

## حریم شخصی در فضای مجازی، با تکیه بر حقوق ایران

فرید محسنی (استادیار)

دانشکده‌ی علوم قضائی و خدمات اداری قوه قضائیه

فریدون قاسم‌زاده (استادیار)

دانشکده‌ی مدیریت و اقتصاد، دانشگاه صنعتی شریف

گسترش شبکه‌ی اینترنت دستیابی به اطلاعات در زمینه‌های مختلف را تسهیل کرده و مسلماً فواید زیادی به دنبال داشته است، ولی در عمل به‌عنوان وسیله‌ی برای نقض حریم شخصی نیز به‌کار رفته است. لذا کشورهای مختلف تدابیر گوناگونی برای حفظ حریم شخصی در فضای مجازی تدارک دیده‌اند. بررسی بسترهای مختلف برای صیانت از حریم شخصی در محیط مجازی - به‌ویژه از لحاظ حقوقی و قانونی - و نیز دامنه‌ی آن در تقابل با حق جامعه برای دانستن، از مسائل مهمی است که در این نوشتار مورد بحث قرار گرفته و با عنایت به قانون تجارت الکترونیکی ایران جوانب آن بررسی شده است.

### مقدمه

تاریخ بشر در دهه‌ی آخر قرن بیستم از طریق توسعه‌ی سریع شبکه‌های رایانه‌ی بهم مرتبط (از جمله اینترنت) در جهان دستخوش تحولی عظیم بوده است. یکی از نتایج این تحول ایجاد امکان دستیابی ساده، سریع و ارزان افراد مختلف در هر نقطه‌ی دنیا به اطلاعات گوناگون است. این تحول بزرگ جهان را به دهکده‌ی کوچک تبدیل ساخته که در آن هر شخصی به راحتی می‌تواند از آخرین تحولات علمی، صنعتی، سیاسی، اقتصادی، فرهنگی و غیره مطلع شود و ارتقاء سطح دانش و آگاهی‌ها امکان تسریع در پیشرفت و رشد درخت تنومند علم بشری و ایجاد رفاه و آسایش در زندگی انسان‌ها را فراهم آورده است، اما در عین حال عدم استفاده‌ی صحیح از این پدیده‌ی ارزشمند پیامدهای نامطلوبی را نیز به دنبال داشته که یکی از آنها نقض «حریم شخصی» افراد با استفاده از این ابزار توسط برخی از اشخاص، سازمان‌ها و یا حتی دولت‌هاست که با اهداف مختلف صورت می‌گیرد.

چنانچه استفاده از اینترنت تابع قانون‌مندی و نظم مشخصی نباشد، اگرچه این امکان بالقوه می‌تواند در مسیر مثبت و در جهت افزایش توانایی‌ها و رشد علمی و رفاه و آسایش انسانها قرار گیرد، در عمل ممکن است در مسیر منفی و به‌صورت مخرب و آزاردهنده مورد استفاده قرار گرفته و ایجاد دشواری در زندگی انسان را سبب شود و حتی به‌عنوان وسیله‌ی برای تهدید اشخاص مورد استفاده قرار گیرد که مصادیق بسیار زیادی از آن طی سالیان گذشته اتفاق افتاده است. مثلاً می‌توان به ارسال هزینه‌ها به‌صورت e-mail یا SMS‌های ناخواسته در حجم انبوه برای مردم، حمله‌ی خرابکارانه به سیستم آموزش الکترونیکی، از

جمله به دانشگاه‌های جورج میسون در ژانویه ۲۰۰۵ و دانشگاه‌هایی مانند تگزاس، جورجیا، میسوری، و کالیفرنیا طی یکی دو سال گذشته و دسترسی به اطلاعات حقوق اساتید، نمرات دانشجویان و غیره،<sup>[۱]</sup> نفوذ به شبکه‌ی بی‌سیم T-Mobile و برداشت مکاتبات و فایل‌های شخصی مشتریان این شرکت معروف که در سال گذشته به مدت ۷ ماه ادامه داشته، اشاره کرد.<sup>[۲]</sup> دو نمونه‌ی اخیر از این قبیل حملات به حریم شخصی افراد با سوءاستفاده از شبکه‌ی اینترنت است که باید برای مقابله با آن تدابیر مناسبی اندیشید. طی چند سال گذشته اقداماتی از سوی کشورهای مختلف در این مورد به عمل آمده است: تصویب مجازات‌های سنگین برای ارسال کنندگان هزینه‌ها و محکومیت یکی از این افراد به زندان طویل‌المدت برای اولین بار و نیز تصویب قانون مجازات در برخی کشورها مانند آمریکا، استرالیا و هنگ‌کنگ برای اشخاصی که با دوربین دستگاه‌های موبایل اقدام به عکس‌برداری از حریم شخصی افراد و ارسال آن برای دیگران می‌کنند.<sup>[۳]</sup> و نیز منع استفاده از دستگاه‌های موبایل دارای دوربین در برخی از کشورها مانند عربستان سعودی<sup>[۴]</sup> نمونه‌هایی از عکس‌العمل دولت‌ها نسبت به نقض حریم شخصی مردم در فضای مجازی است.

جوامع مختلف متناسب با دیدگاه و فرهنگ خود مرزهای متفاوتی برای حریم شخصی افراد قائل‌اند که می‌خواهند دیگران به آن راه نیابند. اینترنت در کنار منافع زیادی که در اختیار جامعه‌ی بشری قرار داده امکانات جدید و متنوعی نیز برای نقض حریم شخصی افراد و افشای اطلاعات محرمانه‌ی ایشان به‌وجود آورده که همین امر موجب عدم اطمینان بسیاری از افراد نسبت به مصونیت از تعرض و در نتیجه کاهش

استفاده از این امکان ارزشمند در بسیاری از موارد شده است. ارائه‌ی یک تعریف جامع از «حریم شخصی» بسیار دشوار است، زیرا نه تنها فرهنگ جوامع بلکه موقعیت‌ها و شرایط گوناگون نیز بر تعریف آن مؤثر است و لذا در بررسی مفهوم «حریم شخصی» باید مجموعه‌ی شرایط اعم از شرایط اجتماعی، مکانی، زمانی و غیره را مد نظر قرار داد. از سوی دیگر، حق حفظ حریم شخصی امری مطلق نیست بلکه روی دیگر سکه حق جامعه برای دانستن است که ممکن است در بعضی از شرایط با آن در تعارض باشد و در نتیجه لازم است در تبیین حقوقی و قانونی موضوع مرزهای این دو با معیارهای روشن به خوبی ترسیم شود.

قانون اساسی جمهوری اسلامی ایران در اصول ۲۲، ۲۳، ۲۵، ۲۸، ۳۲، ۳۳ و ۳۹ به شیوه‌های مختلف تمامیت و حریم شخصی و مصونیت افراد را بیان کرده است؛<sup>[۶]</sup> قانون مجازات اسلامی نیز در مواد مختلفی از جمله ۵۷۰ الی ۵۸۷، و نیز ۶۹۷ الی ۷۰۰ و یا ماده‌ی ۶۴۸ هریک به‌طریقی حریم شخصی افراد را تضمین کرده است ولی با توجه به پدیداری و گسترش اینترنت پاره‌ی مسائل جدی و جدید در خصوص «حریم شخصی» افراد مطرح است که لازم است با توجه به شرایط جدید مجدداً مورد بازنگری قرار گیرند.

در نوشتار حاضر برآنیم که ضمن بررسی مفهوم «حریم شخصی» و جوانب آن در فضای مجازی، راه‌های نقض و سپس راه‌های صیانت از حریم شخصی — به‌ویژه از طرق قانونی و حقوقی — را به‌طور کلی و با عنایت به قانون تجارت الکترونیک ایران مورد بحث قرار دهیم. در این نوشتار ابتدا تعریف «حریم شخصی» ارائه شده و اهمیت توجه به آن با توجه به گسترش اینترنت مورد بحث قرار گرفته است؛ سپس چگونگی جمع‌آوری اطلاعات شخصی افراد با استفاده از اینترنت تشریح و اصول کلی جهت صیانت از حریم شخصی افراد توسط خودشان ارائه شده است و به دنبال آن نقش دولت در ایجاد بسترهای قانونی، فرهنگی و سازمانی برای صیانت از حریم شخصی مردم به‌همراه پیشنهاداتی در این زمینه با توجه به شرایط کشورمان ارائه شده است که رعایت آن در تدوین قوانین جدید می‌تواند آثار بسیار مطلوبی را در حفظ حریم شخصی مردم داشته باشد.

## تعریف حریم شخصی

«حریم شخصی» تاکنون در ایران به‌وسیله‌ی قوانین تعریف نشده است. ارائه‌ی تعریف دقیق و کامل برای «حریم شخصی» کار دشواری است، زیرا عناصری نظیر عرف و فرهنگ اجتماعی و زمان و روحیات افراد در تعیین آن مؤثرند. و به‌لحاظ متفاوت بودن اینگونه عوامل در کشورهای گوناگون و نیز نسبت به اشخاص مختلف، تعیین معیارهای مشخص و تعریف جامع برای آن امری دشوار است. مثلاً اطلاع از عقاید شخصی

یا فرد مورد علاقه، و یا سرگرمی‌های اشخاص در کشورهای مختلف با حساسیت‌های گوناگونی همراه است. ممکن است فاش شدن برخی از اطلاعات شخصی برای افرادی مطلوب باشد در حالی که همان موضوع برای سایرین یا در شرایط دیگر کاملاً نامطلوب باشد. به‌رحال برای محدود کردن دامنه‌ی بحث، لازم است تعریفی هرچند کلی را مبنای قرار دهیم. از نظر اگرانف حریم شخصی عبارت است از «حق اشخاص، گروه‌ها، یا مؤسسات نسبت به تصمیم‌گیری در خصوص این که چه زمانی و تا چه حدی، اطلاعات مربوط به آنها باید در اختیار دیگران قرار گیرد».<sup>[۷]</sup>

با توجه به تعاریف مختلفی که در ادبیات برای «حریم شخصی» وجود دارد (که نمونه‌ی از آن ذکر شد) در نوشتار حاضر تعریف جامع‌تر و عمومی‌تر زیر را مبنای مباحث خود قرار می‌دهیم:

«حریم شخصی عبارت است از حق به حال خود گذاردن افراد و آزاد بودن آنها از مداخله‌ی غیرمعتاد و بدون اجازه در امور شخصی ایشان».<sup>[۸]</sup>

باید توجه داشت که هرچند خواست اشخاص درخصوص حفظ حریم شخصی آنها در جامعه محترم است، ولی حقوق جامعه برای دانستن مطالب نیز به همان میزان اهمیت دارد؛ لذا لازم است ابتدا معیارهایی برای تعیین مرزهای حریم شخصی و تشخیص مصادیق آن تعیین شود. در حقوق همه‌ی کشورها «قانون» و «عرف» دو معیار تشخیص مقررات و قواعد حقوقی محسوب می‌شوند و لذا در بحث حریم شخصی نیز حتی با فرض وجود تعریفی مشخص برای آن در قانون (هرچند که در قوانین موجود ایران این تعریف برای «حریم شخصی» وجود ندارد) یافتن معیارهای مناسب برای تشخیص مصادیق آن ضروری است و از این‌رو دشواری موضوع علیرغم اهمیت بالای آن به‌خوبی آشکار می‌شود. در موارد فقدان قانون، معمولاً عرف جامعه به‌عنوان قانون نانوشته مورد پذیرش جامعه است و حتی دادگاه‌ها نیز براساس آن تصمیم‌گیری می‌کنند، ولی چنان که اشاره شد تفاوت‌های فرهنگی و اجتماعی از عوامل تغییر در تشخیص مرزهای حریم شخصی‌اند؛ به‌عبارت دیگر، شخصیت اجتماعی انسان‌ها در تشخیص مرزهای حریم شخصی آنها مؤثر است.

در قوانین ایران موضوع «حریم شخصی» به‌طور پراکنده مورد توجه قرار گرفته است؛ مثلاً چنانچه پزشک وکیل یا اشخاصی که بر اثر ماهیت شغلی‌شان از اسرار شخصی افراد مطلع می‌شوند آنها را برملا سازند مشمول مجازات‌های کیفری می‌شوند. به‌عنوان مثال براساس ماده ۶۴۸ قانون مجازات اسلامی:

«اطباء و جراحان و ماماها و داروفروشان و کلیه‌ی کسانی که به مناسبت شغل یا حرفه‌ی خود محرم اسرار شناخته می‌شوند هرگاه در غیر از موارد قانونی، اسرار مردم را افشا کنند به سه ماه و یک روز تا

در ادبیات صورت گرفته است. یکی از محققان موضوعات اخلاقی در حوزه IT را به چهار دسته تقسیم کرده است:<sup>[9]</sup>

۱. حریم شخصی: جمع‌آوری، نگهداری و انتشار اطلاعات در مورد اشخاص؛

۱.۱. چه اطلاعاتی را افراد حق دارند در مورد خود نگه دارند و به دیگران نگویند؟

۲.۱. چه اطلاعاتی را می‌توان از شخص خواست تا در اختیار دیگران بگذارد؟

۳.۱. سازمان‌ها چگونه می‌توانند بر عملکرد کارکنان خود نظارت کنند؟

۲. دقت و صحت: اصالت، صداقت، دقت و صحت اطلاعات گردآوری شده، مسئولیت آن و شیوهی جبران خسارت زیان‌دیده.

۱.۲. چه کسی مسئول دقت و صحت اطلاعات گردآوری شده است؟

۲.۲. چه کسی پاسخ‌گوی خطاهای موجود در اطلاعات است؟

۳.۲. خسارت زیان‌دیده از اطلاعات نادرست چگونه باید جبران شود؟

۳. اموال: مالکیت و ارزش اطلاعات و مالکیت معنوی؛

۱.۳. مالک اطلاعات چه کسی است؟

۲.۳. ارزش و بهای منصفانه‌ی اطلاعات چگونه تعیین می‌شود؟

۳.۳. تحت چه شرایطی می‌توان از پایگاه‌های اطلاعات شخصی افراد استفاده کرد؟

۴. قابلیت دسترسی: حق دسترسی به اطلاعات مربوطه و پرداخت هزینه‌های دسترسی به آن و اشخاص مجاز برای دسترسی؛

۱.۴. چه کسی مجاز برای دسترسی به اطلاعات است؟

۲.۴. تجهیزات دسترسی به اطلاعات باید در اختیار چه کسانی باشد؟

۳.۴. یک فرد یا سازمان خاص صلاحیت دسترسی به چه اطلاعاتی و تحت چه شرایطی را دارد؟

چنان که ملاحظه می‌شود به دنبال توسعه‌ی استفاده از اینترنت، مسائل اخلاقی و حقوقی بسیار زیادی پدید آمده است که با عنایت به تعدد فرهنگ‌ها از یک سو، و عدم وجود مرز فیزیکی در ارتباطات اینترنتی، اهمیت و پیچیدگی موضوع بیشتر شده است. مسلماً باید توجه داشت که برای موفقیت مبادلات و تجارت الکترونیکی توجه جدی به

یک سال حبس و یا به یک میلیون و پانصد هزار تا شش میلیون ریال جزای نقدی محکوم می‌شوند.»

با مشخص شدن تعریف «حریم شخصی» و قانون‌مندی آن مهم‌ترین سؤالی که بلافاصله مطرح می‌شود این است که مرز این حریم تا کجا است؟ آیا پزشک در هیچ حالتی حق افشاء اسرار بیمار خود را ندارد؟ یا اگر بیماری شخصی مسری و برای جامعه خطرناک بود، وی موظف به افشای آن نیست؟

بسیاری از این موارد با مسائل اخلاقی مرتبط است که میانی آن در کشورها و جوامع مختلف متفاوت است، یعنی ممکن است امری که در یک جامعه کاملاً اخلاقی است در جامعه‌ی دیگر غیر اخلاقی شناخته شود که این مسئله موجب پیچیدگی بیشتر موضوع می‌شود.

به این ترتیب در می‌یابیم که بررسی موضوع حریم شخصی، ارائه‌ی تعریف مشخصی برای آن، تبیین دامنه و نهایتاً قانون‌مند ساختن آن با دشواری‌های بسیار همراه است. آنچه که تا کنون بیان شد مسائل و مشکلات مربوط به تعریف و قانون‌مندی حریم شخصی در زندگی معمولی است. هنگامی که این موضوع را در قلمرو اینترنت و فضای سایبر مورد بررسی قرار دهیم، به دلیل ابعاد جدیدی که موضوع به خود می‌گیرد این دشواری بسیار غامض و پیچیده‌تر می‌شود. در این نوشتار سعی بر آن است که توجه اصلی موضوع «حریم شخصی» در فضای مجازی که تا کنون کم‌تر در ایران مورد توجه قرار گرفته است متمرکز شود.

## اهمیت حریم شخصی در فضای مجازی

شبکه‌های به هم متصل رایانه‌ی، از جمله اینترنت، امکان دست‌یابی افراد از هر نقطه‌ی دنیا به اطلاعات گوناگون را فراهم آورده‌اند؛ به طوری که عملاً مرزهای جغرافیایی و فیزیکی بین کشورها در بسیاری از موارد برطرف و مفهوم دهکده‌ی جهانی در عمل محقق شده و برای اشخاص از درون رایانه یا تلفن همراه خود پنجره‌ی بی‌تمامی نقاط دنیا گشوده است. هرچند این پیشرفت بستری مناسب برای دست‌یابی عموم مردم به اطلاعات علمی، صنعتی، سیاسی، اقتصادی، فرهنگی و غیره فراهم ساخته، و فوائد و آثار بسیار زیادی در زمینه‌های گوناگون داشته و پیشرفت‌های علمی و تحقیقاتی زیادی به همراه داشته است، در عین حال سوء استفاده از این امکانات ارزشمند مخاطرات و پیامدهای جدی در زمینه‌های مختلف — از جمله نقض «حریم شخصی» — را در پی داشته است. نگرانی انسان‌ها از تجاوز دیگران به حریم شخصی و دست‌یابی آنان به اطلاعات شخصی ایشان، یا نظارت بی‌مورد بر اعمال و رفتار یا تفکرات آن‌ها موجب سلب آسایش، آرایش و امنیت ایشان می‌شود. مباحث زیادی در زمینه‌ی حریم شخصی در فضای مجازی و تقسیم‌بندی و سازمان‌دهی مناسب موضوعات اخلاقی مرتبط با آن

مسائل حقوقی و اخلاقی بسیار مهم است و به همین دلیل شرکت‌ها و سازمان‌ها برای بهبود شرایط اخلاقی در مجموعه‌ی خود تلاش کرده‌اند تا به منظور راهنمایی اعضای خود مجموعه‌ی خود اصول را طراحی و تدوین کنند.

در کشورهایی نظیر ایران که قوانین جامعی در زمینه‌ی «حریم شخصی»، به‌ویژه در زمینه‌ی مبادلات الکترونیکی، وجود ندارد توجه به این‌گونه مسائل برای ایجاد زمینه‌ی رشد و توسعه‌ی استفاده از اینترنت و تجارت الکترونیکی در کشور ضروری است. با توجه به این‌که تجاوز به حریم شخصی افراد در فضای مجازی با استفاده از اطلاعات شخصی مربوط به ایشان انجام می‌شود لازم است ابتدا منشأ پیدایش و گردآوری اطلاعات در فضای اینترنت، و نیز چگونگی نقض یا سوء استفاده از آن را بشناسیم تا بتوانیم راه‌های مختلف حمایت از کاربران از جمله حمایت‌های قانونی را مشخص کنیم.

## چگونگی جمع‌آوری اطلاعات شخصی از طریق اینترنت

جمع‌آوری و نگه‌داری اطلاعات اشخاص بدون اجازه‌ی ایشان، حتی اگر مورد استفاده قرار نگیرد، به‌خودی‌خود ناقض حریم شخصی افراد است، زیرا این کار فی‌نفسه موجبات تهدید و آزار روحی و نگرانی اشخاص را فراهم می‌کند. استفاده از اینترنت امکان جمع‌آوری آسان چنین اطلاعاتی را از افراد، بدون علم و آگاهی ایشان، به‌وجود می‌آورد. مثلاً وقتی فردی از سایت اینترنتی خاصی خرید انجام می‌دهد، اطلاعات زیادی در مورد او با اطلاع یا بدون اطلاع وی، توسط فروشنده جمع‌آوری می‌شود؛ در برخی از سایت‌های پیشرفته‌تر، حتی الگوهای خرید کاربران نیز مشخص می‌شود و مورد استفاده قرار می‌گیرد. این قبیل اطلاعات را بعضاً فقط سایت مزبور مورد استفاده قرار می‌دهد و در بسیاری از موارد به‌عنوان کالای تجاری با ارزش — بدون کسب مجوز از کاربران — معامله می‌شود. گام نخست برای فراهم کردن امنیت در زمینه‌ی اطلاعات شخصی افراد، شناسایی راه‌های جمع‌آوری اطلاعات است. برخی از روش‌های معمول برای جمع‌آوری اطلاعات شخصی افراد در فضای اینترنت عبارت‌اند از: خواندن مکاتبات گروهی اشخاص، پیداکردن افراد در راهنمای اینترنت، ضبط اطلاعات مرورگر اشخاص در مورد آنان، ضبط آنچه مرورگر شخص راجع به او می‌گوید، خواندن نامه‌های الکترونیکی (E-mail) اشخاص، ثبت اطلاعات توسط کاربران در سایت‌های اینترنتی و استفاده از cookie توسط پایگاه‌های اینترنتی؛ دو مورد اخیر از اهمیت بیشتری برخوردارند و به‌عنوان دو منبع اصلی جمع‌آوری اطلاعات محسوب می‌شوند.

ثبت اطلاعات توسط کاربران در پایگاه اینترنتی بدین صورت است

که پایگاه‌های اینترنتی اطلاعات کاربران را از طریق پرسش‌نامه‌هایی که پر می‌کنند (نظیر نام، شماره تلفن، آدرس پست الکترونیکی و حتی علائق و سرگرمی‌های آنان) دریافت می‌کنند. کاربران به‌منظور دستیابی به اسم رمز برای استفاده از امکانات هر سایت اینترنتی، خرید، شرکت در قرعه‌کشی، دستیابی به اطلاعات موجود در آن سایت یا انجام یک بازی اینترنتی اطلاعات را در آن سایت وارد می‌کنند. مثلاً برای کسب نتیجه‌ی یک آزمون از طریق اینترنت ممکن است تکمیل یک فرم در ابتدای کار ضروری باشد. این اطلاعات ممکن است به‌منظور بازاریابی، فروش آنها، یا اهداف گوناگون دیگری مورد استفاده‌ی گردآورندگان آن اطلاعات قرار گیرند، بدون آنکه افراد هدف اصلی از جمع‌آوری این اطلاعات را بدانند یا مجوزی از ایشان برای استفاده‌ی تجاری از این اطلاعات اخذ شود. البته وجود این نگرانی در برخی از کاربران همراه با دلایلی دیگر نظیر کمبود وقت، و نیز عدم تمایل به ارائه‌ی اطلاعات شخصی بعضاً موجب می‌شود که عده‌ی قابل توجهی از کاربران اینترنتی اصولاً از استفاده از امکانات این قبیل سایت‌ها منصرف شوند. براساس تحقیقات انجام شده از بین ۷۷٪ کاربران اینترنت که به‌صورت on-line خرید انجام نمی‌دهند، ۸۶٪ علت آن را ترس از استفاده از شماره‌ی کارت اعتباری یا اطلاعات شخصی خود توسط دیگران بیان داشته‌اند.<sup>[۸]</sup>

وسیله رایج دیگر برای جمع‌آوری اطلاعات فایل‌های Cookie هستند. Cookie یک فایل اطلاعاتی است که بدون اطلاع کاربر بر روی رایانه‌ی وی گذاشته شده و یک پایگاه اینترنتی را قادر به ضبط اطلاعات مربوط به کاربر بر روی رایانه‌ی خودش می‌کند به‌نحوی که بدون اجازه‌ی کاربر این اطلاع قابل استفاده‌ی سایت Cookie گذار باشد. مزیت Cookie برای کاربران عدم انجام کارهای تکراری و ورود اطلاعات مجدد در زمان استفاده‌ی بعدی از سایت و برای سایت اینترنتی جمع‌آوری اطلاعات بسیار مفید در مورد کاربران است.

سایت‌های اینترنتی به دلایل متعددی از Cookieها استفاده می‌کنند. Yahoo یا Excite برای شخصی کردن اطلاعات، Microsoft و Amazon.com برای افزایش فروش و خدمات اینترنتی و نیز Alta و Double click به‌منظور ساده‌کردن پیگیری روابط از این امکان استفاده می‌کنند. CNN با استفاده از Cookie در بخش مربوط به رای‌گیری از رای دادن مجدد اشخاص به یک موضوع خاص (البته به‌صورت محدود) جلوگیری می‌کند. همچنین برخی از طراحان پایگاه‌های اینترنتی با استفاده از Cookieها صفحات سایت خود را براساس علائق کاربران و خواست آنها به‌صورت پویا طراحی و ارائه می‌کنند.

همان‌طور که ملاحظه می‌شود هرچند Cookieها هدف‌مند و بعضاً در مسیر ارائه‌ی خدمات بهتر به کاربران طراحی می‌شوند، در هر حال از دیدگاه حریم شخصی بسیار نگران‌کننده‌اند زیرا به پایگاه‌های اینترنتی این امکان را می‌دهند که برخی اطلاعات خصوصی افراد نظیر مشخصات

برخی از سایت‌های اینترنتی ضمن ارائه‌ی اطلاعات در مورد سایت‌های مربوط به «حریم شخصی» توضیح می‌دهند که علت استفاده از Cookie توسط ایشان چیست و ضمناً اظهار می‌دارند که مشتریان در امر تصمیم‌گیری درخصوص آنچه که این سایت در مورد آنان می‌داند شخصاً مسئول‌اند؛ هدف آنان از این نکته پیشبرد و بهبود خدمات است. در عین حال آنان اعلام می‌دارند که چنانچه شرکت آنها بخواهد از اطلاعات کاربرانش استفاده کند، این کار را بدون جلب رضایت ایشان انجام نخواهد داد.

### روش‌های حفاظت از حریم شخصی

حفاظت از حریم شخصی در دو سطح کلان و خرد قابل بررسی است:

#### حفاظت از حریم شخصی در سطح کلان

پارهی از روش‌ها برای حمایت از حریم شخصی مرتبط با جامعه و تصمیمات کلانی است که خارج از اراده‌ی فردی است و نیازمند بسترهای گوناگونی است که غالباً توسط نهادهای حاکمیتی در جامعه ایجاد می‌شوند و در ادامه به آنها اشاره می‌کنیم:

#### الف) بستر فرهنگی

یکی از مهم‌ترین زمینه‌ها برای حفظ حقوق فردی و رعایت «حریم شخصی» ایجاد فرهنگ عمومی در جامعه مبنی بر ضرورت احترام به حریم شخصی دیگران است. گاهی این امر با آموزه‌های منطقی نظیر قراردادهای اجتماعی همراه است؛ یعنی تفهیم این معنی که اگر بخواهیم حریم شخصی‌مان محفوظ بماند لازم است به حریم شخصی دیگران احترام بگذاریم. مبانی اعتقادی در این خصوص نیز می‌تواند در ارتقاء سطح فرهنگ عمومی مفید واقع شود. ولی افراد جامعه نیز باید بیاموزند که نگره‌داری و حفظ اطلاعات شخصی آنها محدوددهی روشن دارد. روی دیگر سکه حق جامعه برای دانستن است، و لذا حق افراد برای حفظ حریم شخصی امر مطلق نیست که به هیچ عنوان قابل نقض نباشد. بنابراین در کنار ایجاد بستر فرهنگی لازم است مرزهای قانونی معین و روشنی تعریف شود تا روزه‌های سوء استفاده تا حد امکان مسدود شود.

#### ب) بستر قانونی

قانون باید دارای جنبه‌های گوناگون، از جمله تعیین مرزها برای مشخص کردن حد و مرز حقوق شخصی افراد و نیز ضمانت اجراء برای جلوگیری از نقض مقررات باشد. در قانون‌گذاری در خصوص حریم شخصی سه بُعد مهم باید مورد توجه قرار گیرد:

اولاً وضع قانون یا مقررات بازدارنده‌ی که موجب ایجاد ممنوعیت برای نقض حریم شخصی دیگران می‌شود، و نیز پیش‌بینی مجازات برای نقض آن سبب می‌شود که اشخاص از ارتکاب به این عمل اجتناب

فردی، ترجیحات، علایق و خصوصیات شخصی آنها را به صورت خودکار هنگام استفاده از سایت مورد نظر جمع‌آوری کنند، ضمن آن‌که اطلاعات جمع‌آوری شده توسط Cookieها دقیق‌تر از ثبت آنها توسط خود افراد است چون امکان تحریف توسط کاربر در آن به راحتی وجود ندارد.

با توجه به توضیحات فوق مشخص می‌شود که ویژگی Cookieها، علاوه بر مزایایی که برای کاربران دارد، برای بازاریابان اینترنتی بسیار مطلوب است و در پارهی از موارد در مسیر منافع شخصی افراد سودجو و بدون کسب رضایت کاربران، کاربرد تجاری و بعضاً سیاسی دارند.

سؤال مهم این است که آیا افراد اجازه دارند اطلاعات شخصی افراد را با استفاده از ابزارهای قوی که اینترنت در اختیار می‌گذارند، جمع‌آوری و از آن استفاده کنند؛ و اگر «بله»، چگونه و تحت چه شرایطی؟

### روش‌های پیشگیری برای صیانت از حریم شخصی

با توجه به روش‌های جمع‌آوری و استفاده از اطلاعات شخصی افراد روش‌های صیانت از حریم شخصی در پنج اصل مهم خلاصه می‌شود که توسط اکثر کشورها از جمله کشورهای اروپایی، آمریکا و کانادا مورد استفاده قرار می‌گیرد:

۱. اطلاع و آگاهی دادن: گردآورنده‌ی اطلاعات شخصی باید هنگام جمع‌آوری مطالب به مصرف‌کنندگان آگاهی لازم را منتقل کند، به گونه‌ی که کاربران بتوانند درخصوص نوع و حدود افشاء اطلاعات بر مبنای مقاصد گردآورنده تصمیم‌های آگاهانه اتخاذ کنند.

۲. انتخاب و رضایت: کاربران باید از چگونگی استفاده از اطلاعات شخصی‌شان مطلع شوند. رضایت اشخاص می‌تواند از طرق مختلف و در مراحل گوناگون اخذ شود. در هر صورت رضایت کاربران مهم‌ترین عنصر جمع‌آوری اطلاعات است.

۳. دسترسی و مشارکت: کاربران باید بتوانند به اطلاعات شخصی خود دسترسی داشته و صحت آن را کنترل کنند.

۴. تمامیت و امنیت: کاربران باید اطمینان یابند که اطلاعات جمع‌آوری شده محفوظ و صحیح است و در نتیجه لازم است اطلاعات مصون از زیان، دسترسی غیر مجاز، تخریب، استفاده‌ی متقلبانه و نظایر آن باشد.

۵. اجرای قانون و جبران خسارت: شیوه‌ی اجرای قانون و جبران خسارت از موارد مهم حفظ حریم شخصی است. چنانچه قدرت بازدارنده‌ی برای تخلفات وجود نداشته باشد نتیجه‌ی حاصل خواهد شد. لازمه‌های جبران خسارت عبارت‌اند از مداخله‌ی دولت برای حفظ نظم در روابط اشخاص و قانون‌گذاری برای جبران خسارت اشخاص یا پدید آمدن مقررات و عرف‌های مورد قبول عامه.

استفاده‌ی کارمندان در زمان انجام خدمت مجاز شمرده می‌شوند. تنها باید در قوانین روشن شود که کدام نوع نظارت و تا چه میزانی قابل قبول است؟ یا این‌که اساساً چه کسی متولی نظارت بر این قبیل امور باشد؟ همچنین یکی از مقدمات مهم برای قانون‌گذاری وجود تعریف و سیاست مشخص برای حفظ حریم شخصی در جامعه است.

برخی از ادارات و سازمان‌ها با مشخص کردن اهداف خود از جمع‌آوری اطلاعات، یا اطمینان بخشیدن به مشتریان مبنی بر این که این اطلاعات صرفاً برای بهبود کیفیت ارائه‌ی خدمات به ایشان جمع‌آوری می‌شود و مورد خرید و فروش یا سوء استفاده قرار نخواهد گرفت و این که اطلاعات جمع‌آوری شده خارج از اهداف مذکور در سایت مورد استفاده قرار نخواهد گرفت رضایت و اطمینان مشتریان را جلب می‌کنند. بنابراین در تنظیم مقررات نیز می‌توان از این‌گونه روش‌ها بهره جست و مثلاً شرط نمود که جمع‌آوری‌کننده‌ی اطلاعات باید به میزان ضروری و صرفاً برای مقاصد تعریف شده اطلاعات کسب کند و حق واگذاری آنها را به غیر ندارد مگر با اطلاع و رضایت شخص و در عین حال امکان تصحیح و تغییر اطلاعات باید برای صاحب آن وجود داشته باشد و همچنین مسئولیت کیفری و مدنی نقض قانون و حریم شخصی افراد نیز در آن تعیین شده و ضمانت اجرای مناسب برای آن در قانون پیش‌بینی شود.

این‌گونه موارد امور عینی و مشخصی هستند که می‌توانند در تعیین ضوابط و مقررات مربوط به «حریم شخصی» به‌عنوان معیارهای معین مورد استفاده قرار گیرند، معیارهایی که عملاً موجب جلب اطمینان اشخاص و در نتیجه افزایش کاربران اینترنت به دلیل ایجاد اطمینان در ایشان نسبت به حفظ حریم شخصی آنها خواهند بود.

#### ج) بستر سازمانی

در کنار بسترهای فرهنگی و قانونی که در سطح کلان برای صیانت از حریم شخصی اشخاص در جامعه ضروری‌اند، ایجاد بسترهای سازمانی از طریق به‌وجود آوردن و تقویت سازمان‌های غیرانتفاعی موسوم به NGO<sup>۱</sup> که از طریق ارائه‌ی اطلاعات به مصرف‌کنندگان موجب اطمینان بخشیدن به آنان در زمینه حفظ حریم شخصی‌شان می‌شوند ضروری است و موجب می‌شود گردآورندگان اطلاعات استانداردها و ضوابط مربوط به حفظ حقوق شخصی کاربران را مورد توجه قرار دهند. نمونه‌هایی از این سازمان‌ها که امروزه در کشور آمریکا فعال‌اند عبارت‌اند: ج - Trust<sup>(۸)</sup>: سازمانی غیرانتفاعی است که هدفش ایجاد اطمینان و اعتماد در کاربران اینترنت در مورد عدم جمع‌آوری و افشاء اطلاعات شخصی مربوط به ایشان است. این سازمان سیاست ترویج رضایت کاربران را دنبال می‌کند و روش کار آن بدین صورت است که سایت‌های مختلف در صورت کسب شرایط لازم درخصوص رعایت ضوابط مربوط به حریم شخصی که توسط این سازمان تعیین شده، می‌توانند

ورزند. ثانیاً پیش‌بینی جبران خسارت به منظور اعاده‌ی خسارت به کسانی که به دلیل نقض حریم شخصی دچار خسارت مادی یا معنوی شده‌اند براساس قوانین مشخص؛ ثالثاً نظارت بر عملکرد جمع‌آوری‌کنندگان یا اساساً پیش‌بینی متولی برای نظارت بر اجراء صحیح قانون و تشخیص صحت اطلاعات جمع‌آوری شده و تهیه‌ی آیین‌نامه‌ها و غیره.

در برخی از کشورها برای ایجاد ضابطه و نظم اجتماعی قوانینی درخصوص حریم شخصی در اینترنت تصویب شده است. مثلاً در ایالات متحده‌ی آمریکا، قانون فدرال حمایت از حریم شخصی در اینترنت، سازمان‌های فدرال آمریکا را از ارائه‌ی سوابق شخصی یا سوابق شناسایی پزشکی، مالی یا پیشینه‌ی استخدامی مربوط به هر شخص ممنوع می‌کند.

همچنین قانون حمایت از حریم شخصی ضمن ارتباطات و حمایت از مصرف‌کننده در آمریکا از نظر قلمرو و نیز تلاش برای حفظ حریم شخصی در تجارت الکترونیک یکی از جامع‌ترین قوانین در این زمینه است. یکی از موارد مهمی که از طریق قانون‌گذاری قابل تبیین است، نقش و میزان دخالت دولت درخصوص موارد مربوط به حریم شخصی است زیرا در این امر از یک‌سو مسئله‌ی حقوق و آزادی‌های فردی و از سوی دیگر حق جامعه برای دانستن مطرح است، و لازمه‌ی این امر وجود مرزهای روشن و عینی است تا شهروندان نسبت به محدوده‌ی حقوق خود مطلع شوند. مثلاً اگر یکی از مقامات اداری یا سیاسی مرتکب یکی از جرایم مانند اختلاس، سوء استفاده از مقام و غیره شود، نمی‌تواند مدعی شود که خبر اعمال ارتكابی او به لحاظ ضرورت حفظ حریم شخصی وی نباید منتشر شود، زیرا جامعه حق دارد بداند و اهمیت اطلاع عموم از این موضوع بیش از اهمیت حفظ حریم شخصی وی در این مورد است؛ به‌عنوان مثال چنانچه هنرپیشه یا ورزشکاری مرتکب سرقت از فروشگاه شود و استدلالش برای لزوم مخفی ماندن عملش از افکار عمومی حفظ حریم شخصی باشد این خواسته نمی‌تواند مورد قبول دادگاه واقع شود زیرا حق جامعه برای دانستن — به‌ویژه در مورد اشخاص شناخته شده که بعضاً در جامعه به‌عنوان الگو مطرح‌اند — مقدم بر حفظ حریم شخصی آنان است.

مسلماً تجارت الکترونیکی هنگامی به ظرفیت کامل خود می‌رسد که استفاده‌کنندگان از سیاست‌ها، اقدامات، راه‌های رسیدگی به شکایات و محدوده‌ی حقوق خود از طریق قوانین مطلع باشند. مثلاً مسئله‌ی نظارت بر کاربران از امور قابل توجه در این زمینه است.

بسیاری از کاربران در ادارات و شرکت‌ها کنترل می‌شوند. و کارمندان در مقابل نظارت کارفرما بر عملکردشان از حمایت بسیار محدودی برخوردارند. گرچه تلاش‌ها و اعتراضات حقوقی زیادی در این خصوص وجود دارد ولی امروزه غالباً براساس مفاد قوانین در اکثر کشورها، کارفرمایان درخواندن پیام‌های الکترونیکی و نیز نظارت بر نحوه‌ی

ج - ۵) سازمان‌های متفرقه: سایت‌هایی نیز برای ارزیابی فروشندگان توسط مصرف‌کنندگان وجود دارند که از جمله درخصوص حریم شخصی اعلام‌نظر می‌کنند.<sup>۳</sup>

حفاظت از حریم شخصی در سطح خرد صرف‌نظر از وظایف دولت و ارگان‌های اجتماعی، هریک از افراد نیز به‌لحاظ ضرورت پیشگیری باید در هر شرایطی اقدام به حفظ حریم شخصی خود کنند. بدیهی است برای نیل به این هدف لازم است پیشگیری به یک فرهنگ عمومی تبدیل شود. به‌رحال به‌منظور حفظ هرچه بهتر حریم شخصی افراد رعایت مواد زیر توسط کلیه کاربران توصیه می‌شود:

الف) دقت و تأمل قبل از ارائه‌ی اطلاعات شخصی بر روی یک سایت؛

ب) پیگیری درخصوص استفاده از نام خود؛

ج) در دسترس قرار ندادن مکاتبات گروهی؛

د) استفاده از بی‌نام‌کننده‌ها (Anonymizer) به‌هنگام جست‌وجو و استفاده از اطلاعات. نرم‌افزارهای مناسب برای این کار به‌راحتی و از طریق اینترنت قابل تهیه‌اند؛

ه) عدم استفاده از فایل‌های Cookie تا حد امکان؛

و) استفاده از رمز مناسب؛

ز) درخواست از ISP یا کارفرمای مربوطه در مورد این که برای حفاظت از حریم شخصی بسیاری از اطلاعات آنان در بانک‌های اطلاعاتی نگه‌داری شوند. مثلاً وقتی شخصی درخواست خرید تلفن جدید می‌کند، ممکن است فرم پرسشنامه‌ی را تکمیل کند که پس از آن در بانک اطلاعاتی نگه‌داری می‌شود. بانک‌ها، مؤسسات مالی، اداره‌ی مخابرات، آژانس‌های مسکن، بیمارستان‌ها، مدارس، دانشگاه‌ها، ادارات پست، شهرداری‌ها، کتابخانه‌ها، شرکت‌های بیمه و نظایر آن بانک‌های اطلاعاتی هستند که اطلاعات مختلف در مورد اشخاص را در اختیار دارند. مسلماً لازم است ضوابط و مقرراتی برای حفظ اطلاعات، امکان یا چگونگی استفاده از آن، و نیز چگونگی تغییر مطالب و مقام صالح برای دسترسی و نظایر آن مشخص شود تا اشخاص نگران اطلاعات ارائه شده توسط خود نباشند.

### بررسی حریم شخصی در قانون تجارت الکترونیکی

ایران (مصوب ۸۴/۱۰/۲۴)

قانون تجارت الکترونیکی جمهوری اسلامی ایران در تاریخ ۸۲/۱۰/۲۴ به‌تصویب نهایی مجلس شورای اسلامی رسیده است. استفاده از اینترنت

از علامت Trust در سایت خود استفاده کنند و با نمایش علامت مذکور اعتماد مصرف‌کنندگان را به حفظ حریم شخصی آنها توسط سایت حامل این آرم جلب کنند. در واقع وجود این علامت نشان‌گر آن است که سایت مورد نظر به‌لحاظ رعایت ضوابط لازم در جمع‌آوری و نگه‌داری اطلاعات به‌نحو مسئولانه توانسته است مجوز استفاده از علامت Trust را کسب کند. مانند شرکت‌هایی که گواهی‌نامه‌ی ISO دریافت و اجازه‌ی استفاده از آرم مربوطه را تا مدت معینی به‌دست می‌آورند. البته سایت‌ها برای کسب مجوز مذکور باید هزینه‌ی متناسب با نوع فعالیت‌شان پرداخت کنند.

در نیمه‌ی سال ۱۳۰۰، ۱۹۹۸، سایت اینترنتی برجسته از جمله America Online, IBM Ecite, Cyber Cash, AT&T, Netscape, Lycos, Infosseek, Geocities, CNET, Buena Vista Internet Group, Yahoo, The New York Times به‌عنوان شرکت‌کنندگان در Trust قراردادی را امضا کردند. هرچند تاکنون تخلفاتی نسبت به حفظ حریم شخصی توسط شرکت‌هایی که حامل مهر Trust بوده‌اند گزارش نشده است ولی این روش موجبات کنترل و کاهش این تخلفات را به‌صورت نهادی و مستمر فراهم آورده است. ج - ۲) BBB: BBB سازمانی غیرانتفاعی است که وسیعاً توسط اعضاء خود حمایت شده و روش کار این است که در مورد شرکت‌های تجاری قبل از انجام یک خرید، برای مصرف‌کنندگان گزارش تهیه می‌کند. شرکت‌هایی که استانداردهای اینترنتی BBB را رعایت کنند، بر روی وبسایت خود لوگوی BBB Online را نمایش می‌دهند که از این طریق اعتماد مشتریان برای استفاده از سایت مذکور به‌ویژه از لحاظ رعایت حقوق کاربران جلب می‌شود. مصرف‌کنندگان می‌توانند با کلیک کردن روی لوگوی مذکور، گزارش BBB در مورد شرکت‌های عضو را دریافت کنند.

ج - ۳) WHICH Online: سازمانی دیگر برای حمایت از مصرف‌کنندگان است که توسط جامعه‌ی اروپایی حمایت می‌شود و مهر آن نشان‌دهنده‌ی آن است که به مشتریان اطمینان می‌دهد که تجار اینترنتی توسط سازمان مذکور از جنبه‌های مختلف برای روشن شدن استاندارد عملکردشان مورد سؤال و بررسی قرار می‌گیرند. حریم شخصی مصرف‌کنندگان از جمله مسائل مورد سؤال و بررسی سایت مذکور است. ج - ۴) اتحادیه‌ی حریم شخصی اینترنتی: گروهی متمایز و مرکب از شرکت‌ها و مؤسساتی است که حامی حریم شخصی افراد در اینترنت است و رهنمودهایی برای سیاست‌های حریم شخصی و فعالیت‌های اینترنتی ارائه می‌کند و اعضاء مهم آن عبارت‌اند از: Microsoft, IBM, Dell, Compaq, Bell Atlantic, AT&T, Yahoo, Time Warner, Netcom اتحادیه مذکور از برنامه‌های اجرایی نهادهایی مانند Trust و BBB حمایت می‌کند.

در ایران از چندین سال قبل از تصویب این قانون، آغاز شده و لذا در حلقه قانونی رویه‌های مختلفی در جامعه، مراجع قانونی و اداری شکل گرفته است. هرچند قانون مذکور جامع نیست و نکات متعددی برای تکمیل و اصلاح آن باید مد نظر داشت، به‌رحال ظهور آن نویدبخش مشروعیت و مقدمه‌ی برای تکمیل و رشد و نیز تدارک سایر ضوابط و مقررات تکمیلی در آینده است. با توجه به نکات ذکر شده درخصوص حریم شخصی، برخی نکات مهم مربوط به قانون تجارت الکترونیک ایران را در ادامه مورد بحث قرار می‌دهیم:

الف) برای «تجارت الکترونیک» که اصولاً قانون به آن نام تصویب شده در هیچ‌جا تعریفی ارائه نشده و مشخص نیست که آیا طبق تعاریف متداول این قانون شامل زیرشاخه‌های تجارت الکترونیکی نظیر بانک‌داری الکترونیکی، پزشکی الکترونیکی و غیره نیز می‌شود یا برای هر یک از این شاخه‌ها باید قانون جداگانه‌ی مشابه همین قانون وضع و تصویب کرد.<sup>[۱۰]</sup>

ب) فصل سوم از قانون تجارت الکترونیک به‌عنوان حمایت از «داده‌پیام»‌های شخصی اختصاص یافته است. در حالی که اساساً لفظ «حریم شخصی» که رکن اساسی در تجارت الکترونیکی است در این قانون مشخصاً تعریف نشده و حمایت از حقوق اشخاص درخصوص اطلاعات شخصی‌شان مورد بحث و حمایت قرار نگرفته است.

ج) براساس ماده‌ی ۵۸ قانون «ذخیره، پردازش یا توزیع «داده‌پیام»‌های شخصی مبین ریشه‌های قومی یا نژادی، دیدگاه‌های عقیدتی، مذهبی، خصوصیات اخلاقی و «داده‌پیام»‌های راجع به وضعیت جسمانی، روانی و یا جنسی اشخاص بدون رضایت صریح آنها به‌هر عنوان غیر قانونی است.»

براساس ماده‌ی مذکور هرچند حریم شخصی تعریف نشده ولی امنیت موارد و مصادیقی از حریم شخصی مورد حمایت قانون‌گذار قرار گرفته که عبارت‌اند از داده‌پیام‌های شخصی که مبین این موارد هستند: ریشه‌های قومی یا نژادی، دیدگاه‌های عقیدتی مذهبی، خصوصیات اخلاقی و وضعیت جسمانی، روانی یا جنسی.

در متن ماده موارد مذکور به‌عنوان مثال و مصداق ذکر نشده و آنجا که در موارد دیگر ضمانت اجرای کیفری برای نقض ماده‌ی حاضر پیش‌بینی شده است قاعداً چنین استنباط می‌شود که به‌هر دلیل، صرفاً موارد مذکور مدنظر قانون‌گذار برای حمایت قانونی بوده است، حال آن که با توجه به توضیحات قبلی مشخص شد که موارد حریم شخصی محدود به این موارد نیست و گستره‌ی آن بسیار وسیع‌تر است. دلیل انتخاب تنها چند مورد از موارد متعدد مربوط به حریم شخصی توسط تهیه‌کنندگان پیش‌نویس قانون مشخص نیست و شاید تنها دلیل

آن استفاده از متن استاندارد UNCITRAL در مورد قانون تجارت الکترونیکی برای تهیه پیش‌نویس قانون فوق بدون اعمال بسیاری از تغییرات ضروری در آن برای شرایط ایران باشد. به‌هر حال موارد متعدد و حائز اهمیت دیگری وجود دارند که توجه به آنها در حفاظت قانونی از حریم شخصی در فضای مجازی بسیار مهم است که از آن جمله می‌توان از اطلاعات شخصی افراد (مانند وضعیت تأهل یا سن، میزان دارایی یا انتسابات فامیلی، میزان تحصیلات، آدرس‌های مختلف شخص، سوابق کاری، کیفری، اداری و نظایر آن) نام برد که محرمانه‌مانند آنها معمولاً برای اشخاص بسیار مهم است. آیا اگر کسی از این‌گونه اطلاعات شخصی افراد استفاده کند یا آنها را در اختیار دیگران قرار دهد، می‌توان براساس این قانون متعرض او شد؟ به‌علاوه در ماده‌ی مذکور رضایت شخص به‌عنوان تنها شرط برای امکان استفاده از اطلاعات ذکر شده مربوط به او منظور شده است و در آن قید شده: «... بدون رضایت صریح آنها به هر عنوان غیرقانونی است.»

و در نتیجه همان‌طور که ملاحظه می‌شود قانون‌گذار هرگونه استفاده، تحت هر عنوان دیگر را ممنوع دانسته و برای آن ضمانت اجرای نیز قرار داده است. هرچند نیت تنظیم‌کنندگان قاعداً حمایت از حقوق اشخاص و حریم شخصی آنان بوده است، ذکر آن به‌صورت مطلق و بدون قید و شرط و بدون ذکر استثنائات، موجب می‌شود که به‌ناچار و بنابه ضرورت‌ها ضابطه‌ی مذکور نقض شود. لذا باید از ابتدا در قانون توجه داشت که در پاره‌ی موارد مصالح اجتماعی ایجاب می‌کند که مقامات قضائی یا امنیتی بتوانند برای حفظ حقوق اجتماع به این‌گونه اطلاعات، ولو خود شخص رضایت ندهد، نیز از طریق قانونی دسترسی داشته باشند و به‌همین دلیل لازم است قانون خود راساً موارد استثناء را برشمارد. چنان که پیش از این بیان شد در تعارض حقوق فردی در زمینه‌ی حریم شخصی و حق جامعه برای دانستن، در پاره‌ی موارد مهم باید حق جامعه محفوظ بماند و جامعه از اطلاعات شخصی افراد مطلع شود. لذا عدم درج قید و یا استثنائات مهم نظیر «... مگر بنابه دستور مقام قضائی یا امنیتی» و نظایر آن موجب می‌شود که چنانچه مقامات مذکور نیز بنا به ضرورت ماده‌ی مذکور را نقض کنند مشمول ضمانت اجرای آن شوند.

به‌هر حال هنگام تعیین استثنائات قانون برای نقض حریم شخصی باید احتیاط کامل برای انسداد هرگونه منافذ سوء استفاده رعایت شود، به‌گونه‌ی که به‌بهبهانی امنیت، حریم شخصی افراد به‌راحتی نقض نشود زیرا چنان‌که پیش‌تر بیان شد عدم جلب اطمینان کاربران موجب تقلیل استفاده از مبادلات الکترونیکی می‌شود. البته در ماده‌ی ۶۱ این قانون<sup>۴</sup> آمده است که استثنائات و افشای آن برای اشخاص ثالث، اعتراض و غیره براساس آیین‌نامه‌ی مربوطه خواهد بود. هرچند ظاهراً متولی تهیه‌ی این آیین‌نامه نظیر سایر موارد در قانون معین نشده، با فرض تعیین نیز

شخصی به نحو خاص وجود ندارد، اساساً از لحاظ نگارش حقوقی ترجیح داشت عدم مغایرت با قوانین جاریه‌ی کشور منظور می‌شد، ثانیاً در این ماده موارد مناسبی برای حفظ حقوق مربوط به حریم شخصی که در قوانین کشورهای مختلف درج شده ملاحظه می‌شود ولی لازم است کلیات مندرج در آن به نحو اجرایی مد نظر قرار گیرد تا عملاً قابل استفاده و اجرا باشد. مثلاً در بند (ج) از ماده‌ی ۵۹ قید شده که داده‌پیام باید صحیح و روزآمد باشد. گرچه به طور کلی این امر مطلبی مناسب است و عدم رعایت آن توسط گردآورنده عواقب قانونی پیش‌بینی شده در قانون را به دنبال دارد ولی این مقدار برای جلب اطمینان مردم به منظور استفاده‌ی کامل از اینترنت و تجارت الکترونیکی کافی نیست، بلکه وجود نهادهای دولتی و غیردولتی مورد حمایت دولت ضروری است تا به انحاء مختلف این اطمینان را برای اشخاص پدید آورند و به عبارتی صحت مطالب را به گونه‌ی تأیید کنند تا جلب اعتماد عمومی صورت پذیرد. ثالثاً نظر به آنکه در ایران دولت از طریق اعمال تصدی و حاکمیت در اداره‌ی امور مختلف نقش فعال و مؤثری دارد، عملاً تا زمانی که نهادهای خودجوش یا سازمان‌های خصوصی جدی در تجارت و مبادلات الکترونیکی فعال نیستند ترجیح دارد که با تعیین نهادهای خاص به‌عنوان متولی، نقش ناظر، تأیید کننده و مطمئن‌کننده را در خصوص حریم شخصی ایفاء کند تا از این طریق درصد استفاده از تجارت الکترونیکی افزایش یابد.

ماده‌ی ۶۰ قانون<sup>۵</sup> در خصوص ذخیره، پردازش یا توزیع داده‌پیام‌های مربوط به سوابق پزشکی است. همان‌طور که ملاحظه می‌شود علی‌رغم اهمیت آن تفصیل امر به تدوین آیین‌نامه‌ی محول شده است. در واقع با روش مذکور، قانون در حال حاضر تکلیف موضوع را روشن نکرده و اساساً آیین‌نامه از لحاظ حقوقی تجلی مفاد قانون و بسط آن است و نباید در اصل وظیفه‌ی قانون‌گذاری از این طریق به طور کامل محول شود ولی در واقع قانون‌گذار صرفاً عنوان موضوع مرتبط با سوابق پزشکی را مطرح و مفاد آنرا محول به تنظیم آیین‌نامه‌ی خاصی کرده است.

یکی دیگر از نکات مهمی که در این خصوص باید مد نظر قرار گیرد آن است که در زمینه‌ی مسائل پزشکی دو جنبه‌ی مهم وجود دارد: از یک طرف حریم شخصی افراد و ضرورت محرمانه بودن اطلاعات پزشکی آنان نظیر عقیم بودن، ابتلاء به سرطان و یا بیماری‌های خاصی که شاید غالباً ترجیح دهند سایرین از آن‌ها بی‌اطلاع باشند اهمیت دارد. از سوی دیگر با عنایت به گسترش بیماری‌های مسری نظیر ایدز و هیپاتیت حق جامعه برای اطلاع و پیشگیری از سرایت آن به سایرین مد نظر است که لازم است هنگام قانون‌گذاری هر دو نکته مورد توجه قرار گیرد. ماده‌ی ۶۱ قانون نیز نظیر ماده ۶۰ تکلیف موضوعاتی نظیر استثنائات، اعتراض و غیره را به تنظیم آیین‌نامه‌ی مربوطه محول کرده که پس از تنظیم مفاد آن قابل بحث است.

اولاً گاهی در خصوص تهیه‌ی این‌گونه آیین‌نامه‌ها غفلت می‌شود، ثانیاً به لحاظ اهمیت موضوع لازم است در متن قانون موارد مهم تعیین شود و جزئیات آن به آیین‌نامه‌های مربوطه محول شود. لذا تا زمان تهیه‌ی آیین‌نامه نقص قانونی باقی است و از آنجا که طبق ماده‌ی ۷۹ وزارت بازرگانی موظف شده تا زمینه‌های مرتبط با تجارت الکترونیکی را که در اجرای قانون مذکور مؤثر است شناسایی و با ارائه‌ی پیشنهاد و تأیید شورای عالی فناوری اطلاعات، خواستار تدوین مقررات مربوطه و آیین‌نامه‌های آن توسط نهادهای ذیربط شود تا متعاقباً به تصویب هیأت وزیران در آید، لذا جا دارد در این خصوص اقدام لازم را معمول دارد. همچنین کلمه‌ی «رضایت» (مذکور در ماده ۵۸) از لحاظ حقوقی دارای مفهومی دقیق و تخصصی است. به طور کلی «رضایت» در مورد همه‌ی افراد برای مجاز بودن یک عمل کافی و یا اساساً شرط نیست. رضایت برخی از اشخاص در پاره‌ی موارد اساساً نمی‌تواند مبنایی برای صحت و مشروعیت عمل محسوب شود بلکه معیارهای دیگر نظیر عقل و رشد برای نافذ بودن یک عمل حقوقی ضروری است.

همان‌طور که می‌دانیم درصد قابل توجهی از کاربران در مبادلات الکترونیکی کودکان، نوجوانانی هستند که هنوز به رشد کامل نرسیده‌اند. فرض کنید در یک سایت مربوط به نوجوانان، با استفاده از احساسات و تمایلات آنان عکس‌ها، مطالب، خاطرات و بسیاری از مطالب آنان جمع‌آوری و نهایتاً رضایت آنها نیز به طریقی اخذ شود. آیا چنین امری ناقض ماده‌ی مذکور است؟ مسلماً «رضایت» شرط کافی برای امکان ذخیره و پردازش و توزیع اطلاعات نیست و در نتیجه لازم است این‌گونه موارد با حوصله‌ی قانونی مورد مذاقه و بحث و بررسی قرار گیرد.

براساس ماده‌ی ۵۹ قانون مذکور، در صورت رضایت شخص نیز به شرط آن‌که محتوای داده‌پیام موافق قوانین مصوب مجلس شورای اسلامی باشد، ذخیره، پردازش و توزیع «داده‌پیام»‌های شخصی در بستر مبادلات الکترونیکی مشروط به شرایط زیر شده است:

الف) اهداف آن مشخص و واضح باشد؛

ب) تنها به اندازه‌ی ضرورت و متناسب با اهداف اعلام شده باشد و صرفاً برای اهداف مذکور استفاده شود؛

ج) باید صحیح و روزآمد باشد؛

د) دسترسی شخص به اطلاعات مربوط به خود و امکان محو و یا اصلاح آنها میسر باشد؛

ه) درخواست محو اطلاعات توسط شخص در هر زمان مقدور باشد.

اولاً در صدر ماده‌ی مذکور مطابقت داده‌پیام با قوانین مصوب مجلس شورای اسلامی به عنوان شرطی برای آن درج شده که البته به لحاظ آنکه قانون مصوب دیگری در زمینه‌ی مبادلات الکترونیکی و یا حریم

مواد ۷۱ و ۷۲ و ۷۳ قانون مذکور، مجازات نقض مواد ذکر شده را بیان کرده است که در این خصوص نیز ایجاد نهادهای متولی در تشخیص موارد نقض می‌تواند بسیار راه‌گشا و مؤثر باشد. و از طرفی می‌تواند در هماهنگی با مراجع قضایی نقش مطلوبی ایفاء کند.

### نتیجه‌گیری

هرچند تصویب قانون تجارت الکترونیک ایران در سال ۱۳۸۲ (علی‌رغم نواقص و کاستی‌های آن) نویدبخش آغاز قانون‌مند شدن فعالیت‌های اینترنت در تجارت الکترونیکی و جامعه‌ی ما بوده است، برای بهبود و پیشرفت و ارتقاء آن باید تلاش کرد و توجه داشت که بستر قانونی برای توسعه‌ی اینترنت و تجارت الکترونیکی به قوانین متعددی که با جامع‌نگری و توجه به سایر قوانین موجود در کشور تهیه شده باشند و نیز اصلاح قانون مصوب موجود نیاز دارد. همچنین در خصوص قانون مربوط به حریم شخصی اینترنت که مورد توجه نوشتار حاضر است لازم است:

۱. حریم شخصی به‌طور واضح تعریف و معیارهای تشخیص آن معلوم شود. برای این کار ضرورت دارد از دستاوردهای کشورهای دیگر استفاده‌ی مطلوب به‌عمل آید.
۲. در تعارض حق حریم شخصی و حق جامعه برای دانستن، محدوده‌ی مشخصی تعریف شود تا براساس معیارهای عینی بتوان مرزهای آن را تبیین کرد.
۳. گردآورندگان اطلاعات بر اساس قانون:
  - ۱.۳. اهداف خود از جمع‌آوری را به‌نحو روشن و دقیق بیان کنند.

۲.۳. اطلاعات صرفاً به‌میزان لازم و در راستای هدف اعلام شده جمع‌آوری شود.

۳.۳. شخص ذی‌نفع به مطالب جمع‌آوری شده دسترسی داشته باشد و امکان محو و اصلاح آنها وجود داشته باشد.

۴.۳. مطالب جمع‌آوری شده جز با رضایت کامل و قانونی شخص قابل استفاده دیگری نباشد.

۵.۳. اطلاعات باید از لحاظ صحت و دقت بررسی شده و به‌روز نگه‌داری شود.

۶.۳. امکان اعتراض به استفاده از اطلاعات شخصی و تمهیدات فوری و نیز آیین دادرسی کامل برای این امر وجود داشته باشد.

۷.۳. جبران خسارت به‌نحو روشن و حقوقی تعریف شود.

۸.۳. راهکارهای ممانعت از Cookie ها یا جمع‌آورندگان اطلاعات، و نیز مجازات‌های مناسب برای تخلفات آنها پیش‌بینی شود.

برای تحقق این امر لازم است قوانین تکمیلی در ابعاد مختلف حریم شخصی تدوین شود و به‌ویژه با تبیین آیین دادرسی و نیز توسعه‌ی مباحث خسارت و جبران آن زمینه‌ی حمایت هرچه بیشتر از حریم خصوصی در فضای اینترنت فراهم آید تا عملاً موجبات اطمینان عموم از استفاده از تجارت الکترونیکی ایجاد شده و زمینه‌ی رشد و توسعه‌ی مطلوب و پایدار اینترنت و تجارت الکترونیکی در کشور فراهم شود. همچنین باید ضمانت‌های اجرایی لازم در قوانین مورد نظر پیش‌بینی و سازمان و رویه‌های لازم برای پیاده‌سازی مناسب قوانین مزبور و نظارت بر حسن اجرای آنها پیش‌بینی شوند.

### پانویس

1. Non-Government Organization
2. Better Business Bureau
۳. مثلاً سایت Deja.com که در حال حاضر بخشی از Google است و سایت epubliceye.com که به مصرف‌کنندگان اجازه می‌دهد در مورد حریم شخصی، اطمینان و رضایت‌مندی مشتری از فروشندگان اعلام نظر نمایند.
۴. ماده‌ی ۶۱ قانون تجارت الکترونیکی مصوب سال ۱۳۸۲: «سایر موارد راجع به دسترسی موضوع «داده‌پیام»، از قبیل استثنائات، افشای آن برای اشخاص ثالث، اعتراض، فراگردهای ایمنی، نهادهای مسئول دیدبانی و کنترل جریان «داده‌پیام»‌های شخصی به موجب مواد مندرج در باب چهارم این قانون و آیین‌نامه مربوطه خواهد بود».
۵. ماده‌ی ۶۰ قانون تجارت الکترونیکی (مصوب ۱۳۸۲): ذخیره، پردازش و یا توزیع «داده‌پیام»‌های مربوط به سوابق پزشکی و بهداشتی تابع آیین‌نامه‌ی است که در ماده‌ی (۷۹) این قانون خواهد آمد.

### منابع

1. www.washingtonpost.com, (12Jan 2005).

2. www.siliconvalley.com
3. Australian IT, www.australianit.news.com.au, (6Aug 2003).
4. Reuters/CNet, www.news.com, (14 Jun 2003).
5. The Age, 4Oct 2004, www.theage.com
۶. نجفی، مرتضی و محسنی، فرید «حقوق اساسی جمهوری اسلامی ایران»، انتشارات بین‌المللی المهدی، چاپ اول (۱۳۷۹).
7. Agranoff, M.H., "Controlling the threats to personal privacy", *Journal of Information Systems Management*, (summer 1993).
8. Turban, Efram, et al. *Electronic Commerce : A Managerial Perspective*, Prentice Hall (2004).
9. Mason, R.O., "Four ethical issues of the information age", *MIS Quarterly*, (March 1986).
۱۰. قاسم‌زاده، فریدون و محسنی، فرید «چالش‌های قانونی تجارت الکترونیکی در ایران»، کنفرانس بین‌المللی مدیریت، تهران، ایران (۱۳۸۲).