حریم خصوصی در فضای سایبر
«حریم داده‌های الکترونیکی»

کد موضوعی: ۲۹۰
شماره مسلسل: ۸۰۶۹

آبان ماه ۱۳۸۵

گروه ارتباطات و فناوری‌های نوین

فهرست مطالب

حریم خصوصی در فضای سایبر
«حریم داده‌های الکترونیکی»

چکیده

یکی از دغدغه‌های همیشگی بشر متمدن در رابطه با زندگی اجتماعی‌اش این بوده که حریم خصوصی‌اش را از هرگونه تعرض مصون دارد. بدیهی است نگرانی اصلی به نحو قاعده‌مندسازی رابطه شاخه‌های مختلف حاکمیت با اعضای جامعه و همچنین اعضای جامعه با یکدیگر مربوط می‌شود. اما گاهی اوقات، برخی تحولات بنیادین کلیه معادلات را به هم می‌ریزد. بی‌تردید شالوده و محتوای اصلی تمامی امور را اطلاعات تشکیل می‌دهد. عنصری که در عصر حاضر به عنوان ارزشمندترین سرمایه شناخته شده و به همین دلیل، ابزاری بی‌نظیر به نام فناوری اطلاعات و ارتباطات الکترونیک برای بهره‌برداری حداکثر از منافع آن به خدمت گرفته شده است. در فضای سایبر معادلات دنیای فیزیکی قابل اجرا نیست. لذا باید برای داده‌های خصوصی افراد به عنوان انعکاس‌دهنده‌های امور خصوصی‌شان چاره‌جویی اساسی جدیدی کرد. این نوشتار بر آن است تا با تبیین اجمالی مفهوم حریم داده‌های الکترونیکی، چالش‌های بشر امروز را در قبال ساماندهی امور خصوصی‌اش در فضای سایبر مورد بررسی قرار دهد.

مقدمه

از آن زمان که بشر پا به گیتی نهاد، همواره در تلاش بوده برای رسیدن به آرامش و آسایش مطلوبش، مرز مطمئن و غیرقابل گزندی میان امور خصوصی و غیرخصوصی‌اش ایجاد نماید. اموری که نمی‌خواهد جز خودش و آن‌هایی که نسبت به آن‌ها رضایت دارد، دیگران در آن حضور یابند، از آن آگاه شوند یا به هر نحو در آن دخالت کنند. این همان چیزی است که از آن به عنوان **حریم خصوصی**[1] یاد می‌شود.

با این حال، برخلاف ظاهر ساده و کاملاً قاطع این حق که هر کس با مراجعه به وجدان خویش در پذیرش اصل آن تردید نمی‌کند، اما یکی از و حتی شاید بحث‌انگیزترین مباحث حقوق بشری را به خود اختصاص داده است. دلیل اصلی آن هم این است که عوامل بسیار متنوع و حتی متعارضی در

1. Privacy

تعیین حدود و ثغور آن نقش دارند و بر اراده فردی تأثیر می‌گذارند. برای مثال، این‌که حاکمیت جامعه بر چه نظامی استوار است، مانند خودکامه یا مردم‌سالار؛ نحوه وضع و اجرای هنجارهای اجتماعی در قالب‌هایی چون قوانین و مقررات چگونه است و میزان آگاهی و درک افراد جامعه از مفهوم حریم خصوصی چقدر است و تا چه حد حاضرند در نقش‌های مختلف اجتماعی‌ای که عهده‌دار می‌شوند، از حریم خصوصی خود و دیگران حفاظت کنند و به آن احترام گذارند، مانند مجریان قانون یا دیگر افرادی که به حکم قانون یا برحسب وظیفه اجتماعی امکان دخالت در امور خصوصی دیگران را دارند؛ همگی در تحدید یا توسعه حریم خصوصی نقش دارند. البته این حجم تعارض آرا زمانی عینیت بیش‌تری می‌یابد که تحول نگرش افراد را که همگام با تحولات اجتماعی صورت می‌گیرد از نظر دور ندانیم. امروزه تحولات بعضاً بنیادین در حوزه‌های مختلف آنقدر سریع بروز می‌یابند که به خوبی ملاحظه می‌شود دو یا سه نسل همزیست، نسبت به یک موضوع از دیدگاه‌های کاملاً متمایزی برخوردارند.

به این ترتیب، شاید از مجموع تمامی مسائل فوق این‌گونه نتیجه‌گیری شود که دستیابی به راه‌حلی که در آن جمیع مصالح عمومی رعایت گردد و در عین حال، حریم خصوصی افراد محترم شمرده شود، غیرممکن است. با اذعان به این واقعیت، اما ناگزیر باید راهکاری که حداکثر فایده‌مندی را در عین واقع‌گرایی و پایبندی به اصول حاکم بر جامعه عاید می‌کند، اتخاذ گردد. بی‌تردید، توسعه مرزهای حریم خصوصی، باعث فلج شدن بسیاری از امور خرد و کلان جامعه، به‌ویژه حفظ نظم و امنیت ملی خواهد شد، زیرا مجریان قانون با محدودیت‌های بسیاری مواجه می‌شوند و حتی دیگر اقشار جامعه نیز از تبعات آن در امان نخواهند ماند. اما از سوی دیگر، تحدید این مرزها باعث سلب هویت و اختیار عمل از تک‌تک افراد جامعه می‌شود و به دلیل عدم برخورداری از آسایش و آرامش مطلوب، آسیب‌های جبران‌ناپذیری را متحمل خواهند شد.

بر این اساس، به نظر می‌رسد برای ساماندهی حریم خصوصی، ابتدا باید ارکان تعیین‌کننده و تأثیرگذار آن شناسایی گردد. به عبارت دیگر، از کدام منظر می‌توان به سیاستگذاری و قاعده‌مند ساختن این حوزه پرداخت و از آن بیش‌ترین نتایج را کسب کرد؟ این موضوع از آن جهت اهمیت دارد که حریم خصوصی به موضوع، ماهیت، مکان، زمان و خلاصه به هیچ چیز پایبند نیست و مفهومی است که قابلیت اتصاف به هر امر فردی را دارد. لذا باید وجه مشترکی را پیدا کرد که بتواند بدون هیچ محدودیتی تمامی حوزه‌ها را دربرگیرد.

همان‌طور که در ابتدای بحث اشاره شد، حریم خصوصی مجموعه‌ای از امور خصوصی[۱] است. امر خصوصی می‌تواند یک فعل (که البته ترک فعل را هم دربرمی‌گیرد) یا واقعه خصوصی

---

۱. در ابتدای بحث تأکید می‌شود منظور از **خصوصی** معادل Private است و نباید با **شخصی** (Personal) اشتباه گرفت.

باشد. برای مثال، برقراری تماس یک فعل محسوب می‌شود، اما مرگ یک واقعه است. شایان ذکر است ضرورتی ندارد فعل خصوصی رأساً توسط فرد ارتکاب یابد، بلکه ملاک‌های دیگری مورد توجه قرار می‌گیرند که در بخش‌های آتی به آنها خواهیم پرداخت.

با این حال، آنچه در میان کلیه امور وجه مشترک محسوب می‌شود این است که اگر به دنیای خارج انعکاس نیابد، وجود و عدم آن‌ها یکسان خواهد بود. وظیفه این انعکاس به عهده عنصری به نام **اطلاعات**[1] است. مجموعه‌ای از نشانه‌ها و نمادهایی که ماهیت یک واقعه یا فعل را برای یک یا چند حواس پنجگانه قابل درک می‌سازند. بدیهی است امور خصوصی نیز از این قاعده مستثنا نیستند و آگاهی از آنها منوط به دستیابی به اطلاعات راجع به آنها می‌باشد. لذا نتیجه منطقی که می‌توان از این مقدمات گرفت این است که برای **حفظ حریم اشخاص**، باید **اطلاعات راجع به امور خصوصی** آنها محافظت گردد. زیرا هرگونه تعرض به اطلاعات خصوصی، به معنی نقض حریم خصوصی است.

همچنین، با توجه به اهمیت و آثار مستقیمی که اطلاعات بر حریم خصوصی دارد، بایسته و ضروری است کلیه تحولات و دگرگونی‌های آن را به دقت دنبال کرد. ممکن است به مرور زمان از جایگاه و ارزشی برخوردار شود که هرگونه ابتکار عمل بر روی آن مستلزم رعایت پیش‌شرط‌ها و اقدامات بسیاری باشد یا این‌که انعکاس آن در بستر ابزاری تحقق یابد که از ویژگی‌های خاص و منحصر به فردی برخوردار است، تا حدی که به کلی حوزه اطلاعات را تحت‌الشعاع شرایط خاص خود قرار دهد. تمامی این مسائل می‌تواند در نحوه تصمیم‌گیری راجع به حریم خصوصی نقش تعیین‌کننده‌ای داشته باشند.

شایان ذکر است، عصر حاضر به خوبی هر دو رویداد بزرگ فوق را درک کرده است. امروزه بیش از هر زمان دیگر، ارزش واقعی اطلاعات شناخته شده و اکنون نزد صاحبان خرد به عنوان گرانبهاترین و ارزشمندترین سرمایه محسوب می‌شود، تا حدی که شایستگی اتخاذ عنوان عصر حاضر را از آن خود کرده و همان‌طور که می‌دانیم، این دوران **عصر اطلاعات** نام گرفته است.

بدیهی است در چنین دورانی به سادگی نمی‌توان راجع به این سرمایه ارزشمند تصمیم‌گیری کرد یا بدون رعایت بسیاری مسائل دیگر، حتی حدود و ثغور اطلاعات خصوصی افراد را تحدید کرد یا وسعت بخشید. یک کنش به ظاهر کم‌اهمیت و جزئی، به خوبی می‌تواند بازتاب گسترده‌ای داشته باشد. لذا هر اقدامی با احتیاط بسیار انجام می‌شود.

در این راستا، برای این‌که عالی‌ترین اهداف ترسیم‌شده از طریق بهره‌برداری از این سرمایه ارزشمند محقق گردد، تا به حال سعی شده هرگونه مانع و مزاحمی از سر راه برچیده شود. یکی از

1. Information

موانع اصلی، ضعف در جمع‌آوری و ذخیره‌سازی هرچه بیش‌تر اطلاعات و عدم ابزارهای کافی برای پردازش‌های گوناگون برای دستیابی به داده‌های فراوری شده ارزشمندتر بوده است. برای حل این مشکل اساسی، حدود نیم‌قرن پیش، دانشمندان ابزاری به نام **رایانه الکترونیک** را به جامعه بشری معرفی کردند که طی این مدت نه تنها خود آن با چندین دوره تحول بنیادین مواجه بوده که به تبع آن اطلاعات را به طور کامل دگرگون ساخته است. تا حدی که آنچه اکنون راجع به میزان و سرعت دسترس‌پذیری و تنوع و سرعت پردازش داده‌ها در عین حفظ تمامیت آن‌ها ملاحظه می‌شود، حتی در تخیل انسان‌های یک قرن گذشته نیز نمی‌گنجید.

پس از آن‌که اولین رایانه الکترونیکی با نام ENIAC در سال ۱۹٤٦ راه‌اندازی شد، حدود سه دهه طول کشید تا امتیاز و توانایی بهره‌برداری از ابررایانه‌هایی که در اختیار گروهی از متخصصین ارشد و صاحبان بنگاه‌های بزرگ اقتصادی یا مراکز دولتی مهم بودند، از انحصارشان خارج شود و همان‌گونه که **بیل گیتس** آرزویش را داشت، در مقیاس‌های بسیار کوچک‌تر، ولی با کارآیی و تنوع بیش‌تر کارکردهای رایانه‌ای، حتی در منازل مورد استفاده قرار گیرند. البته این فناوری همچنان به‌طور روزافزونی به سمت سادگی و ارزانی پیش می‌رود تا دیگر هیچ‌گونه مانع طبقاتی، مالی، فنی، تخصصی و ... در به‌کارگیری آن وجود نداشته باشد.

اما در میان این همه تغییر و تحولات، آنچه از منظر اطلاعات در بستر سیستم‌های رایانه‌ای قابل توجه است این‌که با تبدیل ابررایانه‌ها به رایانه‌های شخصی کوچک، داده‌های **متمرکز**[1] به داده‌های **غیرمتمرکز**[2] و پراکنده تبدیل شدند. از آن پس، دیگر افراد برای ذخیره‌سازی و پردازش اطلاعاتشان به مراکز ابررایانه‌ها مراجعه نمی‌کردند و در همان محل کار یا منازلشان در مقیاسی محدودتر، ولی تقریباً با همان میزان کارایی امور اطلاعاتی خود را سامان می‌بخشیدند. بدیهی است این وضعیت منجر به پراکنده شدن بخشی از اطلاعات خصوصی شده است و بالطبع سیاستگذاری در حوزه حریم خصوصی را هم تحت‌الشعاع قرار داده است.

اما آنچه خود این تمرکززدایی را با تحول اساسی مواجه ساخته و به واقع وارد عرصه جدیدی کرده است، پیوند سیستم‌های رایانه‌ای به یکدیگر از طریق ارتباطات الکترونیکی است که به تدریج منجر به پیدایش فضای متمایزی از دنیای فیزیکی به نام فضای سایبر[3] شده است. ماهیت لایتناهی این فضا، دیگر رسایی مفهوم تمرکززدایی سیستم‌های رایانه‌ای شخصی را هم از بین برده و قابلیت‌های بدیع و شگفت‌انگیزی در این دنیای بی‌کران به چشم می‌خورد که حتی پایه‌گذاران فناوری اطلاعات و ارتباطات الکترونیکی نیز تصور این انقلاب بنیادین را نداشتند.

---

1. Centralized
2. Decentralized
3. Cyber Space

در چنین فضایی که هیچ‌گونه محدودیت زمانی، مکانی، حجم مورد نیاز برای جمع‌آوری و ذخیره‌سازی داده‌ها و کارکردهای بسیار متنوع پردازش‌های گوناگون با سرعت باورنکردنی در عین حفظ تمامیت آنها وجود ندارد، هر کس در هر موقعیت اجتماعی این اجازه را به خود داده تا برای بهره‌برداری مؤثرتر از سرمایه ارزشمند متعلق به یا در اختیار خودش، جهت حضوری فعال در فضای سایبر تردیدی به خود راه ندهد و آن‌گونه که شاهد هستیم، هرآنچه توانسته متصف به وصف الکترونیکی شود، به این فضا راه یافته است. از داد و ستد[1] و تجارت[2] الکترونیکی، پول[3] و بانکداری[4] الکترونیکی، انواع ارتباطات[5] الکترونیکی، آموزش[6] الکترونیکی، انتخابات[7] الکترونیکی و حتی محاکم[8] الکترونیکی گرفته تا مفاهیم جامع حاکمیتی دولت[9] الکترونیکی و جامعه اطلاعاتی[10]، که بدون هیچ واهمه‌ای از سوی آحاد جامعه به کار می‌رود، به خوبی گویای انس و در عین حال وابستگی روزافزون آن‌ها به فضای سایبر و کارکردهای آن می‌باشد.

با این حال، با کمی ملاحظه دقیق‌تر به هر یک از این حوزه‌های الکترونیکی، به خوبی می‌توان ردپای امور خصوصی اشخاص را به فراخور کارکردهایشان ملاحظه کرد. در حالی که اگر بنا باشد براساس فلسفه وجودی پیدایش فناوری رایانه و به تبع آن فناوری اطلاعات و ارتباطات الکترونیکی عمل شود، نباید محدودیت‌های حاکم بر حریم خصوصی افراد را اعمال کرد. زیرا آنچه در این‌جا معیار قرار گرفته، بهره‌برداری حداکثری از تمامی ظرفیت‌های اطلاعات در فضای سایبر است و هرگونه مانعی می‌تواند این میزان بازدهی را کاهش دهد. بالطبع بخش گسترده‌ای از اطلاعات موجود در فضای سایبر به طور مستقیم یا غیرمستقیم با امور خصوصی افراد ارتباط دارند و هرگونه محدودسازی آن‌ها می‌تواند برای فعالان این عرصه زیانبار باشد.

با این حال، این واقعیت غیرقابل انکار را هم نباید از یاد برد که حفظ حریم داده‌های الکترونیکی به عنوان یکی از جلوه‌های اصلی حریم خصوصی افراد در عصر حاضر، از ارکان اساسی حقوق بشر محسوب می‌شود و هرگونه تغییر و تحولی نباید به بهای زیر پا گذاشتن آن صورت گیرد. لذا تنها راهی که در میان این دو حوزه برگشت‌ناپذیر وجود دارد، یعنی نه امکان برگشت جامعه الکترونیکی به پیش از آن و نه امکان زیر پا گذاشتن اصول مسلم حقوق بشری وجود دارد، اتخاذ یک راهکار متعارف منطقی مبتنی بر اصول مسلم هر حوزه و واقعیات موجود است تا از طرفی لطمات وارده به

1. E-Business
2. E-Commerce
3. E-Cash
4. E-Banking
5. E-Communication
6. E-Learning
7. E-Voting
8. E-Courts
9. E-Government
10. Information Society

هر یک به حداقل برسد و اهداف پیش‌بینی شده برای هر یک به بهترین وجه محقق گردد.

در این راستا، این نوشتار بر آن است در دو بخش به تبیین مفهوم حریم داده‌های الکترونیکی ـ که در واقع تأثیرات متقابل دو حوزه حریم خصوصی و فناوری اطلاعات و ارتباطات الکترونیک است ـ بپردازد. لذا در بخش اول توضیحات کلی و مقدماتی راجع به مفهوم حریم خصوصی و جایگاه داده‌های خصوصی به‌عنوان یکی از ارکان اصلی آن که حتی باعث شده مباحث **راجع به حمایت از داده‌ها** کلیت آن را تحت‌الشعاع قرار دهد ارائه می‌گردد. سپس در فصل دوم به‌طور تخصصی آثار و تبعات کشیده شدن حریم خصوصی افراد به فضای سایبر، هم از بعد مثبت آن، یعنی مطلوبیت‌هایی که این فضا در حفظ آن فراهم آورده و همچنین طرق و عوامل نقض این حق مسلم بشری مورد بررسی قرار می‌گیرد. اما در پایان هیچ‌گونه نتیجه‌گیری از این مباحث به عمل نمی‌آید. زیرا این نوشتار مقدمه‌ای بر گزارش جامع راجع به **طرح حریم خصوصی** که در آینده ارائه خواهد شد محسوب می‌شود و در واقع نتیجه‌گیری‌های آن پیشنهادات اصلاحی یا الحاقی است که در رابطه با این طرح مطرح خواهد شد.

بخش اول- مفهوم حریم خصوصی

در مقدمه ملاحظه شد حریم خصوصی مجموعه‌ای از امور خصوصی است که آن‌ها نیز متشکل از افعال یا وقایع ارتکابی یا منتسب به افراد هستند. اما پرواضح است که از این تعریف مختصر هیچ معیاری نمی‌توان استخراج کرد. زیرا ابهامات آن همچنان پابرجاست. مبنای تفکیک امور خصوصی از غیرخصوصی چیست؟ چه کسی یا چه مرجعی حق دارد یا موظف است نسبت به آن تصمیم‌گیری و تعیین تکلیف کند؟

در هر حال، آنچه مسلم است این‌که به لحاظ تعامل گسترده و مستقیم امور خصوصی با اکثریت قریب به اتفاق شئون زندگی اجتماعی، به‌ویژه در عصر حاضر و همچنین حساسیت‌های زیادی که به دلیل ماهیت حقوق بشری آن وجود دارد، در قاعده‌مندسازی و ساماندهی قوانین و مقررات راجع به آن باید دقت زیادی به خرج داد و به مبانی‌ای تمسک کرد که تاب این امر مهم را داشته باشند.

با توجه به اهمیت موضوع، در این بخش تلاش می‌شود ریشه‌هایی که می‌توان از آن‌ها مفهوم حریم خصوصی و حقوق راجع به آن را استخراج کرد، مورد بررسی قرار گیرد. در این راستا، فصل اول به مباحث راجع به مفهوم خصوصی بودن و فصل دوم به حمایت از داده‌ها و ارتباط آن با حریم خصوصی اختصاص یافته است.

۱. مفهوم خصوصی بودن

از آنچه تاکنون بیان شد، محرز گردید کلید اصلی روشن شدن مفهوم حریم خصوصی و به تبع آن امور خصوصی، روشن شدن مفهوم خصوصی بودن است. در واقع، چنانچه این رکن زیرساخت به خوبی شناسایی و تبیین گردد، در حل مسائل متعاقب آن مشکلی وجود نخواهد داشت. لذا باید این مفهوم به خوبی موشکافی و ریشه‌یابی گردد تا مبانی که برای تبیین آن استخراج می‌گردد، از حجیت کافی برخوردار باشند.

یکی از راه‌هایی که می‌توان به این مقصود رسید، مراجعه به عواملی است که می‌توانند به تعیین حدود و ثغور آن کمک کنند. بی‌تردید در نگاه اول هر یک از اشخاص با توجه به این‌که امور خصوصی به آن‌ها مربوط می‌شود، صالح‌ترین مرجع در تعیین مفهوم خصوصی هستند. به‌عبارت دیگر، هر فرد با توجه به شرایط و اوضاع و احوال بسیار متنوع پیرامون خود، بهترین کسی است که می‌تواند بخشی از امور زندگیش را تحت عنوان امور خصوصی از دیگر امورش جدا سازد.

اما نکته بسیار مهمی که باید مورد توجه قرار داد این است که امور خصوصی در کنار امور غیرخصوصی معنا پیدا می‌کند. به عبارت دیگر، چنان‌چه فردی با هیچ کس در ارتباط و تماس نباشد و به تنهایی زندگی کند، امور خصوصی درباره وی معنایی نخواهد داشت. به‌عبارت دیگر، حریم خصوصی یک مفهوم جمعی است و در جمع معنا پیدا می‌کند. زیرا در این‌جاست که افراد با ترسیم حد و مرز پیرامون اموری که خود آن‌ها را شناسایی کرده‌اند، از ورود دیگران به آن‌ها جلوگیری می‌کنند.

با توجه به این توضیحات، به‌نظر می‌رسد یکی از مؤلفه‌های اساسی که به خوبی می‌تواند در تبیین مفهوم خصوصی بودن مؤثر باشد شناسایی گردید و آن رضایتی[1] است که از اراده فردی برمی‌خیزد. به عبارت دیگر، مهم‌ترین عاملی که می‌تواند مرز میان امور خصوصی و غیرخصوصی را مشخص سازد، رضایت فرد مورد نظر است که در کمال صحت اراده و آگاهی از اوضاع پیرامون خود اعلام کرده است. به همین دلیل، هیچ‌گاه یا به سختی می‌توان دو نفر را پیدا کرد که از امور خصوصی یکسانی برخوردار باشند. زیرا در تعیین این‌که چه کسانی می‌توانند در حریم خصوصی فرد مورد نظر با کسب اجازه‌اش حضور یابند، عوامل و شرایط و اوضاع و احوال بسیاری دخیل هستند.

بنابراین، به نظر می‌رسد با شناسایی عواملی که منجر به صدور **رضایت آگاهانه فردی** می‌شوند، می‌توان به تعریف روشنی از خصوصی بودن و به تبع آن حریم خصوصی دست یافت. ساده‌ترین شکل اعلام رضایت این است که خود فرد صراحتاً و بدون واسطه به فرد یا افرادی

1. Consent

شخصاً رضایت دهد به تمام یا بخشی از امور خصوصی‌اش وارد شوند و دخالت نمایند. حالت دیگر که اتفاقاً امروزه نیز بسیار رایج شده، الزامات قراردادی است. در این‌جا فرد با امضای قرارداد در حوزه‌های مختلف، بخشی از امور خصوصی‌اش را به طرف قرارداد، که می‌تواند شخص حقیقی یا حقوقی باشد، واگذار می‌کند.

اما عام‌ترین حالتی که اتفاقاً بیش از موارد فوق می‌تواند جنبه اجرائی و آثار و نتایج بسیاری به دنبال داشته باشد، قوانین و مقررات مصوب هستند. در یک جامعه مردم‌سالار، که حاکمیت بر پایه اراده اکثریت افراد جامعه قرار دارد، نمایندگان ملت، براساس اختیاری که رأی‌دهندگان آن‌ها با رضایت به آن‌ها تفویض کرده‌اند، حق و وظیفه دارند امور خرد و کلان آن‌ها را از طریق تصویب قوانین مختلف ساماندهی کنند که لاجرم حریم خصوصی یکی از آن‌ها می‌باشد. به این ترتیب، در یک رویکرد کلان می‌توان کلیه قوانین و مقررات مصوب راجع به حریم خصوصی را ناشی از رضایت افراد آن جامعه دانست.

البته ناگفته پیداست احتمال دارد بخشی از افراد جامعه با قوانین و مقرراتی که در رابطه با حریم خصوصی آنها به تصویب می‌رسد موافق نباشند. اما آن‌ها نیز با دیدگاه منطقی‌شان می‌پذیرند که زندگی در یک جامعه متمدن و مردم‌سالار چنین هزینه‌هایی هم دارد و باید به رأی اکثریت احترام بگذارند و اگر آن‌ها هم می‌خواهند نظرات خود را به شکل رسمی منعکس کنند، تنها سازوکار قابل قبول سیر همین رویه است.

در این راستا، صاحبنظران بسیاری سعی کرده‌اند با توجه به دیدگاه‌هایشان حریم خصوصی را تبیین و تعریف کنند. گروهی به رضایت صریح افراد بهای زیادی داده‌اند، اما گروه دیگر واقع‌بینانه‌تر به قضیه نگاه کرده‌اند. برای مثال، پروفسور وستین[1] در رابطه با حریم خصوصی می‌گوید: ادعای افراد، گروه‌ها یا نهادها در تعیین زمان، نحوه و میزان دسترس‌پذیری اطلاعات راجع به خودشان برای دیگران. همان‌طور که ملاحظه می‌شود، در این تعریف بر حق خودتعیینی[2] تأکید ویژه‌ای شده است. اما باید دید در دنیای امروز این ادعا تا چه اندازه قابل قبول است. پرواضح است به میزان مشارکت اجتماعی افراد، حریم خصوصی‌شان تحت تأثیر قرار می‌گیرد و عملاً نمی‌توانند انتظار داشته باشند امور خصوصی‌شان مصون بماند. زیرا خودشان با عنایت به همان رضایتی که مورد تأکید قرار گرفت، خواسته یا به ناچار افراد بیش‌تری را به حریمشان راه می‌دهند. همچنین، نمایندگان ملت که حق و وظیفه حمایت از حریم اشخاص را از طریق وضع مقررات به عهده دارند، باید در حفظ نظم و امنیت جامعه نیز جدی باشند و همین مسأله باعث می‌شود در راستای منافعی

1. Westin, AF
2. Self-Determination

که در نهایت و به‌طور مستقیم عاید خود افراد جامعه می‌شود، از برخی حقوق راجع به امور خصوصی آن‌ها چشم‌پوشی نمایند.

با توجه به همین واقعیات انکارناپذیر، گروهی از صاحبنظران تلاش کرده‌اند با اتخاذ یک رویکرد میانه به راهکارهای منطقی‌تر و مؤثری دست یابند. برای مثال، پروفسور گویسون[1] که از منتقدان اصلی حق خودتعیینی در تبیین حریم خصوصی است و آن را خلاف واقع‌گرایی می‌داند، از منظر دیگری حریم خصوصی را بر سه عنصر بنا نهاده است: ۱. رازداری،[2] ۲. ناشناس ماندن،[3] ۳. خلوت.[4]

منظور از رازداری، محدودیت انتشار اطلاعات راجع به خود است. در ناشناس ماندن، عدم توجه دیگران به هویت خود مد نظر قرار می‌گیرد و منظور از خلوت نیز عدم مجاورت مادی با دیگران تعریف شده است. همچنین، پروفسور فلدمن[5] مفهوم موافقی را اما در سه عنصر رازداری، متانت[6] و خودمختاری[7] منعکس کرده است.

آنچه در این دو تعریف و تعاریف مشابه جلب توجه می‌کند، اشتراک لفظ رازداری است. این عنصر مستقیماً بر آنچه مورد تأکید این نوشتار است، یعنی حریم اطلاعات خصوصی، اشاره دارد. به عبارت دیگر، آنچه افراد در این‌جا دنبال می‌کنند این است که بر اطلاعات معرفشان کنترل و نظارت داشته باشند که به این ترتیب، تنها بحث افشای آن‌ها مطرح نیست و استفاده‌های آتی یا مکرر را نیز دربرمی‌گیرد.

بر این اساس، شایان ذکر است این عنصر تا حدی در قلمرو حریم خصوصی جدی تلقی می‌شود که عده‌ای کل این قلمرو را در حریم اطلاعات خصوصی خلاصه کرده‌اند و حتی در بعضی کشورها، برای حمایت از حریم خصوصی افراد، قوانینی تحت عنوان **حمایت از داده‌ها** به تصویب رسیده است. لذا با توجه به این‌که اولاً اسنادی قانونی تحت عنوان حمایت از داده‌ها برای حمایت از حریم خصوصی افراد وجود دارد، ثانیاً محوریت این نوشتار بر داده‌های خصوصی قرار دارد و بررسی مباحث راجع به حمایت از داده‌ها می‌تواند بر شناخت هرچه بهتر **حریم داده‌های الکترونیکی** مؤثر باشد و در نهایت این‌که برخی پژوهشگران کشورمان با عنایت به همان اسناد قانونی و نوشته‌های حقوقی مطالعاتی را حتی تا مرحله تدوین پیش‌نویس لایحه با عنوان حمایت از داده‌ها پیش برده‌اند در فصل بعد به اجمال مختصر توضیحاتی راجع به مفهوم حمایت از داده‌ها و رابطه آن با حریم خصوصی ارائه خواهد شد.

---

1. Gavison, R
2. Secrecy
3. Anonymity
4. Solitude
5. Feldman, D
6. Dignity
7. Autonomy

۲. مفهوم حمایت از داده‌ها[1] و رابطه آن با حریم خصوصی

به‌طور خلاصه، آن‌گونه که از اصطلاح حمایت از داده‌ها نیز پیداست، غالباً به‌مدیریت اطلاعات خاص گفته می‌شود. به‌عبارت دیگر، این دیدگاه غالباً از سوی کسانی به‌کار می‌رود که به‌دنبال قاعده‌مندسازی و ساماندهی **داده‌های کسب وکار**[2] هستند. لذا در این‌جا آنچه محوریت دارد و در خصوص آن بحث و تبادل نظر زیادی می‌شود، خطرپذیری داده‌ها و مدیریت آن[3] است.

به این ترتیب، همان‌طور که ملاحظه می‌شود، حوزه حمایت از داده‌ها ماهیتی فنی و کاربردی دارد و با حریم خصوصی که یک مفهوم حقوق بشری است تفاوت دارد. اما این نکته را هم نمی‌توان انکار کرد که مباحث این دو حوزه در برخی ابعاد تلاقی‌هایی با یکدیگر دارند. برای مثال، با این‌که مفاهیم خطر و مدیریت آن در میان مشاغل و حِرَف کاربرد دارد، اما حریم خصوصی را هم می‌توان از منظر آن‌ها مورد بررسی قرار داد. بر این اساس، سه عامل خطر می‌توانند به عنوان اجزای تشکیل‌دهنده حریم خصوصی مورد توجه قرار گیرند:

۱. خطر بی‌عدالتی به دلیل نادرستی فاحش داده‌های شخصی، استنتاج ناعادلانه، اقدام تدریجی (استفاده تدریجی از داده‌ها به مقاصدی سوای از آنچه به خاطر آن جمع‌آوری شده‌اند) یا اثبات خلاف اصالت البرائه. برای مثال، در اثر تطبیق داده‌ها[4] که فناوری اطلاعات و ارتباطات الکترونیک به کلی آن را متحول کرده و امکان مرتبط ساختن اکثریت داده‌های راجع به یک فرد را فراهم آورده، ممکن است نسبت به شناختی که نسبت به هر یک از اجزای داده‌ها حاصل می‌گردد، نگرش عمیق‌تری در اثر ملاحظه مجموعه به هم‌مرتبط داده‌ها حاصل شود و تصمیمات جدیدی در خصوص فرد مورد نظر اتخاذ گردد.

۲. کنترل شخصی بر جمع‌آوری اطلاعات شخصی در نتیجه نظارت بیش از حد و ناعادلانه بر جمع‌آوری داده‌ها بدون رضایت مسندٌالیه داده‌ها[5] و همچنین ممانعت یا مأیوس داشتن فعال از به‌کارگیری ابزارهای جبرانی این‌گونه خطرات، مانند نرم‌افزارهای رمزنگاری و ناشناس‌کننده‌ها.

۳. به خطر افتادن متانت در نتیجه افشا یا بروز آشفتگی در نتیجه عدم شفافیت تشریفات اطلاعات، تعرض فیزیکی به فضاهای خصوصی، شناسایی غیرضروری یا عدم ناشناس ماندن یا افشای غیرضروری یا ناعادلانه اطلاعات شخصی بدون کسب رضایت از مسندالیه آن‌ها.

همان‌طور که ملاحظه می‌شود، بسیاری از موارد مذکور در فوق، به خوبی موضوعات راجع به حمایت از داده‌ها را منعکس می‌کنند. اما تمایزات برجسته میان آن‌ها را نیز نباید نادیده انگاشت. به

---

1. Data Protection
2. Business Data
3. Risk Management
4. Data Matching
5. Data Subject

همین دلیل، برخی کشورها به هنگام تنظیم اسناد قانونی داخلی یا پیوستن به اسناد قانونی منطقه‌ای یا بین‌المللی، سعی کرده‌اند این‌گونه تمایزها را به خوبی مورد ملاحظه قرار دهند و صریحاً بر آن‌ها تأکید کنند. از میان آن‌ها، کشور انگلستان به عنوان یکی از معدود کشورهایی که از سوی دو نظام بزرگ حقوقی، یعنی **حقوق عرفی و رومی ژرمنی**، احاطه شده است و همان‌طور که می‌دانیم، مباحث راجع به حمایت از داده‌ها بیش‌تر در میان کشورهای تابع نظام رومی ژرمنی و مباحث راجع به حمایت از حریم خصوصی بیش‌تر در میان کشورهای تابع نظام حقوق عرفی رایج است، دانشمندان آن به هنگام طرح مباحث این حوزه، به‌خوبی این‌گونه تمایزات را مورد توجه قرار داده‌اند. زیرا باید از یک سو به نظام حقوقی کشورشان، یعنی حقوق عرفی و از سوی دیگر به دستورالعمل‌های شورای اروپا که با رویکرد رومی ژرمنی نگارش می‌یابند پایبند باشند. لذا بررسی نظریات آن‌ها می‌تواند حقایق بسیاری را درباره ارتباط این دو مفهوم آشکار سازد. در این رابطه عیناً به گزارش کمیته راجع به حمایت از داده‌ها که به تبیین این مسأله پرداخته اشاره می‌شود:

گزارش کمیته راجع به حمایت از داده‌ها Cmnd,7341,1998 مفهوم حریم داده‌ها [1]

۲/۰۳- بعضی از ابعاد حریم خصوصی هیچ ارتباط نزدیکی با ساماندهی داده‌های شخصی در سیستم‌های اطلاعات ندارند، مانند ورود غیرمجاز به منزل، اختیار ورود و تفتیش و لطمه به اعتبار در رسانه‌ها. همچنین، ابعادی از حمایت داده‌ها هستند که هیچ‌گونه ارتباط نزدیکی با حریم خصوصی ندارند. برای مثال، استفاده از اطلاعات نادرست یا ناقص برای تصمیم‌گیری راجع به اشخاص، به واقع تحت شمول حمایت از داده‌ها قرار می‌گیرد، ولی هیچ دغدغه‌ای راجع به حریم خصوصی برنمی‌انگیزد.

*۲/۰۴- کمیتهٔ یانگر [2] باید به تمامی ابعاد حریم خصوصی بپردازد. اما وظیفه ما بررسی حمایت از داده‌هاست. در واقع این دو حوزه با یکدیگر همپوشانی دارند و آن حوزه‌ای که تحت شمول هر دو قرار می‌گیرد را می‌توان **حریم اطلاعات** یا بهتر از آن **حریم داده‌ها** نامید. این حوزه حائز اهمیت است و ما مجال خوبی یافتیم در این گزارش به آن بپردازیم. اما فی‌نفسه تمام حوزه حمایت از داده‌ها را دربرنمی‌گیرد و ما مجبوریم به نکاتی توجه کنیم که مستقیماً از مسائل حریم خصوصی ناشی نمی‌شوند. با این حال، ما دریافتیم ارزیابی مفهوم حریم داده‌ها آثار و نتایج سودمندی دارد. به‌همین دلیل، بر مفهومی از آن تکیه کردیم که عبارت است از «ادعای فرد در کنترل جریان داده‌های راجع به خودش».*

داده‌های خصوصی

۲/۰۵- در این‌که چه داده‌هایی «خصوصی» تلقی شود، دیدگاه‌های بسیار متنوعی وجود دارد. این تنوع

1. Data Privacy
2. Younger Committee

از یک فرد به فرد دیگر، از جامعه‌ای به جامعه دیگر، از کشوری به کشور دیگر و حتی در دوره‌های زمانی مختلف نیز ملاحظه می‌شود.

۲/۰۶- بعضی اشخاص مایلند دیگران راجع به آن‌ها بیش‌تر بدانند. در این‌جا سن، شخصیت، خلق و خو، دیدگاه‌ها و عقاید تمامی نقش‌آفرینان تعیین‌کننده است. تنوع‌های اجتماعی و فرهنگی در میان بخش‌های مختلف یک جامعه نیز تأثیرگذار است. تنوع نهادها، فرهنگ‌ها و آداب و رسوم و شیوه و ویژگی‌های سیاسی حکومت در میان جوامع مختلف، از عوامل متمایز هستند. تغییراتی که در دیدگاه‌های یک جامعه رخ می‌دهد نیز با عوامل بسیاری ارتباط دارد، از جمله توسعه اقتصادی، تغییر استانداردهای آموزشی، مشارکت اجتماعی و فرصت‌های بالفعل برای خودتعیینی.

۲/۰۷- معیار «خصوصی بودن» تنها بر داده‌ها استوار نیست. زیرا ممکن است یک داده در یک چارچوب، بسیار خصوصی تلقی شود، ولی در دیگری به هیچ‌وجه خصوصی نباشد. صرفنظر از این، حتی اگر داده‌ای خصوصی تلقی شود، به این معنا نیست که فقط باید برای شخصی که به او مربوط می‌شود شناسانده گردد. بلکه به این معناست که او می‌خواهد این داده‌ها تنها برای خودش و آن‌هایی که او ***موافقت*** *کرده آگاه گردند، افشا شود. راه‌های بسیاری برای حصول این‌گونه توافقات وجود دارد. ساده‌ترین شکل این است که افراد داده‌ها را مستقیماً به دیگری تحویل می‌دهند. این می‌تواند یک اقدام کاملاً داوطلبانه یا عمل به الزامی باشد که در یک قرارداد گنجانیده شده است. حالت دیگر، قانونی است که قوه مقننه منتخب آن شخص به تصویب رسانده و مطابق آن ارائه داده‌ها به فرد یا مرجع خاصی را مقرر داشته است. با این حال، اگر هدف استفاده از داده‌ها و شرایطی که باید مطابق آن این اهداف محقق گردند تبیین نگردد، هیچ‌کس نمی‌تواند راجع به این‌گونه توافقات اظهارنظر کند.*

به نظر می‌رسد توضیحات ارائه شده از سوی این کمیته آنقدر رسا و جامع می‌باشد که باب هرگونه توضیح و تفسیر اضافی را می‌بندد. لذا در ادامه صرفاً برای این‌که زمینه ورود به بخش بعد فراهم گردد، به یکی از اسناد اولیه راجع به این حوزه که اصول حاکم بر حریم داده‌های شخصی را برشمرده است، منعکس می‌گردد. این سند از سوی سازمان توسعه و همکاری اقتصادی (OECD) منتشر شده و با این‌که الزام‌آور نیست، اما همانند دیگر اسناد منتشره از سوی این مرجع، مبنای تدوین و تصویب اسناد الزام‌آور بسیاری در عرصه‌های ملی، منطقه‌ای و بین‌المللی بوده است. لذا به‌عنوان یک سند مادر به آن اشاره می‌گردد.

رهنمودهای حمایت از حریم خصوصی و جریان فرامرزی داده‌های شخصی[1] OECD-1980

بخش دوم- اصول اساسی اجرای ملی اصل محدودیت در جمع‌آوری

۷. باید در جمع‌آوری داده‌های شخصی، محدودیت‌هایی اعمال و از مجاری قانونی و به شکل منصفانه آن‌ها را تحصیل کرد و در صورت لزوم، مسندالیه داده‌ها آگاه یا رضایتش جلب گردد.

اصل کیفیت داده‌ها

۸. داده‌های شخصی باید با اهدافی که به‌کار می‌روند مرتبط باشند و تا حدی که در راستای این اهداف ضرورت ایجاب می‌کند، باید دقیق، کامل و روزآمد باشند.

اصل مشخص بودن هدف

۹. اهدافی که در راستای آنها داده‌های شخصی جمع‌آوری می‌شوند، باید حداکثر تا زمان جمع‌آوری مشخص گردند و استفاده بعدی از آن‌ها به رعایت آن اهداف یا نظایر آنها که مغایر نیستند محدود شود و در صورت تغییر هر هدف، به آن تصریح گردد.

اصل محدودیت در استفاده

۱۰. داده‌های شخصی نباید افشا گردد، در دسترس قرار گیرد یا به دیگر مقاصد غیرمقرر در بند «۹» فوق به‌کار رود، مگر این‌که:

الف) مسندالیه داده‌ها راضی باشد،

ب) به حکم قانون.

اصل تضمینات امنیتی

۱۱. داده‌های شخصی باید در برابر خطراتی مانند فقدان، دسترسی غیرمجاز، تخریب، استفاده، اصلاح یا افشا، از تضمینات امنیتی متعارف برخوردار باشند.

اصل شفافیت

۱۲. باید یک سیاست عمومی شفاف‌سازی راجع به پیشرفت‌ها، اقدامات و سیاستگذاری‌ها در خصوص داده‌های شخصی برقرار شود. ابزارهای تأسیس موجودیت و ماهیت داده‌های شخصی، اهداف به‌کارگیری آنها و همچنین، هویت و محل سکونت معمول کنترل‌کننده داده‌ها باید در دسترس باشد.

اصل مشارکت فردی

۱۳. فرد باید حق داشته باشد:

الف) از کنترل‌کننده داده‌ها تأییدیه در اختیار داشتن یا نداشتن داده‌های راجع به خودش را اخذ کند یا به نحو دیگری اقدام نماید،

1. Guidelines On The Protection Of Privacy And Transborder Flows Of Personal Data

ب) با او ارتباط برقرار کند، داده‌های مرتبط با او:

- *در خلال زمان متعارف،*
- *با پرداخت هزینه‌ای که نباید گزاف باشد،*
- *به شیوه‌ای متعارف،*
- *به شکلی که برایش به سادگی قابل فهم باشد؛ ارائه گردد.*

پ) اگر درخواستش برای انجام مفاد قسمت‌های (الف) و (ب) رد شد، با استدلال همراه باشد و بتواند به آن اعتراض کند،

ت) به داده‌های مرتبط با خودش اعتراض کند و اگر موفقیت‌آمیز بود، داده‌ها پاک، تصحیح، تکمیل یا اصلاح شوند.

اصل پاسخگویی

۱۴. کنترل‌کننده داده‌ها باید در برابر تمهیداتی که بر اصول فوق تأثیرگذارند پاسخگو باشد.

*بدیهی است در این مختصر کلام، حق مطلب در خصوص مباحث بسیار مفصل و بنیادین حریم خصوصی و همچنین حمایت از داده‌ها که به عقیده **پروفسور گلمن**[1] یک تکه از کیک حریم خصوصی به حمایت از داده‌ها می‌رسد، ادا نشد. در هر حال امید است با این زمینه‌سازی امکان طرح مباحث اصلی در بخش بعد فراهم شده باشد.*

بخش دوم- حریم خصوصی در فضای سایبر

در بخش گذشته ملاحظه کردیم یکی از جلوه‌های اصلی حریم خصوصی افراد، اطلاعات خصوصی آن‌هاست. به همین ترتیب، یکی از راه‌های مؤثر و نتیجه‌بخش مصون نگه داشتن حریم خصوصی، دور نگه داشتن اطلاعات خصوصی از هرگونه تعدی و تعرض است. لذا با توجه به تأثیرگذاری متقابل و مستقیم این دو حوزه بر یکدیگر، یعنی حریم خصوصی و اطلاعات در مفهوم عام آن، باید هرگونه تغییر و تحول در آن‌ها را به دقت مورد بررسی قرار داد تا سیاست‌ها و راهبردهای خرد و کلان با هماهنگی لازم اتخاذ گردد.

در این راستا، همان‌طور که در مقدمه اشاره شد، فناوری اطلاعات و ارتباطات الکترونیک یکی از پدیده‌هایی است که به کلی اطلاعات را وارد مرحله جدیدی کرده و به همین نسبت کلیه امور مرتبط با آن را تحت‌الشعاع شرایط منحصر به فرد و ویژه خود قرار داده که بدیهی است اطلاعات خصوصی و به تبع آن حریم خصوصی از این تأثیر و تأثرگذاری در امان نبوده‌اند. البته تأکید بر

1. Gellman, R

این مسأله به معنای تأثیر پذیرفتن **منفی** حریم داده‌های الکترونیکی از فضای سایبر نیست. بلکه اتفاقاً در بعضی موارد، نسبت به دنیای فیزیکی از مزایا و مطلوبیت‌هایی نیز برخوردار است. اما نمی‌توان انکار کرد که زمینه‌های تعرض به حریم الکترونیکی افراد، همانند بسیاری از سوء استفاده‌های مجرمانه و ناهنجار، از سهولت همه‌جانبه بسیار بیش‌تری در این فضا برخوردار شده‌اند. به هر حال، در این بخش، تلاش می‌شود هر دو بعد منفی و مثبت تأثیرگذاری فضای سایبر بر حریم خصوصی افراد مورد بررسی قرار گیرد.

۱. مطلوبیت‌های فضای سایبر برای حریم خصوصی

دلیل این‌که ابتدا مطلوبیت‌ها و نقاط قوت فناوری اطلاعات و ارتباطات الکترونیکی نسبت به دنیای فیزیکی اشاره می‌گردد، آن است که بر این مهم تأکید شود آن‌گونه که ابداع‌کنندگان این فناوری با حسن نیت و در راستای توسعه و پیشرفت همه‌جانبه بشری، چنین پدیده شگفت‌انگیزی را عرضه داشته‌اند، چنان‌چه به شکل صحیح و عاری از هرگونه سوء نیت به‌کار رود، نه تنها برای هیچ حوزه‌ای مشکل‌آفرین نیست، بلکه رشد و ارتقای آن‌ها را با شتابی باورنکردنی میسر خواهد کرد. به درستی و بدون هیچ‌گونه اغراقی، حتی این واقعیت در مورد حوزه بسیار حساسی نظیر حریم خصوصی نیز صادق است. در ادامه ابعاد مختلف حریم خصوصی که در بستر فضای سایبر تحولات مثبتی یافته‌اند مورد بررسی قرار می‌گیرد.

به‌طور کلی، مباحث راجع به حریم خصوصی در فضای سایبر، که در واقع محوریت آن با **داده‌های الکترونیکی** است، را می‌توان در دو شاخه اصلی قرار داد:

۱. ارتباطات خصوصی الکترونیکی، و ۲. داده‌های خصوصی الکترونیکی.

در همین جا تأکید می‌شود دلیل اصلی این تفکیک حساسیت ویژه ارتباطات خصوصی افراد در حوزه کلان حریم خصوصی است و الا بر هیچ‌کس پوشیده نیست که محتوا و شالوده ارتباطات خصوصی جز داده‌های خصوصی الکترونیکی نمی‌باشد.

۱-۱. ارتباطات خصوصی الکترونیکی

بشر از دیرباز به حوزه ارتباطات خصوصی خود به‌عنوان یکی از ارکان ضروری و حتی حیاتی زندگی اجتماعی‌اش نگریسته و به آن بها داده است. تلاش مستمر برای دستیابی به ابزارهای جدیدتر با کارایی بهتر در برقراری ارتباطات خصوصی مؤید اهمیت آن است. بی‌تردید، برقراری **نظام پستی**، تحولی بنیادین در این عرصه به شمار می‌رود. زیرا به افراد امکان داده با اطمینان

کامل از مصون ماندن **محرمانگی**[1] **و تمامیت**[2] داده‌های خصوصی مکتوبشان، با دوردست‌ترین نقاط جهان ارتباط خصوصی برقرار کنند.

اما این پدیده نتوانست نیازهای اصلی بشر را در برقراری **ارتباط زنده** با نقاط دیگر برآورده سازد. تا این‌که **اختراع تلفن** به این رؤیا واقعیت بخشید و موانع ذاتی زمانی و مکانی برچیده شد. اما همچنان رؤیای برقراری ارتباطات مطلوب‌تر، حتی به شکل چندرسانه‌ای، محقق نشده بود تا این‌که فناوری **رایانه الکترونیک** به کمک فناوری **مخابرات آنالوگ** آمد و با پیدایش **فناوری اطلاعات و ارتباطات الکترونیک** تقریباً هرگونه مانعی برطرف شد.

امروزه انواع ارتباطات خصوصی مکتوب، صوتی و حتی ویدئویی الکترونیکی با کیفیتی باور نکردنی به صورت زنده و با امکانات جانبی بسیار به صورت بی‌سیم یا باسیم در فضای سایبر به طور گسترده در اختیار همگان قرار گرفته و نسبت به امکاناتی که این فضا برای برقراری این‌گونه ارتباطات ارائه می‌دهد، نه تنها هزینه‌های آن بسیار پایین است که کار با آن‌ها نیز بسیار آسان است و نیاز به هیچ‌گونه مهارت فنی خاصی نیست و به همین دلیل تقریباً کسی نیست که حداقل با برخی از آن‌ها آشنا نباشد و از طریق آن‌ها با دیگران ارتباط برقرار نکرده باشد. از پیجرها[3] گرفته تا پست الکترونیک[4] و محیط‌های گپ[5] حتی سه بعدی که می‌توان به دلخواه طراحی کرد و حتی امکان برگزاری نشست‌های گروهی خصوصی را به‌شکل چندرسانه‌ای ترتیب داد، گوشه‌ای از قابلیت‌های فضای سایبر است که بی‌تردید در آینده شاهد نمونه‌های بسیار شگفت‌انگیزتر نیز خواهیم بود. به هر حال، هدف این است که هرگونه مرز مکانی و زمانی برچیده شود و در واقع آنچه از آن تحت عنوان **دهکده کوچک جهانی** یاد می‌شود، متمرکز شدن افراد در فضای بی‌کران ولی کاملاً در دسترس سایبر است.

به هر حال، این وضعیت فی‌نفسه تحولی شگفت‌انگیز و مثبت در عرصه ارتباطات خصوصی و به تبع آن حریم خصوصی افراد تلقی می‌شود. زیرا باعث شده آن‌ها به بهترین وجه امور خصوصی‌شان را توسعه دهند و در بسترهای دیگری جز دنیای فیزیکی از مواهب یک محیط خصوصی با امکانات مطلوب برخوردار شوند.

اما در کنار پیشرفت‌هایی که تقریباً می‌توان آنها را در زمره **توسعه کمی** امور خصوصی افراد قرار داد، نباید **بهبود کیفی** آن‌ها را نادیده گرفت. در دنیای فیزیکی ابزارهای محدودی برای مصون داشتن محرمانگی و تمامیت ارتباطات خصوصی از انواع تعرضات وجود دارد. اما نمونه‌های بسیار

---

1. Confidentiality
2. Integrity
3. Pagers
4. E-Mail
5. Chat

پیشرفته‌تر آن‌ها در فضای سایبر در دسترس است که امکان حفظ حریم داده‌های الکترونیکی را به شکل بسیار مطلوب‌تری فراهم ساخته است. در ادامه به دو شیوه رایج که از کارایی بالایی برخوردارند اشاره می‌شود.

۱. **رمزنگاری**[1] **و استگانوگرافی**[2]: دلیل اشاره به این دو کارکرد در یک قسمت این است که هر دو جهت مصون داشتن محرمانگی و تمامیت **محتوای**[3] ارتباطات از تعرضات گوناگون به‌کار می‌روند. در رمزنگاری، به‌طور خلاصه، **متن اصلی**[4] به **رمزنوشته**[5] تبدیل می‌شود و تا **کلید رمزگشای**[6] آن موجود نباشد، غیرقابل خواندن خواهد بود. اما استگانوگرافی که شیوه نوینی محسوب می‌شود، به فرد امکان می‌دهد محتوای پیامش را در میان محتوای دیگری که ظن‌برانگیز نیست جای دهد و به این ترتیب، ذهن هر متعرضی را منحرف سازد.

هم‌اکنون فضای سایبر برای انجام این کارکردها ابزارهایی ارائه می‌دهد که خنثی‌سازی آن‌ها تقریباً غیرممکن است و به‌همین دلیل به بهترین وجه می‌توانند حریم داده‌های الکترونیکی افراد را حفظ نمایند. اما در قسمت‌های بعد خواهیم دید که بهره‌برداری بی‌حد و حصر از آن‌ها برای دیگر امور، به‌ویژه حفظ نظم و امنیت ملی که توسط مجرمین به خطر می‌افتد، مشکلاتی جدی را به وجود آورده است.

۲. **ناشناس‌کننده‌ها**[7]: ابزار بسیار کارامد دیگری که فضای سایبر در اختیار کاربرانش قرار داده تا از امور خصوصی خود حداکثر حفاظت را به عمل آورند ناشناس‌کننده نام دارد. این ابزار، در واقع مکمل رمزنگارها و استگانوگرافی محسوب می‌شود. زیرا مسیر حرکت ارتباطات خصوصی را به گونه‌ای مخدوش می‌کند که ردیابی آن برای دیگران اگر غیرممکن نگردد، بسیار مشکل خواهد بود. این مسأله از آن جهت اهمیت دارد که برخلاف دنیای فیزیکی، مسیر حرکت پیام‌های الکترونیکی از خود سوابقی با عنوان **داده ترافیک**[8] به جا می‌گذارد که نه تنها خودشان ارزشمند هستند، بلکه می‌توانند زمینه شناسایی اطلاعات خصوصی دیگر را نیز فراهم کنند. لذا این ابزار می‌تواند از بروز بسیاری تعرضات به حریم خصوصی افراد جلوگیری نماید.

۲-۱. داده‌های خصوصی الکترونیکی

با توجه به توضیحاتی که در ابتدای فصل داده شد، در این قسمت آن دسته از داده‌های خصوصی

---

1. Cryptography
2. Steganography
3. Content
4. Plain Text
5. Cipher Text
6. Decipher or Decryption Key
7. Anonymizers
8. Data Traffic

بررسی می‌شوند که دیگر حوزه‌های راجع به امور خصوصی افراد را دربرمی‌گیرند و از شمول ارتباطات خصوصی الکترونیکی خارج هستند.

پیش از هر چیز شایان ذکر است، از زمان‌های بسیار دور، اطلاعات راجع به افراد در سطوح مختلف جامعه جمع‌آوری و مبادله می‌شدند، لذا به خوبی می‌توان عمر جمع‌آوری داده‌های شخصی را به اندازه عمر جوامع طولانی دانست. با این حال، این کار به‌عنوان یک حرفه، که امروزه بر روی آن سرمایه‌گذاری زیادی صورت می‌گیرد، انجام نمی‌شده و غالباً به‌عنوان یکی از قدیمی‌ترین عادات مورد توجه قرار می‌گرفته است.

اما با توجه به تحولات بنیادینی که در نگرش انسان عصر حاضر نسبت به ماهیت اطلاعات صورت گرفته و به عنوان گرانبهاترین سرمایه مورد توجه قرار گرفته و در این راستا ابزار بسیار توانمندی به نام فناوری اطلاعات و ارتباطات الکترونیکی به کمک بشر آمده تا دیگر نسبت به نحوه و میزان جمع‌آوری، ذخیره‌سازی، انواع پردازش‌های سودمند در کم‌ترین زمان ممکن با بیش‌ترین اطمینان نسبت به حفظ تمامیت داده‌ها هیچ‌گونه دغدغه‌ای وجود نداشته باشد، بهره‌برداری از اطلاعات خصوصی افراد نیز به عنوان بخشی از مجموعه کلی اطلاعات مورد نیاز برای گردش کار امور خرد و کلان جامعه، از آن حالت سنتی‌اش خارج شده و جلوه حرفه‌ای پیدا کرده است. به عبارت دیگر، همانند حوزه ارتباطات خصوصی، با وارد شدن اطلاعات خصوصی به فضای سایبر، از آن حالت بلااستفاده خارج و به یک سرمایه ارزشمند و همچنین ابزار کار در بسیاری از امور الکترونیکی تبدیل شده است. برای مثال، با ارائه اطلاعات خصوصی به یک بنگاه یا مؤسسه اعتباری، می‌توان شماره اعتباری دریافت کرد و در فضای سایبر به داد و ستد و تجارت الکترونیکی پرداخت یا از خدمات آموزشی آن‌لاین بهره‌برد.

به هر حال، واقعیت این است که بشر امروز مجبور است برای عقب نماندن از قافله جامعه اطلاعاتی، بسیاری از اطلاعات خصوصی خود را در اختیار دیگران قرار دهد تا بتواند در حوزه‌های مختلف حضور مؤثری داشته باشد. اما نباید نادیده انگاشت که در قبال این چشم‌پوشی، عواید زیادی نصیب وی می‌گردد و همان‌طور که در فوق اشاره شد، فضای سایبر این مزیت را به دنبال داشته که بخشی از سرمایه راکد بشری را به جریان انداخته و حتی موجبات سودآوری آن را فراهم آورد. البته در این‌جا بحث سوءاستفاده‌های احتمالی از این داده‌ها مطرح نیست و در این مقطع فرض بر این است که با رعایت تمامی جوانب راجع به حفظ محرمانگی و تمامیت داده‌های خصوصی امکان بهره‌برداری فایده‌مند از آن‌ها از طریق **دسترس‌پذیر**[1] ساختن در فضای سایبر فراهم آمده که پیش از این در دنیای فیزیکی وجود نداشت یا به‌صورت محدودی امکانپذیر بود.

1. Availability

مزیت دیگری که فضای سایبر برای داده‌های خصوصی اشخاص به ارمغان آورده، **تطبیق** آن‌ها بر یکدیگر است که پیش از این به آن اشاره شد. پیش از ظهور فناوری رایانه و حتی سه چهار دهه پس از آن، داده‌های حوزه‌های مختلف به صورت **غیرمتمرکز** نگه‌داری می‌شدند و عملاً یا امکان گردآوری تمامی داده‌های راجع به یک فرد وجود نداشت یا با دشواری‌های بسیاری همراه بود. اما فضای سایبر این امکان را فراهم آورده که هر شخص، البته نسبت به میزان مشارکت جدی عرصه‌های مختلف اجتماع در امور آن‌لاین، اطلاعات راجع به خودش را در کم‌ترین زمان ممکن جمع‌آوری نماید و بهتر از امور شخصی و خصوصی‌اش آگاه شود. بسیار اتفاق می‌افتد که اشخاص از بعضی امور خصوصی مستند و ثبت شده‌شان آگاهی ندارند و چه بسا در اثر این بی‌اطلاعی هزینه‌های جبران‌ناپذیری را متحمل شده یا فرصت‌های ارزشمندی را از دست داده‌اند. امروزه با اتصال روزافزون انواع **پایگاه‌های داده**[1] به شبکه‌های آن‌لاین، امکان دسترسی افراد به داده‌های راجع به خودشان و کاوش در میان آن‌ها فراهم شده است.

۲. آسیب‌پذیری‌های حریم داده‌های الکترونیکی

در فصل گذشته تلاش شد با به تصویر کشیدن مزایا و وجوه مثبت فضای سایبر برای حریم خصوصی افراد، مباحث خاص این حوزه با نگاهی خوشبینانه و توأم با حسن نیت آغاز شود. کما این‌که هدف اصلی پدیدآورندگان این فناوری برای تمامی عرصه‌ها همین بوده و هرگز به دنبال فتح باب انواع سوءاستفاده‌های زیانبار نبوده‌اند. با وجود، این نمی‌توان انکار کرد که بهره‌برداری **بدون تبعیض** از این فضا، به مجرمین و منحرفین امکان داده، برای نتیجه‌گیری بهتر و مؤثرتر از نیات شومشان، این فضا را در اولویت اهداف خود قرار دهند. بدیهی است حریم داده‌های الکترونیکی نیز از این وضعیت مستثنا نیست و آماج انواع تعرضات و آسیب‌ها قرار دارد.

اما برای شناسایی آسیب‌پذیری‌های حریم داده‌های الکترونیکی راه‌های گوناگونی وجود دارد. در این‌جا، با توجه به هدفی که این نوشتار دنبال می‌کند، عواملی که به مقاصد گوناگون این حوزه را مورد تعرض قرار می‌دهند معرفی می‌گردند. دلیل انتخاب این گزینه جامعیت آن است. زیرا از طریق آن می‌توان نوع داده‌های خصوصی که از سوی عوامل مختلف مورد توجه قرار گرفته‌اند را نیز شناسایی و با سیاستگذاری صحیح و به موقع نسبت به رفع آسیب‌پذیری‌های آن‌ها اقدام کرد. این عوامل عبارتند از: ۱. مجریان قانون، ۲. ارائه‌دهندگان خدمات شبکه‌ای، ۳. سایر افراد.

1. Data Base

۱-۲. مجریان قانون

منظور از مجریان قانون، که نماد بارز آن **پلیس** است، کلیه مراجعی هستند که به حکم قانون موظفند نظم و امنیت را در جامعه برقرار سازند و حفظ نمایند. به این منظور، آن‌ها ابتدا از وقوع هرگونه اقدام مجرمانه جلوگیری می‌کنند که مجموعه تدابیر اتخاذی‌شان تحت عنوان **تدابیر پیشگیرانه از وقوع جرم** قرار می‌گیرد. سپس در صورت وقوع جرائم، تلاش می‌کنند با شناسایی عوامل جرم و دستگیری و تحویل آن‌ها به مراجع ذی‌صلاح قضائی، علاوه بر اجرای عدالت، از تکرار آن‌ها جلوگیری کنند.

اما هدف از اشاره به این مراجع در این مبحث آن است که از آن‌جا که فرض بر این است مطیع قانون هستند و از هرگونه **اقدام خودسرانه فراقانونی یا فروقانونی** خودداری می‌کنند، لذا قوانین و مقررات ناظر بر اقداماتشان باید با دقت بسیار تدوین گردد تا آن‌ها به اختیار یا به ناچار برای انجام وظایفشان برخلاف موارد مقرر عمل نکنند. برای مثال، در حوزه مباحث راجع به حریم خصوصی، این قانون است که مقرر می‌کند تحت چه شرایطی مجریان قانون حق دارند وارد منازل یا دیگر اماکن خصوصی افراد شوند و طبق چه ضوابطی به تفتیش آن‌ها و توقیف اشیای مورد نیاز بپردازند.

با این حال، شایان ذکر است فضای سایبر ویژگی‌های خاص و منحصر به فردی را به جامعه حقوق کیفری، به‌ویژه مجریان قانون تحمیل کرده که بسیاری از ضوابط قابل اجرا در دنیای فیزیکی از هیچ‌گونه کارایی در این‌جا برخوردار نیستند و باید برای آن‌ها خط‌مشی‌های جداگانه‌ای تدوین کرد. عدم حضور فیزیکی مجرمین در محل وقوع نتایج مجرمانه و مشکل بودن شناسایی آن‌ها به دلیل امکان اتخاذ هویت‌های مجعول و غیرواقعی در فضای سایبر و حتی در صورت شناسایی آن‌ها، مشکل بودن دستگیری‌شان به دلیل وجود فاصله فیزیکی که حتی بسیار اتفاق می‌افتد به فراسوی مرزها کشیده شود و مشکلات راجع به رعایت مقررات کیفری سایر کشورها را مطرح کند، همگی باعث شده تصمیم‌سازان و سیاستگذاران حوزه **آیین دادرسی کیفری**، قوانین و مقررات کاملاً متمایزی را که بعضاً دارای امتیازاتی نسبت به ضوابط دنیای فیزیکی است وضع نمایند و حتی به آن‌ها جلوه منطقه‌ای و بین‌المللی نیز ببخشند.

با این حال، هر اندازه وضعیت عملکرد مجریان قانون در فضای سایبر بغرنج باشد، باز هم باید به‌نحوی اقدامات آن‌ها را ضابطه‌مند کرد که از تعرض به حقوق مسلم کاربران، به‌ویژه حوزه حساس حریم داده‌های الکترونیکی‌شان جلوگیری کرد یا عواقب آن را به حداقل ممکن رساند. به همین منظور، همزمان با طرح مباحث راجع به توسعه اختیارات مجریان قانون در فضای سایبر، مسائل راجع به عدم تعرض به آن‌ها نیز مطرح گردیده است. در ادامه آن دسته از اقدامات مجریان

قانون که بر حسب وظایفشان منجر به نقض حریم داده‌های الکترونیکی می‌شود مورد بررسی قرار خواهد گرفت. در این راستا، مباحث در دو قسمت مطرح می‌گردد:

الف) اقدامات تعرض‌آمیز مجریان قانون جهت پیشگیری از وقوع جرائم،

ب) اقدامات تعرض‌آمیز مجریان قانون در پی‌جویی و تعقیب مجرمین.

الف) اقدامات تعرض‌آمیز مجریان قانون جهت پیشگیری از وقوع جرائم

پیش از ورود به مباحث اصلی، دو نکته خاطرنشان می‌گردد. اولاً تعرض‌آمیز بودن یک اقدام دلیل بر غیرقانونی بودن آن نیست. زیرا همان‌طور که اشاره شد، ممکن است قانونگذاران به این نتیجه برسند برای حفظ نظم و امنیت جامعه، لازم است اشخاص از برخی حقوقشان، از جمله حریم خصوصی‌شان چشم‌پوشی کنند که البته نفع مستقیم آن ابتدا متوجه خود آن‌ها خواهد بود. ثانیاً پیشگیری از وقوع جرم، وظیفه‌ای نیست که تنها به عهده مجریان قانون باشد. بلکه دیگر اشخاص و مراجع نیز به فراخور نوع کارکردهای اجتماعی که به عهده دارند، ممکن است به موجب قانون مکلف به پیشگیری از وقوع جرائم تحت حوزه خودشان باشند که در گفتار بعد به گروه نقش‌آفرین بسیار مهم دیگر در این حوزه اشاره خواهد شد.

اما در خصوص تدابیر پیشگیرانه سایبری که برای جلوگیری از وقوع جرائم سایبری یا مرتبط با فضای سایبر به اجرا درمی‌آیند، باید خاطرنشان کرد گزینه‌های متنوعی وجود دارد. اما آنچه مجریان قانون می‌توانند در حوزه کاری‌شان به اجرا گذارند، **تدابیر نظارتی**[1] است که در فضای فیزیکی نیز نمونه‌هایی از آن را در قالب **دوربین‌های مداربسته الکترونیکی** جهت کنترل اماکن خاص شاهد هستیم. اما آنچه در فضای سایبر به کار می‌رود، مجموعه‌ای از **برنامه‌های رایانه‌ای** هستند که بر حسب نوع برنامه‌ریزی‌ای که برایشان صورت گرفته، کلیه داده‌های راجع به مبادلات الکترونیکی کاربرانی که به هر دلیل در مظان ارتکاب جرم هستند را جمع‌آوری می‌کنند تا مسئولان ذی‌ربط به صورت زنده آن‌ها را بررسی کنند یا این‌که ذخیره می‌شوند تا در وقت مقتضی بررسی گردند. این اقدام تا حدی مورد توجه مجریان قانون کشورها قرار گرفته که برخی از آن‌ها **پلیس گشت سایبر**[2] نامیده شده‌اند. زیرا همانند پلیس گشت دنیای فیزیکی، به‌گونه‌ای اوضاع سایبری را تحت کنترل دارند که هرگونه احتمال وقوع جرم یا دیگر ناهنجاری‌ها را به اطلاع مراجع ذی‌ربط می‌رسانند.

با این حال، ناگفته پیداست از این ابزارها می‌توان برای پی‌جویی و تعقیب مجرمین نیز استفاده کرد. زیرا در هر حال، اطلاعات بسیاری، به‌ویژه داده‌های خصوصی افراد، را در اختیار مجریان

1. Monitoring Measures
2. Cyber Patrol

قانون قرار می‌دهند و آن‌ها می‌توانند به‌عناوین مختلف از آن‌ها بهره‌برداری کنند. لذا اگر ضابطه مشخصی برای استفاده از آن‌ها وجود نداشته باشد، بهترین ابزار برای لطمه زدن به حریم داده‌های الکترونیکی افراد محسوب می‌شوند.

ب) اقدامات تعرض‌آمیز مجریان قانون در پی‌جویی و تعقیب مجرمین

از آن‌جا که مجریان قانون، به‌ویژه پلیس، عمده تلاش خود را صرف پی‌جویی و تعقیب مجرمین می‌کنند، اقداماتشان در این حوزه بیش‌تر مورد توجه قرار می‌گیرد. البته نباید حساسیت کار آن‌ها را در این مقطع نادیده انگاشت. زیرا در مرحله پیشگیری از وقوع جرم، هنوز هنجار قانونی نقض نشده و مجریان قانون باید به ضرورت‌ها اکتفا و از اقدامات نابه‌جا خودداری کنند. اما در این‌جا جرمی اتفاق افتاده و اجرای عدالت و احقاق حقوق بزه‌دیدگان ایجاب می‌کند مجرم یا مجرمین مورد نظر شناسایی و تحویل مراجع ذی‌صلاح قضائی گردند. لذا قاعدتاً باید ابتکار عمل بیش‌تری به مجریان قانون داده شود.

با این حال، شایان ذکر است اقدامات مجریان قانون در این مقطع نیز تا حدی تحت نظر است که در برخی کشورها، به‌ویژه آن‌هایی که رسماً مباحث راجع به حریم خصوصی افراد را آغاز کرده‌اند، اولاً و بالذات نقض حریم افراد را به آن‌ها منتسب کرده‌اند و عملاً از دیگر ناقضین حریم افراد چشم‌پوشی کرده‌اند. برای مثال، هنگامی که دو قاضی امریکایی به نام‌های **ساموئل وارن**[1] و **لوئیس براندیس**[2] حدود صد سال پس از تصویب قانون اساسی کشورشان، یعنی ۱۸۹۰، در خصوص حریم خصوصی افراد یکی از جنجال‌آمیزترین مقالات را نوشتند، مخاطبشان مجریان قانون بود و به آن‌ها هشدار دادند با توسل به معاذیری چون اجرای قانون، به اموری از اشخاص که حق دارند در آن‌جا **تنها**[3] باشند، بدون اجازه وارد نشوند. این میزان حساسیت نهایتاً باعث شد در راستای حمایت از حریم خصوصی افراد **اصلاحیه چهارم قانون اساسی**[4] به تصویب برسد و در آن صراحتاً مجریان قانون خطاب قرار گرفتند. در این اصلاحیه آمده است: «حق عموم افراد جامعه در مورد امنیت جان، منزل، اوراق و اعمال آن‌ها در برابر تفتیش و توقیف‌های نامتعارف نباید مورد تعرض قرار گیرد. هیچ قراری نباید صادر شود، مگر این‌که سبب محتملی صادر شود و مدرک مستدلی مانند سوگند یا شهادت نیز مؤید آن باشد و باید مکانی که قرار است تفتیش شود و اشخاص یا اشیایی که توقیف شوند، به دقت مشخص شده باشد». شایان ذکر است مراجع حقوقی

1. Samuel Warren
2. Louis Brandeis
۳.حق تنها ماندن (Let To Be Alone) اصطلاحی است که از آن زمان به‌عنوان معادلی رسا برای تبیین مفهوم حریم خصوصی به‌کار رفته است.
4. Fourth Amendment to the U.S. Constitution

این کشور، از جمله قضات و مجریان قانون، از این اصلاحیه قاعده «**انتظار متعارف حریم خصوصی**»[1] را استخراج کرده‌اند و تاکنون بر اساس آن رویه‌های لازم‌الاجرای بسیاری حتی در حوزه‌های جدید، مانند سیستم‌های رایانه‌ای و مخابراتی صادر شده است.

همچنین، در اسناد بین‌المللی و منطقه‌ای متعددی که تاکنون در راستای ساماندهی اقدامات مجریان قانون در فضای سایبر به تصویب رسیده، بر رعایت حقوق مسلم کاربران، به‌ویژه حریم خصوصی آن‌ها تأکید شده است. برای مثال، **کنوانسیون اروپایی جرائم سایبر**[2] که بیش از دو سوم آن به مقررات حوزه مجریان قانون اختصاص دارد، در رابطه با لزوم رعایت حقوق کاربران اشعار می‌دارد: «***ماده*** (۱۵). **شرایط و تضمین‌ها**: ۱. اعضا باید اطمینان دهند که تصویب، اجرا و اعمال اختیارات و رویه‌های پیش‌بینی شده در این بخش، در شرایط و تضمین‌های حقوق داخلیشان گنجانیده‌اند و در راستای حمایت شایسته از حقوق و آزادی‌های بشری است که از جمله آن‌ها حقوق برخاسته از تعهداتی است که آن‌ها در کنوانسیون شورای اروپا راجع به حمایت از حقوق و آزادی‌های اساسی بشر (۱۹۵۰) و میثاق حقوق مدنی و سیاسی سازمان ملل متحد (۱۹۶۶) و دیگر اسناد بین‌المللی لازم‌الاجرای حقوق بشر پذیرفته‌اند. این شرایط و تضمین‌ها باید به دنبال برقراری اصل تناسب باشند».

با این حال، همان‌طور که ملاحظه می‌شود، در این کنوانسیون نیز بر لزوم رعایت **اصل تناسب**[3] تأکید شده است. زیرا در عین قبول حساسیت‌های ناشی از مصون ماندن حریم داده‌های الکترونیکی افراد از هرگونه تعرض، به‌ویژه اقدامات تعرض‌آمیز مجریان قانون، این واقعیت نیز پذیرفته شده که اگر آن‌ها از اختیار عمل‌هایی برای انجام وظایفشان برخوردار نباشند، عملاً مجرمینی که به‌طور روزافزون ارتباطشان با این فضا بیش‌تر می‌شود و به خوبی می‌توانند آن‌ها را از طریق آثار الکترونیکی به‌جا مانده و همچنین دیگر سوابق الکترونیکی **محکمه‌پسند** شناسایی کنند و تحویل مراجع قضائی دهند، از اجرای عدالت به دور خواهند ماند و به تدریج فضای سایبر به بستر بسیار مناسبی برای اقدامات مجرمانه تبدیل خواهد شد.

۲-۲. ارائه‌دهندگان خدمات شبکه‌ای

یکی از وجوه تمایز اصلی فضای سایبر با دنیای فیزیکی این است که تعامل با آن نیازمند عبور از پلی به نام ارائه‌دهندگان خدمات شبکه‌ای[4] است. تفاوتی نمی‌کند اتصال به این فضا به شکل بی‌سیم، مثلاً از طریق تلفن‌های همراه، یا باسیم، مانند اتصال از طریق رایانه‌های شخصی متصل به مودم،

1. Reasonable Expectation of Privacy
2. European Convention on Cyber Crime, 2001
3. Proportionate Principle
4. Network Providers

صورت گیرد. در هر حال عبور از این پل الزامی است.

بدیهی است در اختیار داشتن این گلوگاه از اهمیت بسیار زیادی برخوردار است. زیرا به تبع آن اطلاعات بسیاری نصیب صاحبان و متصدیان آن می‌شود و آن‌ها می‌توانند از اختیار عمل بسیاری برخوردار باشند. هرگونه تعامل با فضای سایبر همگی از خود سوابقی به جا می‌گذارند که می‌توانند گویای واقعیات بسیاری، از جمله و به‌ویژه امور خصوصی کاربران باشند. همچنین، اگر قصد هرگونه سوءاستفاده وجود داشته باشد، هم از لحاظ کیفی و هم از لحاظ کمی بیش از همه تحقق آن برای ارائه‌دهندگان خدمات میسر است. آن‌ها به راحتی می‌توانند انواع بسیاری از داده‌های الکترونیکی خصوصی راجع به افراد را در مقیاس بسیار بالا گردآوری کنند و نسبت به دیگران از هیچ‌گونه مشکل و محدودیت فنی و نیروی انسانی متخصص برخوردار نیستند. به‌همین دلیل، بایسته و ضروری است اقدامات این گروه از فعالان زیربنایی فضای سایبر تحت شمول قواعد و ضوابط دقیق و لازم‌الاجرایی قرار گیرد تا باب هرگونه سوءاستفاده احتمالی بسته شود.

در این راستا، برای این‌که بتوان نتیجه مؤثر و کاربردی از مسائل مطروحه گرفت، پیش از هر چیز لازم است هویت ارائه‌دهندگان خدمات شبکه‌ای از طریق شناسایی اقدامات تخصصی آن‌ها به خوبی تبیین گردد. سپس مطابق با نوع اقداماتشان و بالطبع داده‌های خصوصی الکترونیکی و حتی غیرالکترونیکی که دریافت می‌کنند، سیاستگذاری‌های اصولی- کاربردی انجام داد.

در این راستا، به‌طور کلی ارائه‌دهندگان خدمات شبکه‌ای را با توجه به نوع اقداماتی که در فضای سایبر عهده‌دار هستند، می‌توان به چهار دسته اصلی تقسیم کرد که عبارتند از: الف) خدمات نام دامنه، ب) خدمات انتقال، ج) خدمات دسترسی، د) خدمات میزبانی.

در ادامه به اختصار به بررسی هر یک از این موارد می‌پردازیم.

الف) خدمات نام دامنه[1]: پیش از ورود به بحث، ابتدا لازم است توضیحاتی راجع به خود نام دامنه داده شود. همان‌طور که در دنیای فیزیکی هر فضای خاصی دارای هویت و نام خاصی است، در فضای سایبر هم فضاهایی که از سوی ارائه‌دهندگان خدمات میزبانی واگذار می‌شود، هویت دارند که در قالب یک نام بروز می‌یابد. این نام که معمولاً معرف ویژگی‌های آن محدوده خاص است، **نام دامنه** نامیده می‌شود. از طریق این نام می‌توان سایت مورد نظر را در شبکه‌ها، به‌ویژه شبکه جهانی اینترنت جستجو کرد. شایان ذکر است شکل اولیه این نام یکسری اعداد است که در چهار گروه سه‌تایی به نمایش درمی‌آیند و به آن‌ها آدرس IP گفته می‌شود. اما از آنجا که یادآوری این ارقام دوازده‌تایی برای عموم مردم دشوار است، یک سیستم به نام **سرور نام دامنه**[2] این ارقام را بر

1. Domain Name Service
2. Domain Name Server

نام‌هایی که متقاضیان ارائه می‌دهند تطبیق می‌دهد و به این ترتیب کاربران می‌توانند حتی با درج نام دامنه، سایت مورد نظر خود را جستجو کنند.

همان‌طور که ملاحظه می‌شود، مراجع ثبت نام دامنه درباره کلیه فعالان سایبری که به آن‌ها نام دامنه ارائه کرده‌اند، اطلاعات ارزشمندی در اختیار دارند. بی‌تردید، بخش عمده‌ای از این اطلاعات ماهیت خصوصی دارند و آن‌ها حق ندارند بدون مجوز قانونی یا رضایت آن‌ها، مبادرت به افشای آن‌ها کنند یا از آن‌ها سوءاستفاده نمایند. در غیر این صورت، احتمال وارد آمدن خسارات سنگین دور از انتظار نخواهد بود.

ب) خدمات انتقال[1]

طیف دیگری از خدمات زیربنایی شبکه‌های اطلاع‌رسانی رایانه‌ای، خدمات انتقال است. ممکن است در نگاه اول این شبهه ایجاد شود که این نوع خدمات مشابه خدمات دسترسی است که در ادامه خواهد آمد. اما با توضیحاتی که داده می‌شود، تفاوت‌های بنیادین این دو و لزوم بررسی آن‌ها در دو مبحث جداگانه آشکار خواهد شد. همان‌طور که از نام این خدمات پیداست، وظیفه آن برقراری ارتباطات الکترونیکی شبکه‌ای است که با نمونه‌های بسیار متنوع آن آشنا شدیم. به این ترتیب، می‌توان گفت کارکرد این خدمات در فضای سایبر، بسیار شبیه سیستم‌های مخابراتی و پستی در دنیای فیزیکی است.

بدیهی است چنانچه ارتباطات خصوصی را حساس‌ترین حوزه حریم خصوصی در نظر بگیریم، این خدمات حساس‌ترین فعالیت شبکه‌ای را از منظر حریم خصوصی به عهده دارند. به همین دلیل، در اسناد مختلفی که تاکنون راجع به خدمات شبکه‌ای به تصویب رسیده، بیش‌ترین ارفاقات نسبت به این گروه اعطا شده و آن‌گونه که از عنوانشان پیداست، در حد یک **مجرای ارتباط الکترونیکی** موظفند حداکثر توان فنی و پرسنلی‌شان را به‌کارگیرند تا ارتباطات الکترونیکی بدون لطمه به محرمانگی و تمامیت‌شان برقرار شوند و به اتمام رسند. حتی آن‌ها حق ندارند با توسل به معاذیری نظیر پیشگیری از وقوع جرم یا پی‌جویی و تعقیب مجرمان، فراتر از الزامات قانونی به ارتباطات خصوصی الکترونیکی کاربران تعرض کنند و در این اسناد دستورات مصرحی راجع به نحوه نگهداری سوابق ناشی از پیام‌ها و همچنین محتوای آن‌ها آمده است.

ج) خدمات میزبانی[2]

یکی از موضوعات بدیهی در انجام هر کاری این است که باید فضایی برای آن اختصاص یابد. با

1. Mere Conduit
2. Hosting

این‌که عده‌ای فضای حاکم بر شبکه‌ها را مجازی تلقی و حتی فضای سایبر را فضای مجازی[1] معنا می‌کنند، اما راجع به این مسأله هیچ اختلافی وجود ندارد که به هر حال فعالیت در این فضای مجازی هم به‌شکل رؤیایی نیست و فضایی با حجم مشخص تخصیص می‌یابد و حتی زمان مشخصی برای بهره‌برداری از آن تعیین و اصولاً در قبال آن وجه پرداخت می‌شود.

با قبول این واقعیت، پذیرش واقعیت دیگری هم بدیهی می‌نماید که تخصیص و ساماندهی این فضا به یک متولی نیاز دارد. به واگذارکنندگان فضاهای شبکه‌ای، **خدمات میزبانی** گفته می‌شود. آن‌ها موظفند با به‌کارگیری امکانات فنی لازم، زمینه بهره‌برداری مناسب از فضای واگذاری را فراهم و هرگونه اشکال اساسی به وجود آمده را برطرف کنند.

خدمات میزبانی در چرخه تعاملات شبکه‌ای از اهمیت بسیاری برخوردار است. زیرا وجود فضای سایبر و بهره‌برداری از آن منوط به این خدمات است. اما این وضعیت حساس و تعیین‌کننده هرگز مجوز عمل خودسرانه و تعرض‌آمیز را صادر نمی‌کند. این خدمات فقط موظف است فضای درخواستی را با رعایت استانداردهای فنی و حرفه‌ای مقرر در اختیار متقاضیان قرار دهد و دیگر نسبت به نوع فعالیتی که متقاضی در آن فضا انجام می‌دهد حق هیچ‌گونه دخالتی ندارد. می‌خواهد متقاضی آن فضا را به یک پایگاه پست الکترونیکی تبدیل کند یا این‌که در آن فقط به ذخیره یا پردازش داده‌ها بپردازد یا این‌که طبق روال معمول، سایتی راه‌اندازی کرده و به اطلاع‌رسانی شبکه‌ای بپردازد.

همان‌طور که ملاحظه می‌شود، ارائه‌دهندگان خدمات میزبانی نیز به‌دلیل در اختیار داشتن یکی از ارکان اصلی فضای سایبر، از اختیار عمل بالایی برخوردارند و به‌همین دلیل، دستورالعمل‌های مفصل و روشنی نیز برای آن‌ها وضع شده تا از هرگونه عمل تعرض‌آمیز خودداری کنند که بدیهی است یکی از آن‌ها حریم داده‌های الکترونیکی اشخاص است.

د) خدمات دسترسی[2]

همان‌طور که از نام این خدمات پیداست، امکان دسترسی سیستم‌های مختلف رایانه‌ای، نظیر کامپیوترهای رومیزی، کامپیوترهای قابل حمل، تلفن‌های همراه و نظایر آن را با شبکه‌های اطلاع‌رسانی رایانه‌ای فراهم می‌کنند. این خدمات برای خود سلسله مراتبی دارند که به اجمال عبارتند از:

- **ارائه‌دهندگان خدمات دسترسی حضوری (کافی‌نت‌ها):**[3]

این مراکز که روز به روز بر تعدادشان در سراسر کشورمان افزوده می‌شود، با دایر کردن

1. Virtual Space
2. Access Service Providers
3. Coffee Nets

مکان‌هایی با چندین سیستم رایانه‌ای متصل به شبکه اینترنت، به ارائه خدمات دسترسی می‌پردازند. هرچند ممکن است به فراخور امکاناتشان خدمات دیگری نیز ارائه دهند.

- **ارائه‌دهندگان خدمات اینترنتی[1] (ISP)**

افرادی که امکان مراجعه به خدمات دسترسی حضوری برایشان میسر نیست یا این‌که نمی‌خواهند به آن‌ها مراجعه کنند و قصد دارند از محل کار یا منزل یا حتی به شکل بی‌سیم از طریق سیستم‌های رایانه‌ای مستقل خود با اینترنت ارتباط برقرار کنند، می‌توانند از یک ارائه‌دهنده خدمات اینترنتی **اعتبار**[2] موقت یا دائم اخذ کنند.

- **ایجادکنندگان نقطه تماس بین‌المللی**[3]

اگر کاربری بخواهد با سایتی ارتباط برقرار کند که میزبان آن در خارج از کشور قرار دارد، ارائه‌دهنده خدمات اینترنتی باید با یک ایجادکننده نقطه تماس بین‌المللی ارتباط برقرار کند. این خدمات امکان دسترسی فرامرزی کاربران را فراهم می‌کند و به همین دلیل، از نقش تعیین‌کننده‌ای برخوردار است، زیرا کاربران جز در زمینه ارتباطات شبکه‌ای که تحت شمول خدمات انتقال قرار می‌گیرد، برای دیگر تعاملات شبکه‌ای از طریق خدمات دسترسی اقدام می‌کنند.

به این ترتیب، این خدمات به دلیل در اختیار داشتن بخش قابل توجهی از داده‌های خصوصی کاربران برای ارائه خدمات دسترسی و همچنین سوابقی که راجع به‌نحوه تعاملات سایبری‌شان به دست می‌آورند، از ابتکار عمل بالایی نسبت به مصون داشتن یا تعرض شدید به حریم داده‌های الکترونیکی‌شان برخوردارند. لذا باید تحت شمول مقررات دقیق و لازم‌الاجرایی قرار گیرند.

همچنین، از آنجا که تمامی ارائه‌دهندگان خدمات به‌عنوان مجموعه‌هایی حرفه‌ای فعالیت می‌کنند، نباید در رابطه با آنها ضوابط حرفه‌ای برآمده از مقررات **خودتنظیمی**[4] را نادیده انگاشت. امروزه برای اجرای هرچه صحیح‌تر و مؤثرتر قوانین جامع و کلی مصوب، عمدتاً مسائل فنی و تخصصی مربوطه به مراجع ذی‌ربط واگذار می‌شود تا آن‌ها با شناخت اساسی‌تری که از حوزه فعالیت‌شان دارند، در اجرای صحیح آن‌ها ضوابط مربوطه را وضع نمایند. این ضوابط می‌توانند به‌ویژه برای حوزه‌های جدید که عمدتاً برای قانونگذاران ناآشنا می‌باشند، بسیار مفید واقع شوند. البته در صورتی که از محدوده مجاز پیش‌بینی شده فراتر نروند. حال با توجه به اهمیت و حساسیت روزافزون حریم داده‌های الکترونیکی و نقشی که ارائه‌دهندگان خدمات می‌توانند ایفا کنند، جایگاه و اهمیت این‌گونه مقررات به خوبی مشخص خواهد بود.

---

1. Internet Service Providers
2. Account
3. International Access Points
4. Self-Regulation

۳-۲. دیگر فعالان سایبری

دلیل اصلی متمایز ساختن دو گروه مجریان قانون و ارائه‌دهندگان خدمات شبکه‌ای از دیگر فعالان سایبری، این بود که آن‌ها به ترتیب اهرم قانون و پل‌های اصلی ارتباط با فضای سایبر را در اختیار داشتند. اما این تأکید به این معنا نیست که دیگر فعالان سایبری از هیچ نقش تأثیرگذاری بر حوزه حریم داده‌های الکترونیکی برخوردار نیستند و نباید به آن‌ها در سیاستگذاری‌های خرد و کلان توجه کرد.

به‌طور کلی، هر کس تحت هر عنوانی به ارائه خدمات سایبری می‌پردازد، بخشی از داده‌های خصوصی مراجعین خود را دریافت می‌کند. حال ممکن است این دستیابی به موجب قانون باشد، خود کاربر با رضایت برای بهره‌مندی از خدمات بیش‌تر آن‌ها را ارائه دهد، یا این‌که فعال سایبری مورد نظر به طرق مجاز یا غیرمجاز به آن‌ها دست یابد. مهم‌ترین مثالی که می‌توان در رابطه با الزام قانونی ارائه داده‌های خصوصی بیان کرد، به فعالیت‌هایی مربوط می‌شود که برای گروهی از کاربران مجاز و برای بقیه غیرمجاز تلقی می‌شود. برای مثال، در بسیاری از کشورها دسترسی به **محتوای مستهجن بزرگسالان** برای کاربران زیر ۱۸ سال تمام ممنوع است. لذا برای تفکیک افراد مجاز از غیرمجاز در بدو ورود به سایت‌ها، از آن‌ها خواسته می‌شود اطلاعات معتبر معرف خود را وارد نمایند. یکی از مهم‌ترین این داده‌ها **شماره کارت اعتباری** است. زیرا تنها به اشخاص بالای ۱۸ سال تمام داده می‌شود و می‌تواند بهترین معرف باشد. با این حال، محرز است این شماره بسیار ارزشمند است و می‌تواند موجبات انواع سوءاستفاده‌ها، به‌ویژه زیان‌های مالی را فراهم نماید.

همچنین، بهره‌برداری کاربران از فعالیت‌های رسمی، نظیر خدمات بانکداری الکترونیکی، آموزش الکترونیکی یا دیگر امور اداری در جامعه کنونی، مستلزم این است که یکسری داده‌های خصوصی در پایگاه‌های داده به صورت آن‌لاین نگهداری شود و همچنین داده‌های خصوصی دیگری نیز به محض مراجعه به سایت‌ها دریافت شود که بالطبع همان مسائل با شدت و ضعف خود مطرح خواهند بود.

شایان ذکر است، مقررات برخی کشورها به صاحبان سایت‌ها اجازه می‌دهند برای تسهیل پیشبرد فعالیت‌های مشروع خود، داده‌های خصوصی کاربران را دریافت و به نحو مقرر مورد استفاده قرار دهند. اما برای این‌که اختیار عمل از مراجعین سلب نگردد، در صفحه اول آن‌ها، گزینه‌ای با عنوان **خط مشی حریم خصوصی**[1] تعبیه شده و در آن جزئیات نحوه استفاده از داده‌های خصوصی ذکر گردیده تا در صورت عدم رضایت کاربر، از وارد کردن آن‌ها خودداری کند.

---

1. Privacy Policy

اما در جایی که فعالان سایبری رأساً مبادرت به دریافت داده‌های خصوصی کاربران می‌کنند، تهدیدات جدی‌تری بروز می‌یابد، حتی اگر برخی از آن اقدامات مشروع باشند. برای مثال، **کوکی‌ها**[1] برنامه‌هایی هستند که متناسب با نوع برنامه‌ریزی‌شان، به محض اتصال یک کاربر به سایت مربوطه، به سیستم رایانه‌ای وی انتقال می‌یابند و کلیه اطلاعات راجع به نوع سیستم عامل، برنامه‌های کاربردی موجود و همچنین، علایق و مطلوبیت‌های فردی کاربر را به سایت مورد نظر منتقل می‌کنند. با این حال، باید توجه داشت با این‌که درجاتی از کوکی‌ها مجاز شناخته شده‌اند و برای ساماندهی حوزه‌های سایبری، به‌ویژه ارائه خدمات شبکه‌ای و همچنین داد و ستد و تجارت الکترونیکی مفید ارزیابی می‌شوند، اما می‌توانند لطمات زیانباری نیز به حریم داده‌های الکترونیکی افراد وارد آورند. چنانچه آن‌ها به‌گونه‌ای برنامه‌ریزی شوند که کلیه داده‌های خصوصی اشخاص را انتقال دهند یا این‌که سایت مورد نظر داده‌های خصوصی دریافتی را به دیگر سایت‌ها نیز انتقال دهد، دیگر چیزی به نام داده‌های خصوصی، رضایت کاربر و اساسی‌تر از همه حریم داده‌های الکترونیکی معنا نخواهد داشت.

متأسفانه چندی است این وضعیت به حد نگران‌کننده‌ای رسیده است. زیرا عده‌ای جمع‌آوری، ذخیره‌سازی و بهینه‌سازی داده‌های خصوصی کاربران را **حرفه** خود قرار داده‌اند یا خود از آن‌ها جهت اقدامات تعرض‌آمیز بعدی استفاده می‌کنند یا به مرتکبین آن‌ها می‌فروشند. بارزترین آن‌ها **آدرس‌های پست الکترونیکی** و کلیه داده‌های خصوصی راجع به آن‌ها هستند که برای ارسال **پیام‌های تبلیغاتی ناخواسته الکترونیکی** (که به اختصار **اسپم**[2] نامیده می‌شود) مورد استفاده قرار می‌گیرند و در همین راستا، برنامه‌هایی طراحی شده‌اند که به‌طور خودکار آدرس‌های کاربران را از فضای سایبر جمع‌آوری می‌کنند یا این‌که به‌صورت پیش‌فرض آن‌ها را تولید می‌کنند و به مبالغی مانند هر یک میلیون ۵۰ دلار فروخته می‌شود.

همچنین، مسأله دیگری که بهره‌برداری از داده‌های خصوصی را البته برای سودجویان به شکل بهینه‌ای فراهم ساخته و در قسمت‌های قبل نیز به آن اشاره گردید، تطبیق داده‌هاست. این مزیت که از ویژگی متمرکزسازی و یکپارچه‌سازی داده‌ها در فضای سایبر نشأت می‌گیرد، به افراد امکان می‌دهد با کنار هم قرار دادن کلیه یا اکثر داده‌های خصوصی به نتایجی دست یابند که در حالت پراکندگی‌شان غیرممکن یا بسیار مشکل بود. بدیهی است این وضعیت برای سودجویان نیز بسیار مطلوب می‌باشد. زیرا به‌طور نتیجه‌بخش‌تر و مؤثرتر می‌توانند برای سوءاستفاده از داده‌های خصوصی افراد برنامه‌ریزی کنند.

---

1. Cookies
2. Spam

با توجه به توضیحات فوق، به نظر می‌رسد ساماندهی حریم داده‌های الکترونیکی در حوزه این فعالان، به مراتب نسبت به دو گروه مجریان قانون و ارائه‌دهندگان خدمات شبکه‌ای مشکل‌تر است. زیرا در این‌جا شخصیت‌های بسیار متنوع‌تری به فعالیت‌های بسیار متنوعی مشغولند که سیاستگذاری و برنامه‌ریزی برای امور آنها مجاهدتی عظیم می‌طلبد. متأسفانه آنچه در این‌جا کار را مشکل‌تر می‌سازد این است که بجز آن‌هایی که همانند مجریان قانون و ارائه‌دهندگان خدمات به شکل رسمی فعالیت می‌کنند، مانند بانکداران الکترونیکی، بقیه به هیچ‌گونه محدودیتی مقید نیستند و در واقع ابتکار عمل در دست آن‌هاست که با مهارت فنی بالا و تجربه ارزشمندی که از تعامل با این فضا به دست آورده‌اند، می‌توانند هرگونه فعالیت مجاز یا غیرمجازی را طرح‌ریزی و اجرا کنند.

منابع و مآخذ

1. Rowland, Diane & Macdonald, Elizabeth; Information Technology Law; Cavendish Publishing; 2005.

۲. فضلی، مهدی، بررسی مسئولیت کیفری ارائه‌دهندگان خدمات اینترنتی، پایان‌نامه دوره کارشناسی ارشد حقوق جزا و جرم‌شناسی، دانشگاه تهران، پردیس قم، مهرماه ۱۳۸٤.

۳. جلالی فراهانی، امیرحسین، پیشگیری وضعی از جرائم سایبر در پرتو موازین حقوق بشر، فصلنامه تخصصی فقه و حقوق، ش ٦، ۱۳۸٤.

۴. دفتر ارتباطات و فناوری‌های نوین، مرکز پژوهش‌های مجلس، کنوانسیون جرائم سایبر، ش ۷٦٤٦، سال ۱۳۸٤.

۵. نوری، علی‌محمد و نخجوانی، رضا، حقوق حمایت داده‌ها، تهران، نشر گنج دانش، ۱۳۸۳.

۶. وزارت دادگستری ایالات متحده امریکا، ترجمه امیرحسین جلالی فراهانی، تفتیش و توقیف سیستم‌های رایانه‌ای و تحصیل ادله الکترونیک در تحقیقات کیفری، ۲۰۰۲، معاونت حقوقی و توسعه قضائی قوه قضائیه، ۱۳۸۲.

۷. دزیانی، محمدحسن، جرائم حمایت از داده (گزارش توجیهی)، سازمان مدیریت و برنامه‌ریزی کشور، ۱۳۸۱.

۸. قاجار قیونلو، سیامک، حریم خصوصی/ حمایت از داده‌ها، چارچوب مدل قانونگذاری برای ایران، انتشار محدود سازمان مدیریت و برنامه‌ریزی کشور، ۱۳۸۰.

شناسنامه گزارش	شماره مسلسل: ۸۰۶۹

عنوان گزارش: حریم خصوصی در فضای سایبر «حریم داده‌های الکترونیکی»

Report Title: cyber privacy "data protection"

نام دفتر: گروه ارتباطات و فناوری‌های نوین

تهیه و تدوین: امیرحسین جلالی فراهانی

ناظر علمی: بتول پاکزاد

متقاضی: معاونت پژوهشی

ویراستار: ـــــ

واژه‌های کلیدی و معادل انگلیسی آن‌ها: ـــــ

منابع و مآخذ تهیه گزارش:

در انتهای گزارش درج شده است.

تاریخ انتشار: ۱۳۸۵/۸/۲۳