم، تهران، انتشارات میزان (۱۳۹۷)

۱۱. برقی، ابوجعفر، «المحاسن»، قم: دارالکتب الإسلامیه، چاپ دوم، (۱۳۷۱)

۱۲. سازمان تنظیم مقررات

۱۳. عطار، شیما، «حریم خصوصی در شبکه های اجتماعی مجاز» مجله پژوهش های حقوقی (علمی- ترویجی) ، شماره ۲۴، (۱۳۹۲)، ص ۱۱۸

منابع لاتین :

۱. [۵Douglas v Hello! Ltd (No. ۳] ۲۰۰۳(Ch); [۷۸۶] EWHC ۲۰۰۳) ; EMLR۹۹۶All ER ۶۴۱.) ۲۰۰۳Apr.(۱۱Court: Chancery Division. Judge: Lindsay J. Date of Judgment: /۵rb.com/case/douglas-v-hello-ltd-no-۵http://www.

۲. ۱۹۸۶Electronic Communications Privacy Act (ECPA) of

۳. Fitzgerald، Anne، Fitzgerald، and Brian Fitzgerald، Cyber Law: Cases and Materials on Internet، Digital Intellectual Property and E Commerce Supplementary Material : ۱۴Chapter، Internet Service Provider Liability، ۲۰۰۲LexisNexisButterworths ۲۲, p

۴. Graham J.H. Smith. Internet Law and Regulation. Sweet and Maxwell. Third edition. London. ۲۰۰۲. P. ۱۷۳.

۵. https://www.itu.int/pub/T-RES

۶. https://www.icann.org/resources/pages/spam-phishing-۲۰۱۷-۰۶-۲۰-en