http://www.LPSC.ir
چهارمین کنفرانس ملی
حقوق و علوم جزا
مهر ماه ۱۳۹۶
4th National Conference on
Law & Criminal Sciences (October, 2017 IRAN)

حریم خصوصی در شبکه های اجتماعی

سمیه حبیب زاده[۱]*، کیومرث کلانتری [۲]،
دانشگاه آزاد اسلامی واحد چالوس

چکیده

حریم خصوصی به عنوان یکی از حقوق بنیادین بشری ، از جمله مهمترین حقوق فردی در دوران مدرن به شمار می رود که هم از نگاه شرع مقدس اسلام وهم از دید قوانین کشورها واسناد بین المللی ، محترم ومصون از تعرض می باشد . حق انسان بر خلوت و تنهایی و تنهایی و داشتن حریم خصوصی و به دور از نظارت و مداخله های غیر قا نونی و خود سرانه دیگران ، یکی از حقوق اولیه و بنیادین او به شمارمی رود به طوری که برای برخورد اری از چنین حقی نیاز به هیچ دلیل و توجیهی نیست . بدون تردید تجاوز به حریم خصوصی یک فرد به شرا فت ، حیثیت و استقلال فردی انسان لطمه وارد می کند بنا بر این باید از افراد در برابر نقض حریم خصوصی آن ها حمایت کرد . متأسفانه در نظام حقوقی جمهوری اسلامی ایران ، مقررات جامعی در زمینه حمایت از حریم خصوصی ، چه درمحیط واقعی وچه در فضای مجازی وجود ندارد . در حالی که هر نوع اطلاعاتی که جنبه شخصی دارند باید مورد حمایت قانونگذار قرار گیرند. شبکه اجتماعی ، مجموعه از افراد ، سازمان یا موجودیت های اجتماعی دیگر است که توسط یک مجموعه ای از رابطه های اجتماعی مانند مبادله اطلاعات ، همکاری یا دوستی مرتبط شده اند. تجزیه و تحلیل شبکه اجتماعی می تواند به منظور مطالعه عملکرد شبکه های کامپیوتری ، الگوهای جریان اطلاعات در جوامع ، رفتار ناشی از سیستم های فیزیکی و بیولوژیکی مورد استفاده قرار بگیرد حریم خصوصی افراد در شبکه های اجتماعی یکی از مهارت های مهمی است که کاربران می بایست از آن اطلاع داشته باشند .بعضی از افراد بدون هیچگونه توجهی هر چیزی را به اشتراک میگذارند از آنجایی که استفاده ما از اینترنت با دستگاه ها و برنامه های جدید روبه افزایش است، فهم چگونگی کنترل حرریم خصوصی حائز اهمیت میباشد.لازم به ذکر است با رشد چشمگیر فناوری های نوین اطلاعاتی و ارتباطی، مرز میان حریم خصوصی و زندگی اجتماعی بسیار باریک است. در واقع، این فناوری ها در کنار مزایای بسیار، زمینه‌ساز بروز لطماتی بر زندگی فردی و اجتماعی شده اند. آنچه این اثرات منفی را پررنگ می‌نماید بحث نقض حریم خصوصی افراد می‌باشد.

واژه‌های کلیدی: اطلاعات شخصی، حریم خصوصی،فناوری های نوین، مداخلات غیر قانونی.

۱- دانشجوی کارشناسی ارشد حقوق جزا و جرم شناسی
۲- دکتری حقوق جزا

۱- مقدمه

حریم خصوصی از منظر اسناد بین المللی، اسناد منطقه ای و قانون داخلی کشور ایران مورد توجه قرار گرفته است و همه اینها حیثیت و اسرار زندگی خصوصی انسان را مورد حمایت قرار می دهند .از آن جمله می توان به ماد ه ی (21) اعلامیه ی جهانی حقوق بشر، مصوب 1948 میلادی، اعلامیه ی حقوق بشر اسلامی 1990 قاهره، کنوانسیون حقوق بشر اروپایی، بیانیه 1968تهران، کنوانسیون شورای اروپا راجع به آزادی های اساسی، مصوب 1950 و کنوانسیون شورای اروپا راجع به حق حریم خصوصی در1995 اشاره کرد. هم چنین اصل (22) و (25) قانون اساسی ایران به مصونیت و عدم تعرض به حریم خصوصی افراد اشاره دارد، مگر در مواردی که با مصالح عمومی و حقوق دیگران در تزاحم باشد .بدیهی است، جواز این مداخلات با تشخیص مراجع ذی صلاح قضایی مقدور می باشد .در بررسی حمایت قانونی از حیثیت افراد در ایران می توان به قانون نحوه ی مجازات اشخاصی که در امور سمعی و بصری فعالیت های غیرمجاز می نمایند،مصوب 1372 ، ماد هی (640) قانون مجازات اسلامی و مواد ۱،۲،۱۶،۱۷ جرایم رایانه ای مصوب 1388 اشاره کرد .این مواد در راستای حفظ حیثیت افراد ا یجاد شده اند که به طورکلّی می توانند فضای مجازی را نیز در بر گیرند . علاوه بر حمایت کیفری از عفّت و اخلاق عمومی، حمایت از حریم خصوصی افراد، نیز به طور غیر مستقیم در اهداف اشاره شده ی فوق قرار میگیرد.

۲- کلیات و مفاهیم

۲-۱- مفهوم حریم خصوصی

حریم خصوصی، حق افراد برای برخورداری از حمایت در برابر مداخله بی اجازه ی دیگران در امور زندگیِ خود و خانواده شان است؛ خواه این عمل با ابزار مستقیم فیزیکی صورت پذیرد یا به وسیله نشر اطلاعات.(نمک دوست،۱۳۸۵،ص ۲۰۱). تعریف دیگری که به این تعریف نزدیک تر است، بر این موضوع اشاره دارد که حریم خصوصی، حق افراد برای حمایت شدن در مقابل ورود بدون اجازه به امور و زندگی افراد و خانواده هایشان، با ابزار مستقیم فیزیکی یا به وسیله ی نشر اطلاعات است .(جعفری،۱۳۸۵،ص ۴۸) در جایی دیگر در تعریف حریم خصوصی گفته شده: حریم خصوصی محدوده ای از زندگی شخص است که به وسیله ی قانون و عرف تعیین شده و ارتباطی با عموم ندارد، به نحوی که دخالت دیگری در آن ممکن است باعث جر یحه دار شدن احساسات شخص یا تحقیر وی نزد دیگران به عنوان موجود انسانی شود(رحم دل، ۱۳۸۴،ص ۱۲۹).در قوانین ایران اعم از قانون اساسی و یا عادی ،عبارت حریم خصوصی مورد استفاده قرار نگرفته است. و قانونگذار، به طور کلی، به استعمال الفاظی دال بر این معنا بسنده کرده است؛ از آن جمله می توان به مواد ۱ و ۲[1] قانون جرایم رایانه ای مصوب ۱۳۸۸

---

[1] -مادة (1) قانون جرايم رايانه اي در ارتباط با دسترسی غير مجاز مقرر می دارد: هرکس به طور غير مجاز به داده ها يا سامانه هاي رايانه اي يا مخابراتي که به وسيلة تدابير امنيتي حفاظت شده است دسترسي يابد، به حبس از نود و يک روز تا ... محکوم خواهد شد.
مادة (2) قانون جرايم رايانه اي در ارتباط با شنود غير مجاز مقرر می دارد: هرکس به طور غير مجاز محتواي در حال انتقال ارتباطات غير عمومي در سامانه هاي رايانه اي يا مخابراتي يا امواج الکترومغناطيسي يا نوري را شنود کند، به حبس از شش ماه تا ... محکوم خواهد شد.

در ارتباط با دسترسی و شنود غیر مجاز و مواد ۱۶ و ۱۷ [۱]همان قانون در ارتباط با حتک حیثیت اشاره کرد. اطلاعات شخصی و ارتباطات خصوصی با دیگران، که موضوع مقاله حاضر می باشد، جزو حریم خصوصی افراد قلمداد شده است. از این رو، با توجه به تعاریف مذکور می توان گفت حریم خصوصی، قرین عباراتی هم چون آسودگی خاطر، امنیت اسرار، حیثیت و آبروست و مفهوم آن امری نسبی است که از کشوری به کشور دیگر متفاوت است. تعریف حریم خصوصی که از موضوعات بسیار مهم حقوق بشری است، بسیار دشوار است؛ زیرا، تعریف حریم خصوصی به فرهنگ و زمینه ه ای اجتماعی و محیطی وابستگی دارد . در بسیاری از کشورها، این مفهوم با مقوله حفظ اطلاعات، که حریم خصوصی را در معنای مدیریت اطلاعات شخصی تفسیر می کند، پیوند خورده است(مرکز اطلاعات حریم خصوصی الکترونیکی،۲۰۰۲،ص ۱).[۲] گستردگی و انعطاف مفهوم حریم خصوصی به اندازه ای است که بدون تعیین معیارهای لازم برای مشخص کردن حدود آن نمی توان اقدام به اعمال سیاست حقوقی در حمایت از آن نمود. در بیشتر کشورها، تجاوز به حریم خصوصی از طریق فناوری اطلاعات و ارتباطات تحت شمول دو نوع مقررات کیفری قرار دارد : نخست، مقررات سنتی که ا ز حریم خصوصی اشخاص به طور عام حمایت می کند؛ مانند جرایم افتراء، افشای اسرار خاص و یا شنود، ضبط و افشای ارتباطات خصوصی؛ دوم :مقررات کیفری جدید قوانین راجع به حریم خصوصی، در ارتباط با رایانه ها، س یستم ه ای پردازنده و به طور کلی فناوری اطلاعات و ارتباطات، که نخستین تفاوت مربوط به داده هایی است که استفاده از آن ها ممنوع می باشد(زیبر،۱۳۸۶، ص ۱۸۳).

۲-۲- مفهوم حریم خصوصی در فضای مجازی

حریم خصوصی محدوده معقولی است که فرد انتظار دارد از دسترس دیگری مصون بماند .این دیگری، هم می‌تواند دولت باشد و هم سایر اشخاص حقیقی و حقوقی. حریم خصوصی در فضای مجازی تعریفی جز این ندارد، اما این فضا باعث شده تهدیدات و فرصت‌های جدیدی درحریم خصوصی افراد ایجاد شود. در این قسمت نگاهی داریم به این تهدیدها و فرصت‌ها که بدین شرح می باشد:

۲-۲-۱- ارتباط حریم خصوصی و اینترنت

ابتدا باید به ریشه حریم خصوصی بپردازیم. حریم خصوصی از زمانی اهمیت پیدا می‌کند که فرد اهمیت دارد و بدون فرد، حریم او هم وجود نخواهد داشت. از این‌روست که حریم خصوصی یک مفهوم مدرن است. در گذشته آنچه مهم بود جمع و جامعه بود و از این‌رو حریم جامعه یعنی مرز اهمیت پیدا کرده است. این گونه است که جنگ‌ها در گذشته از نظر کمی بسیار بودند و توجه زیادی هم به آنها شده است .با این حال در دوران مدرن با رشد تفکرات انسانگرایانه فرد اهمیت می‌یابد و همین

---

[۱] -ماده (16) قانون جرايم رايانه اي در ارتباط با هتک حيثيت مقرر مي دارد: هرکس به وسيلة سامانه هاي رايانه اي يا مخابراتي، فيلم يا صوت يا تصوير ديگري را تغيير دهد يا تحريف کند و آن را منتشر يا با علم به تغيير يا تحريف منتشر کند، به نحوي که عرفاً موجب هتک حيثيت او شود، به حبس از نود و يک روز تا ... محکوم خواهد شد.
ماده (17) قانون جرايم رايانه اي در ارتباط با حتک حيثيت مقرر مي دارد: هرکس به وسيله سامانه هاي رايانه اي يا مخابراتي، صوت يا تصوير يا فيلم خصوصي يا خانوادگي يا اسرار ديگري را بدون رضايت او جز در موارد قانوني منتشر کند، يا دسترس ديگران قرار دهد، به نحوي که منجر به ضرر يا عرفاً موجب هتک حيثيت او شود، به حبس از نود و يک روز تا ... محکوم خواهد شد.

[۲] -Electronic Privacy Information Center(EPIC).

موضوع خود را در حریم خصوصی نشان می‌دهد. حال توجه به این نکته جالب و ضروری است که همین فرد، تاثیرگذارترین عنصر در فضای مجازی است. فرد است که به اینترنت به مثابه کاربر آن هویت می‌بخشد. این موضوع بخصوص در سال‌های جدید و با ظهور شبکه‌های اجتماعی شکل تازه‌ای به خود گرفته است، چون در شبکه اجتماعی، آن که در مرکز توجه است همین کاربر یا به عبارتی فرد است .اوست که تولید محتوا می‌کند، نظر می‌دهد و جریان می‌سازد. حال که معلوم شد چرا و چگونه موضوع حریم خصوصی با فضای مجازی و شبکه اجتماعی گره خورده است باید به بسترهای مناسب نقض حریم خصوصی در فضای اینترنت بپردازیم و بعد از آن به این موضوع خواهیم پرداخت که چه کسانی با چه اهدافی اقدام به نقض حریم خصوصی در فضای مجازی و شبکه‌های اجتماعی می‌کنند.

۲-۲-۲- ناشناخته ماندن، فرصتی برای نقض حریم:

بستر اول این است که فرد یا کاربر در فضای مجازی امکان ناشناخته ماندن دارد .درست است که سازمان‌های اطلاعاتی و پلیسی و نیز هکرهای حرفه‌ای توانایی تشخیص هویت را دارند و درست است که بسیاری از کاربران با هویت معلوم در این فضا حاضر می‌شوند، اما مهم این است که امکان ناشناس ماندن برای کاربران در وضع عادی وجود دارد. این ناشناخته ماندن به صورت همزمان می‌تواند فرصت و تهدیدی برای حریم خصوصی در فضای مجازی باشد. از سویی فردی که ناشناخته بماند در حقیقت فردی جدید یا هویتی متفاوت برای خود اعتبار می‌کند تا حریم خصوصی واقعی او مصون بماند و از سوی دیگر همین فرد می‌تواند تهدیدی برای دیگر کاربران اینترنتی باشد. او می‌تواند با همین هویت نامعلوم تخلفات مختلفی انجام دهد که یکی از آنها نقض حریم خصوصی است.

۲-۳- مفهوم جرایم مجازی

جرایم سایبری، نوعی از جرایم اینترنتی می‌باشند که شامل جرم‌هایی هستند که در محیط سایبر بوجود می‌آیند، که در این مقاله ما به تعریف محیط سایبر که یک محیط مجازی می‌باشد و به ویژگی محیط سایبر، بطوریکه کاربران می‌توانند به هرگونه خدمات اطلاعاتی الکترونیکی در سراسر دنیا دستیابی پیدا کنند و چگونگی ایجاد جرایم که در فضای سایبر کپی عین اصل می‌باشد و انواع مجرمین محیط سایبر شامل هکرها، کرکرها، فریک‌های تلفن و انواع جرم‌های ممکن بانام سایبرکرایم و در مورد جرم آینده با نام تروریسم سایبر که مانند تروریست‌های معمولی دارای انگیزه‌های سیاسی برای ارتکاب جرایم هستندو همچنین بحران سازهای سایبر شامل ویروسها، عنکبوتهای موتورهای جستجو و پالس‌های الکترومغناطیسی، کرم‌ها و بمب‌های منطقی و در مورد پلیس سایبر که مطابق با خاص بودن جرم‌های سایبر، نیاز به آموزش‌های خاص دارند(باستانی،۱۳۸۳،ص ۴۵). پروفسور اولریش زیبر یکی از صاحب نظران معروف حقوق جزای رایانه معتقد است امروزه اجماع بین‌المللی براین است که جرم رایانه‌ای باید به طور کامل تعریف شود.

بنابراین تعریف کامل پذیرفته شده توسط گروه متخصصان oecd در سال ۱۹۸۳میلادی اصطلاح جرم رایانه‌ای بدین ترتیب تعریف شده: هرگونه رفتار غیرقانونی، غیراخلاقی یا غیرمجاز که مشتمل بر داده‌پردازی اتوماتیک یا انتقال داده‌ها باشد. مطالعات جدید مفاهیم وسیع‌تر و پیشرفته‌تری را از مجرمیت داده‌ها، یا جرم اطلاعاتی ارائه می‌کند.پروفسورشیک یکی از حقوقدانان

برجسته اتریشی در تعریف جرم رایانه‌ای چنین می‌گوید: جرم رایانه‌ای به هر عمل مجرمانه‌ای گفته می‌شود که در آن رایانه وسیله یا هدف ارتکاب جرم باشد.

برخی معتقدند گوناگونی تعاریف ارائه شده از جرم رایانه‌ای ناشی از اختلاف در دیدگاه‌هاست. برخی آن را ناشی از تفاوت در میزان دانش و آگاهی صاحب نظران می‌دانند؛ اما به نظر می‌رسد مشکلات موجود در تعریف جرم رایانه‌ای بیشتر از ماهیت این جرم ناشی می‌شود چگونه می‌توان تعریفی جامع و کامل از جرمی ارائه کرد که طیف وسیعی از اعمال، از نوشتن یک نامه توسط کارمند در رایانه‌ای گرفته تا بهره برداری از رایانه برای اختلاس میلیون‌ها دلار، را دربرگیرد.

هنوز این مجادلات پیرامون جرایم رایانه‌ای در میان صاحب نظران ادامه داشت. که با بروز اینترنت نوع دیگری از جرایم با عنوان جرایم اینترنتی مطرح گردید. و هنوز این واژه به بحث و مناظره در محافل علمی و تخصصی کشیده نشده بود که واژه جدیدی از جرایم رایانه‌ای تحت عنوان جرم سایبر در حال شکل گیری بود. پیدایش و شیوع جرایم تحت عنوان جرم سایبر بر پیچیدگی و دشواری ارائه تعریف کامل از جرم رایانه‌ای افزود و خود به مشکلی نو بدل شد .

۲-۴- مفهوم فناوری های امنیت اطلاعات

امنیت اطلاعات[1] به حفاظت از اطلاعات و به حداقل رساندن خطر افشای اطلاعات در بخش های غیرمجاز اشاره دارد . امنیت اطلاعات مجموعه ای از ابزارها برای جلوگیری از سرقت، حمله، جنایت، جاسوسی و خرابکاری و علم مطالعه روش های حفاظت از داده ها در رایانه ها و نظام های ارتباطی در برابر دسترسی و تغییرات غیرمجاز است .با توجه به تعاریف ارائه شده، امنیت به مجموعه ای از تدابیر، روش ها و ابزارها برای جلوگیری از دسترسی و تغییرات غیرمجاز در نظام های رایانه ای و ارتباطی اطلاق می شود فن آوری به کاربرد علم خصوصاً برای اهداف صنعتی و تجاری یا به دانش و روش های مورد استفاده برای تولید یک محصول گفته می شود.

۳- تاریخچه حریم خصوصی در فضای مجازی:

۳-۱- پیشینه ی حریم خصوصی در قانون اساسی ایران:

قانون اساسی ایران نیز گوشه چشمی به حریم خصوصی داشته است. اگرچه نویسندگان بر این باورند که طیف وسیعی از اصول قانون اساسی بویژه در فصل حقوق ملت با مفهوم حریم خصوصی در ارتباط و وابستگی‌اند و در عین حال هیچ اصلی بصراحت به مساله حریم خصوصی نپرداخته است، با این حال شاید بتوان اصل بیست و پنجم قانون اساسی را مرتبط‌ترین اصل با حریم خصوصی افراد دانست: «بازرسی و نرساندن نامه‌ها، ضبط و فاش کردن مکالمات تلفنی، افشای مخابرات تلگرافی و تلکس، سانسور، عدم مخابره و نرساندن آنها، استراق سمع و هر گونه تجسس ممنوع است مگر به حکم قانون «.نحوه نگارش اصل هیچ منعی برای گسترش دایره شمول آن به مصادیق جدید نظیر نامه‌های الکترونیک ایجاد نمی‌کند. استثنای پایانی قانون مگر به حکم قانون خود دایره وسیعی از اقدامات قانونی ـ قضایی را لازم می‌آورد. این استثنا به این معناست که موارد چنین تجسسی باید دقیقا در قانون روشن شود و در هر مورد خاصی باید با حکم پیشین مقام قضایی وفق شرایط قانونی انجام گردد. ماده ۱۰۰ قانون برنامه پنج ساله چهارم، دولت را مکلف به تدوین لایحه منشور حقوق شهروندی می‌کرد. یکی از محورهایی که

[1] - Information Security.

باید در این قانون تعریف و مورد حمایت قرار می‌گرفت، حفظ و صیانت از حریم خصوصی افراد بود. چند ماه بعد سیدمحمد خاتمی در روز پایانی ریاست‌جمهوری خود، لایحه حمایت از حریم خصوصی را همراه چند لایحه کلیدی دیگر تقدیم مجلس شورای اسلامی کرد. با این حال مجلس هیچ‌گاه وارد بررسی این لایحه نشد، زیرا هم نمایندگان مجلس با آن از در مخالفت در آمدند و هم دولت جدید در فروردین ۱۳۸۵ اقدام به استرداد آن کرد. این در حالی بود که گزارش کارشناسی مرکز پژوهش‌های مجلس به شماره مسلسل ۷۵۹۱ از آن لایحه استقبال کرد.

۳-۲- تاریخچه جرایم رایانه ای در ایران:

در خصوص تاریخ وقوع جرم رایانه ای در ایران، نمی توان وقوع آنرا با سال ۱۳۴۱ که رایانه وارد ایران شد همزمان دانست. کار برد رایانه در سالهای اولیه بسیار محدود بوده و در دهه ۵۰ و ۶۰ کم کم بر تعداد رایانه های موجود در ایران و همچنین وسعت برنامه های رایانه ای افزوده شد به دلیل عدم وجود قانون مدون و آمار دقیق از جرائم و سوء استفاده از رایانه نمی توان تاریخچه ای مشخص بیان نمود .

با توجه به گسترش رایانه و تکنولوژی اطلاعات در ایران با گسترش تخلفات مرتبط با کپی و تکثیر غیر مجاز نرم افزارها و برنامه هایرایانه ای سرانجام پس از سالها بحث و بررسی قانون حمایت از پدید آورندگان نرم افزارهای رایانه ای » در دی ماه ۱۳۷۹ تصویب شد که آئین نامه اول آن نیز در ۷۰ ماده تهیه و در اواخر سال ۱۳۸۰ جهت بررسی و تصویب به هیات وزیران ارسال شد .(فراهانی،۱۳۸۴،ص ۲۶).و در سال ۱۳۸۱ نیز طرح قانون تجارت الکترونیکی تهیه که نهایتاً متن آن در سال ۱۳۸۲ به تصویب نهایی مجلس شورای اسلامی رسید. از جمله موارد مهمی که می‌توان به آنها شاره نمود عبارتند از: جرم انگاری جعل، کلاهبرداری کامپیوتری، حمایت کیفری از حقوق مصرف کننده، حمایت از داده‌ها و کپی رایت.

براساس اطلاعات موجود اولین جرم اینترنتی در ایران در تاریخ ۲۶ خرداد ۱۳۷۸ به وقوع پیوست. که در آن یک کارگر چاپخانه و یک دانشجوی کامپیوتر در کرمان اقدام به جعل چک های تضمینی مسافرتی کردند و چون تفاوت و تمایز چندانی بین جرم کامپیوتری و جرم اینترنتی وجود ندارد، عمل آنها به عنوان جرم اینترنتی محسوب می شود.

بعد از این بود که گروه های هکر جرم های دیگری را مرتکب می شدند، مواردی چون جعل اسکناس، اسناد و بلیطهای شرکت های اتوبوسرانی، جعل اسناد دولتی از قبیل گواهینامه، کارت پایان خدمت، مدرک تحصیلی و جعل چک های مسافرتی و عادی بخشی از این جرایم اینترنتی هستند.

۳-۳- تاریخچه جرایم سایبری در ایران:

براساس اطلاعات موجود اولین جرم اینترنتی در ایران در تاریخ ۲۶ خرداد ۱۳۷۸ به وقوع پیوست. یک کارگر چاپخانه و یک دانشجوی کامپیوتر در کرمان اقدام به جعل چک‌های تضمینی مسافرتی کردند و چون تفاوت و تمایزی چندان بین جرم کامپیوتری و جرم اینترنتی وجود ندارد، عمل آن‌ها به عنوان جرم اینترنتی محسوب می‌شود.بعد از این بود که گروه‌های هکر موسوم به گروه مش قاسم و ...، جرم‌های دیگری را مرتکب می‌شدند، مواردی چون جعل اسکناس، اسناد و بلیط‌های شرکت‌های اتوبوسرانی، جعل اسناد دولتی از قبیل گواهینامه، کارت پایان خدمت، مدرک تحصیلی و جعل چک‌های مسافرتی و عادی بخشی از این جرایم اینترنتی هستند(حسن بیگی،۱۳۸۴،ص ۸۷).

براساس آمارهای موجود در سال ۱۳۸۴، ۵۳ مورد پرونده مربوط به جرایم اینترنتی در کشور تشکیل شد که کشف جرائم آمار ۵۰ درصدی را نشان می‌دهد.از مهمترین موارد جرم اینترنتی و رایانه‌ای در سال گذشته، ۳۲ مورد سوء استفاده از کارت‌های اعتباری ۱۱ مورد کلاهبرداری اینترنتی، ۷ مورد ایجاد مزاحمت از طریق اینترنت ، ۳ مورد کپی رایت و ۲ مورد نشر اکاذیب از طریق اینترنت و ۵ مورد موضوعات متفرقه بوده است. باتوجه به آمارهای سال ۸۴ میزان کشفیات مربوط به کلاهبرداری، جعل و سایر جرائم رایانه‌ای و اینترنتی ۱۱ درصد رشد را نشان می‌دهد.می‌توان گفت امسال هم جرایم رایانه‌ای و اینترنتی در کشورمان اتفاق افتاده که شاید یکی از مهمترین و خبرسازترین آنها، توزیع سی دی مستهجن منسوب به یکی از بازیگران مشهور زن بود و از مصادیق بارز جرم رایانه‌ای است.

۴- حریم خصوصی در شبکه های اجتماعی و فضای مجازی:

۴-۱- نقض حریم خصوصی کاربران:

حق انسان بر خلوت و تنهایی و داشتن حریم خصوصی به دور از نظارت و مداخله های غیر قانونی و خود سرانه دیگران، یکی از حقوق اولیه و بنیادین او به شمارمی رود. تجاوز به این حریم، به شرافت ، حیثیت و استقلال فردی افراد لطمه وارد می کند. بنابراین در برابر نقض حریم خصوصی، باید از افراد حمایت کرد .امروز با ظهور فناوری های نوین اطلاعاتی و ارتباطی ، پیدایش و گسترش رسانه های جدید و نیز توسعه فضای مجازی، امکان نقض حریم خصوصی اشخاص در این حوزه تسهیل شده و دغدغه ها و نگرانی های جدی ایجاد کرده است. حریم خصوصی در این فضا، حقی است که افراد برای حفظ اطلاعات شخصی خود و نحوه انتقال آن به دیگران دارند. شنود و رصد مکالمات و دسترسی به اطلاعات شخصی افراد، تهدیدی است که کاربران اغلب به آن بی توجه هستند .بزه دیدگان" جرایم سایبری اغلب افرادی هستند که به راحتی اطلاعات خود را در اختیار دیگری قرار داده‌اند. ضعف شخصیتی، ناآشنایی با محیط مجازی و بی‌دقتی در محافظت از داده‌ها از مهمترین دلایل قربانی شدن افراد در فضای مجازی است. اغلب نقض کنندگان حریم خصوصی به دلایلی نظیر افسردگی، عصبانیت، حسادت، حس انتقامجویی، حقارت و توجه نکردن به مسائل و اصول اخلاقی و ارزش‌های جامعه، خود را مجاز به ورود به حریم خصوصی قربانیان دانسته و خسارت‌های جبران‌ناپذیری را به حیثیت، مال و حتی جان افراد وارد می‌کنند .اطلاعات در فضای مجازی بسیار آسیب پذیرتر از مال و جان بوده و نیازمند رعایت جوانب امنیتی دقیق تر است. تلفن همراه وسیله مناسبی برای نگهداری اطلاعات، عکس و فیلم های خصوصی نیست و مجرمان را برای ارتکاب جرم بیشتر تحریک می کند. نقض حریم خصوصی افراد که احساس ناامنی روانی و اجتماعی در پی دارد، در بسیاری موارد به فروپاشی خانواده و از بین رفتن آبروی افراد منتهی می شود.عکس‌های آنلاین و پیام های ارسالی در وبلاگ ها و شبکه های اجتماعی که قابلیت ذخیره سازی بلندمدت دارند، به راحتی زمینه سوء استفاده دیگران را برای اهداف دیگر فراهم می کنند. از اینرو برای حفظ اطلاعات شخصی و جلوگیری از چنین پیامدهایی، افراد برای به اشتراک گذاشتن اطلاعات شخصی و بانکی در فضای مجازی با مقاصد نامعتبر و ناشناس، منع شده اند.در بسیاری موارد، محتوای تولید شده هر چند برای عضویت در یک شبکه اجتماعی و یا در جمع دوستان و نزدیکان ارائه شده باشد، به عنوان حربه ای علیه خود او استفاده می شود.شنود یا کمین سایبری نیز به شکل مستقیم و هدفمند ناقض حریم خصوصی افراد است. فضای نامحدود اینترنت، بستر خوبی برای کمین شکارچیانی است که در گمنامی به دنبال طعمه هستند(جاوید نیا،۱۳۸۷،ص ۶۷).تعقیب مکانی کاربران نیز همان ورود به حریم خصوصی افراد است که با برخی نرم افزارهای

اجتماعی میسر شده است. این مسئله می‌تواند کاربر را در برابر حملات سایبری، تبلیغات ناخواسته و حتی نقض حریم خصوصی فیزیکی آسیب‌پذیر کند. بسیاری از شرکت ها و صاحبان سرمایه با استفاده از اطلاعات شبکه، سلایق مخاطب، رفتارها و الگوهای خاص مصرف را در مناطق جغرافیایی جمع آوری کرده و منطبق با آن کالا و خدمات خود را بدون اطلاع گیرنده، بر او تحمیل می کنند .رسانه‌های جدید، علایق، تحرکات و رفتارهای کاربر را با جای پاهایی که از خود به‌جای گذاشته مشخص می کنند و در اختیار شرکت‌های تجاری و تبلیغاتی می گذارند تا حریم خصوصی افراد با محتوای تبلیغاتی اشباع و به توافق بیانی دیگر، نقض شود.کاربر و رسانه یا شبکه اجتماعی نیز یک نوع دسترسی به اطلاعات و نقض حریم خصوصی است. ارائه‌دهنده سرویس در توافقی کلی، مالک تمام اطلاعات آپلود شده کاربرانش می شود. گاهی دولت ها از همین شبکه ها نظیر فیسبوک به عنوان منبع اطلاعاتی برای کشف جرم، مکان‌یابی، رد یا تأیید ادعاها و همچنین فاش کردن مکاتبات خصوصی استفاده می‌کنند.

۴-۲- جلوه های نقض حریم خصوصی در شبکه های مجازی:

فناوری اطلاعات و ارتباطات به سرعت به جمع آوری اطلاعات شخصی افزوده است و افزایشِ نقض حریم خصوصی در فضای مجازی ب هویژه اینترنت، نگرانی ه ای زیادی را برای کاربران به وجود آورده است؛ به طوری که اگر اشخاص مطمئن باشند، اطلاعات هویتی و شخصی آنان در مقابل اشخاص ثالث فاش نمی شود، آن ها تمایل زیادی به استفاده آزادانه از اینترنت دارند .حریم خصوصی، برای شرکت ه ایی که اطلاعات از مشتریان خود را از طریق تارنما دریافت می کنند، نیز موضوع بسیار مهمی است .بعضی از این شرکت ها، سیاست های تأمین حریم خصوصی افراد را بر روی تارنمای خود توسعه داده اند .شرکت ها برای دست یابی به اطلاعات شخصی افراد، بایستی ملزم به ایجاد قرارداد و اجرای سیاست های تأمین حریم خصوصی باشند.(حسنی،۱۳۸۵،ص ۸۹).

تجار تمایل زیادی به استفاده از اطلاعات خصوصی افراد برای بهبود بازار دارند و اکثر شرکت ها از فروش اطلاعات هویتی اشخاص سود می برند. گسترش فناوری های جدید و توان استفاده از وسایل و امکاناتی که به راحتی قابلیت نفوذ در مکان های خصوصی را دارند؛ از جمله دورب ین ه ای دید در شب و یا میکروفن های مخفی و سایر ابزارهایی که زمانی فقط از سوی سازمان های جاسوسی قابل استفاده بود و امروزه به راحتی در اختیار همه افراد جامعه قرار دارد، امکان مداخله در حریم خصوصی را به شدت افزایش داده است(آقا بابایی،۱۳۸۹،ص ۶۳). در کشور ایران نیز همسو با تحولات جهانی، با توسعهی فناوری ه ای مربوط به ضبط و انتشار تصویر و صوت و همچنین گسترش اینترنت هر روزه شاهد سوء استفاده از این وسایل علیه حیثیت و آبرو و حریم خصوصی افراد هستیم .این فناوری، به جای آن که وسیله ی آرامش باشد، به ابزاری تبدیل شده اند که آبرو و حیثیت افراد را تهدید می کنند .فیلم های منتشر شده در اینترنت و بلوتوث تلفن ه ای همراه، دست کار ی، ذخیره و پردازش داده های شخصی، ورود به حریم خصوصی از طریق دورب ین ه ای پیشرفته دیجیتالی و ... که خصوصی ترین روابط افراد را به نمایش می کشند و حتی می توانند به فروپاشی خانواده ی قربانیان منجر شود، تهدیدی برای حریم خصوصی تمامی افراد محسوب می شوند. یک فهرست از فناوری های اطلاعات و ارتباطات که به طور بالقوه می تواند عامل

خدشه و تجاوز به حریم خصوصی باشد شاملِ شناسایی فرکانس رادیویی RFID [۱] کارت های هوشمند، قرارداد ارسال صدا در بستر اینترنت VOIP[۲] و فناوری های بی سیم می باشد. حریم خصوصی افراد در فضای مجاز ی را می توان در دو حوزه بررسی کرد:

۱- ارتباطات خصوصی یا غیر عمومی که به اشکال مختلف مکتوب، صوت، تصویر یا حتّی چند رسانه ای به صورت هم زمان یا غیر هم زمان در سراسر جهان برقرار می شوند.

۲- پایگاه های داده ای [۳] که حاوی اطلاعات شخص یاند [۴] یا حتّی اطلاعات شخصی حساس [۵] افراد را نگهداری می کنند و دسترسی به آن ها کار چندان مشکلی نیست .پس به طور کلی، می توان گفت، حریم خصوصی افراد در فضای مجازی با اجرای چهار عملیات تولید، جمع آوری، پردازش و انتقال داده ها و اطلاعات، مورد تجاوز مجرمان و تبهکاران قرار می گیرد، و بدین طریق حریم خصوصی افراد را تهدید می کنند.

۴-۲-۱- تولید و جمع آوری داده

تولید و ایجاد داده، اولین مرحله از فرایند عملیاتی داده در فضای مجازی از طریق فناوری اطلاعات و ارتباطات می باشد . در این مرحله به استفاده از سیستم ه ای مخابراتی و رایانه ای داده ها تولید می شوند؛ برای نمونه، به وسیله نرم افزارهای موجود در رایانه، میتوان فایل های متنیِ حاوی اطلاعات افراد را ایجاد نمود. در جمع آوری داده، فرد داده های آمادهای را که توسط اشخاص ایجاد شده و یا اطلاعات موجود در فضای حقیقی را جمع آوری می کند؛ برای نمونه، مجرمان، به وسیله دوربینِ فیلم برداریِ نصب شده بر روی رایانه، تصاویر خصوصی افراد را ضبط و جمع آوری می کنند، و یا نسبت به شنود اطلاعاتی اقدام می نمایند و از این طریق حریم خصوصی افراد را مورد تجاوز قرار می دهند. انسان بر حریم خصوصی خویش حقی دارد که تمام عقلاء آن را می پذیرند.

همان طور که هیچ کس نمی تواند در حقوق افراد دیگر به غیر اذن و اجا زه آنها تصرف کند، نمی تواند در حقوق خصوصی افراد نیز بدون اذن و اجازه ایشان وارد شد .این امری مسلم و حتمی بین تمام جوامع بشری است .در فضای مجازی و جامعه اطلاعاتی، نه تنها به کارگیری داده های کاذب بلکه جمع آوری و ذخیره داده های صحیح نیز می تواند عاملی جهت تجاوز به حریم خصوصی و حقوق اشخاص باشد .شاخصه ی غیر مجاز بودن چنین اعمالی می تواند هم روش های جمع آوری داده ها و هم محتوای داده ها را در بر گیرد.

۴-۲-۲ پردازش و انتقال یا تبادل داده:

---

[1]- Radio frequency identification.

[2]- Voice over Internet Protocol.

[۳] - پايگاه هاي داده اي، مراكزي هستند كه اطلاعات افراد به صورت داده و صفر و يك بر روي سرورهاي مخصوص نگهداري مي شوند .اين پايگاه ها توسط سيستم مديريت پايگاه داده اي كنترل مي شوند، سيستم نرم افزاري كه به كاربر اين اجازه را مي دهد تا اطلاعات را ذخيره سازي، بازيافت و اصلاح كند.

[4] - Personal Informations.

[5] - Sensitive Personal Informations.

در مرحله پردازش داده ها و اطلاعات نیز، حریم خصوصی افراد خدشه دار می شود. فناوری اطلاعات و ارتباطات این امکان را فراهم آورده است که مجرم از طریق داده ای کاذب، داده ها و اطلاعاتی را ایجاد نماید که به حریم خصوصی افراد لطمه وارد شود؛ برای مثال، اگر بخشی از تصویر قربانی در اختیار مجرم قرار گیرد، او می تواند با استفاده از نرم افزارهای پیشرفته آن را تبدیل به عکس مستهجن نماید، که سایت های اینترنتی صندوق های صوتی و پستی وسیله ی مناسبی برای تبلیغ، توزیع و عرضه این گونه تصاویرغیراخلاقی می باشند .بنابراین، پردازش، انتقال یا افشای اطلاعات کاذب حتّی توسط دارنده قانونی آن ها ممنوع است .این امر به دلیل عدم انعکاس واقعیت و کذب بودن، می تواند به نقض حریم خصوصی منجر شود و حیثیت فرد را خدشه دار نماید. انتقال داده ها توسط فناوری های ارتباطی و مخابراتی بسیار سریع، اما نامطمئن است و مجرمان با اضافه کردن برخی سیستم ها در مس یر تبادل اطلاعات آن را مورد سوء استفاده قرار می دهند؛ برای نمونه، ایمیل های ارسالی افراد را مورد بازبینی قرار می دهند و حریم خصوصی افراد را خدشه دار می کنند. دامنهی وسیع مرحله ی پردازش غیر مجاز از به کارگیری داده های شخصی، شامل هرگونه عملیات منطقی بر روی داده ها، تغییر، ترکیب، مقایسه و پاک کردن آن ها می شود .جرایمی هم که ناشی از نقض اصول مربوط به این مرحله است، تقریباً گسترده است .به طور منطقی می توان جرایم مرتبط با این مرحله را بدین شرح برشمرد:

۱- پردازش برای هدف نامشروع، حتی اگر تحصیل و ذخیره داده ها به صورت مشروع و قانونی انجام شده باشد.

۲- پردازش داده های شخصی بدون جلب رضایت موضوع داده ها، یا اجازه صریح قانون گذار پردازش در شرایط غیر مجاز.

۳- پردازش، با روش های غیر صادقانه و فری بآمیز جهت کسب نتیجه های خاص یا تولید و استفاده از داده های کاذب.

۴- تخریب یا تغییر داده های شخصی؛ نقض اصل شفافیت در پردازش داده ها.

۵- پردازش داده های ناشناس با روشی که موجب آشکارسازی هویت شخصی می گردد.

۶- پردازش، بیش از حد ضرورت یا غیر مرتبط با هدف اعلام شده یا موارد مجاز قانونی پردازش غیر مرتبط.این جرایم در عمل گاهی با تخلفات قبلی مانند تحصیل غیر مجاز در هم می آمیزند و موجب ارتکاب جرایم خطرناکی مثل سرقت هویت[1] می شوند.

۴-۳- مصادیق نقض حریم خصوصی در شبکه های اجتماعی:

جنبه دیگر موضوع همانطور که معروض گردید مربوط به ناقضان حریم خصوصی در فضای مجازی است. این بزهکاران زمانی که وارد فضای مجازی یا همان اینترنت می‌شوند در خیالی خام آنرا (ملک طلق) خود دانسته و اجازه هرگونه فعالیت و ورود به حریم خصوصی دیگران را به خود می‌دهند. در زیر به برخی مصادیق نقض حریم خصوصی در فضای مجازی که در قانون جرایم رایانه ای جرم انگاری شده است می‌پردازیم:

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

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

[1]- Identity theft.

-3دسترسی غیرمجازبه داده‌های سری در حال انتقال در سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده یا تحصیل و شنود آن.

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

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

۶-حذف یا تخریب یا مختل یا غیرقابل پردازش نمودن داده‌های دیگری از سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده بطور غیرمجاز.

۷-از کار انداختن یا مختل نمودن سیستم‌های رایانه‌ای یا مخابراتی بطور غیرمجاز نظیر غیرفعال سازی دیتابیس تارنماها و ممانعت از دسترسی افراد به سایتهای شخصی.

۸-ممانعت از دسترسی اشخاص مجاز به داده های یا سیستمهای رایانه ای یا مخابراتی بطور غیرمجاز.

۹-ربودن داده‌های متعلق به دیگری بطور غیرمجاز.

۱۰-هتک حیثیت از طریق انتشار صوت و فیلم تحریف شده دیگری بوسیله سیستم‌های رایانه‌ای یا مخابراتی.

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

-12فروش یا انتشار یا در دسترس قرار دادن گذرواژه یا هر داده‌ای که امکان دسترسی غیرمجاز به داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتی متعلق به دیگری را فراهم می‌کند.

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

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

۴-۴- حمایت قانون از حریم خصوصی

ویژگی های خاص فضای سایبری اقتضا می کند قانونگذار حمایت مؤثرتری از حقوق کاربر انجام دهد. علاوه بر حمایت های قانونی در قانون اساسی جمهوری اسلامی ایران و منع تعرض به آبرو و جان و مال و حقوق و مسکن و پیشه و عقائد و اطلاعات خصوصی افراد، در قانون جرائم رایانه‌ای نیز مصادیق محتوای مجرمانه در فضای مجازی مورد تاکید و مجازات‌های متفاوتی برای مخلان آن در نظر گرفته شده است. در ماده ۱ فصل اول این قانون با عنوان «جرائم علیه محرمانگی داده‌ها و سیستم‌های رایانه‌ای و مخابراتی» آمده است «هرکس به طور غیرمجاز به داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتی که به وسیله تدابیر امنیتی حفاظت شده است دسترسی یابد، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج تا بیست

میلیون ریال یا هر دو مجازات محکوم خواهد شد «.برابر ماده ۳ نیز شنود اطلاعات حبس از یک تا سه سال یا جزای نقدی از بیست تا شصت میلیون ریال یا هر دو مجازات؛ انتشار اطلاعات به صورت غیر مجاز به حبس از دو تا ده سال؛ فروش یا افشای اطلاعات به سازمان یا شرکت یا گروهی دیگر به حبس از پنج تا پانزده سال را برای خاطی به همراه دارد .اگر کسی به طور غیرمجاز داده‌های کاربر را از سیستم رایانه حذف، تخریب یا غیرقابل پردازش کرده است به حبس از شش ماه تا دو سال یا جزای نقدی از ده تا چهل میلیون ریال یا هر دو مجازات محکوم می‌شود. همچنین اعمالی مانند وارد کردن، انتقال دادن، پخش، حذف کردن، متوقف کردن، دستکاری یا تخریب داده‌های سیستم‌های رایانه‌ای حبس از شش ماه تا دو سال یا جزای نقدی از ده تا چهل میلیون ریال یا هر دو مجازات را به همراه دارد. برابر ماده ۱۰ این قانون نیز مخفی کردن داده‌ها، تغییر گذرواژه که مانع دسترسی اشخاص به داده‌های سیستم‌های رایانه‌ای خودشان می‌شود از نود و یک روز تا یک سال حبس یا جزای نقدی از پنج تا بیست میلیون ریال یا هر دو مجازات را به همراه دارد .قانون با هتک حرمت سختگیرانه‌تر برخورد کرده است و هرکس به وسیله سیستم‌های رایانه‌ای، فیلم یا صوت یا تصویر دیگری را تغییر دهد یا تحریف و آن را منتشر کند، به نحوی که عرفاً موجب هتک حیثیت او شود، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد. اگر این تغییر به صورت مستهجن باشد، مرتکب به حداکثر هر دو مجازات مقرر محکوم می‌شود. انتشار تصویر یا فیلم خصوصی یا خانوادگی یا اسرار دیگری و انجام این اعمال به قصد تشویش اذهان عمومی نیز با مجازاتی مشابه پاسخ داده می‌شود.همیشه فرصت‌ها، مخاطرات خاص خود را نیز به همراه داشته اند. کاهش ارتباطات مستقیم و رودررو و چند لایه شدن هویت افراد در فضای مجازی، امکان هر نوع سوءاستفاده را در پوشش ارتباط فراهم کرده است. رواج گسترده تر رسانه های نوین در سال های آینده و گردش عظیم اطلاعات با حداقل نظارت، موج جدیدی از تهدید و نگرانی برای امنیت کاربران ایجاد خواهد کرد که جز با سواد رسانه ای و افزایش توانمندی های فردی برای شناخت و تفکیک اطلاعات مناسب و سالم و نیز دفع متجاوزان حریم خصوصی نمی توان به مکانیسم مطمئن تری برای تعامل مفید و استفاده از ظرفیت های بالقوه این شبکه ها امیدوار بود.

۴-۵- امنیت شبکه و پیشگیری از نقض حریم خصوصی

امنیت شبکه نیز موضوع مهمی است که تأثیر بسزایی در پیشگیری از نقض حریم خصوصی دارد .با این وجود، بین گستره ی کاربردهای فناوری اطلاعات و ارتباطات و فناوری های امنیتی آن فاصله ای وجود دارد که شکاف آسیب پذیر ی نام دارد . با توجه به این که شتاب توسع هی فناوری اطلاعات و ارتباطات از امنیت فناوری اطلاعات و ارتباطات بیشتر است، لذا در طول زمان این شکاف گسترده تر می شود و تأمین امنیت شبکه هی چگاه به طور مطلق امکان پذیر نیست کاربرانی می توانند موفق تر باشند که همواره فناوری های امنیتی به روز شده را در اختیار داشته باشند و در ضمن با در نظر گرفتن ضعف های آن ها، همواره تدابیر احتیاطی را نیز لحاظ کنند. به عنوان نمونه، در برنامه ریزی ارتباط سیستم با شبکه، فقط بخش های کاملاً ضروری را با شبکه ارتباط دهند و با شیوه مطمئن و به صورت منظم از اطلاعات نسخ هی پشتیبان تهیه و در یک پایگاه داده ای مطمئن ذخیره کنند. برخی اغلب در پی دست یابی به امنیت کاملند، ولی این موضوع غیر عملی و محال است و تجربه نشان داده که امنیت صددرصد وجود ندارد .برقراری امنیت کامل بسیار گران و غیر ممکن است، زیرا نمی توان همه ضعف ها و حملات آتی را پیش بینی کرد .حتّی در محصولاتی که به دقّت طراحی شده اند نیز آسیب پذیر ی

هایی دیده می شود .هم چنین به طور پیوسته روش های جدید حمله به حریم خصوصی در حال کشف شدن است و سیاست های امنیتی اغلب پیچیده، مبهم، ناسازگار و وابسته به نظرِ نیروی انسانی است .هم چنین سازمان ها به علّت استفاده از امکانات فناوری دیگران، از عدم امنیت کامل استقبال می کنند، و فقدان زیر ساختارها ی رمزنگاری در ایران از اهمیت موضوعِ امنیت کاسته است ظهور فناوری های جدید مستلزم تولید سیستم های امنیتی متناسب با آن می باشد، این در حالی است که این کار با وقفه ای طولانی صورت می گیرد. با ایجاد امنیت شبکه از طریق دیوارهای آتشین [1]، رمزنگاری [1]، ضد ویروس و... می توان از حریم خصوصی محافظت نمود .اگر اطلاعات دربارهی افراد اَمن نباشد، این امر می تواند حریم خصوصی آنان را تهدید کند .این نوع استدلال نشان می دهد که حفظ حریم خصوصی نیازمند امنیت است .اگر اطلاعات همه افراد آشکار شود، در این صورت، تهدیدهای امنیتی بسیار راحت تر خواهد بود. حریم خصوصی و امنیت با یکدیگر هم پوشانی دارند و همدیگر را تقویت می کنند .امنیت در سطح کاربران می تواند به عنوان پیش شرط حریم خصوصی مد نظر
قرار گیرد؛ به این دلیل که نبود امنیت، منجر به دسترسی غیر مجاز به داده ها می شود، که این به نوبه خود حریم خصوصی مجازی آنان را به خطر می اندازد .حفاظت از حریم خصوصی از طریق گمنامی اجازه می دهد تا بعضی از افراد با پلیس ارتباط برقرار کنند و کمک های لازم را ارایه کنند، که اگر هویت آن ها شناخته شده بود، امکان داشت، این کار را انجام ندهند.

۵- نتیجه گیری

جامعه ی امروزی به طور فزاینده ای در جنبه ه ای آموزشی، ارتباطی، اطلاعاتی، اقتصادی و ...به فناوری اطلاعات و ارتباطات وابسته شده است .با نفوذ فناوری اطلاعات و حریم ارتباطات به محیط ه ای کاری و خانگی، نگران ی ه ای فراوانی از باب نقض به وجود آمده است .این فناوری که حاصل تلاش سال ها تحقیق و پژوهش خصوصی بشر می باشد، ذاتاً ویژگی منفی و مخرب ندارد؛ بلکه اگر انسان تحت سیطره پنهان آن قرار گیرد و سرنوشت خود را در اختیار پیشرفت این فناوری قرار دهد، خطرناک می شود .به طوری که، فضای مجازی ایجاد شده توسط فناوری اطلاعات و ارتباطات با شکستن حریم خصوصی افراد از هر قشر و ر ده ای و انتشار خصوص ی تر ین اطلاعات مربوط به افراد اعم از مکتوب، تصاویر، صدا، چند رسانه ها و... ، باعث ناآمنی روانی و اجتماعی شده است که می تواند پیامدهای جبران ناپذیری را به همراه داشته باشد .از این رو، مدیریت اطلاعات شخصی، برای کاربران، درخواست کنندگان خدمات و شرکت ه این فناوری اطلاعات و ارتباطات، به یک نیاز بسیار مهم بدل شده است . تا با استفاده از راهکارهای امنیتی و تدابیر پیشگیرانه پلیس از نقض حریم خصوصی در فرایند تولید، جمعآوری و ذخیره سازی، پردازش و تبادل اطلاعات و داده، جلوگیری نمایند. بر این اساس، امکان نقض حریم خصوصی در فرایندهای مذکور توسط اقدامات ناجا امکان پذیر است؛ اما ناجا با توجه به وظایفی که طبق قانون بر عهده دارد، بایستی از نقض حریم خصوصی پیشگیری نماید، که این اقدامات ناجا نیز در سطح گسترده، به نوبه ی خود می تواند منجر به نقض حریم خصوصی افراد در فضای مجازی گردد .از این رو، با توجه به این که حق حریم خصوصی به عنوان یک حق بشری مورد توجه و حمایت

[1] - Firewalls.

اسلام، مقررات بین المللی و قانون اساسی ایران می باشد؛ ناجا نخست بایستی مفهوم، قلمرو و چارچوب حریم خصوصی مجازی را برای مأموران خود تعریف و تبیین نماید؛ زیرا به دلیل روشن نبودن قانون و تعریف حریم خصوصی، افراد در برخورد با حریم خصوصی، به طور سلیقه ای اعمال قانون خواهند نمود؛ دوم، اجرای درست مأموریت ه ای پیشگیرانه و کشف جرم نیازمند تربیت متخصصان فن آوری اطلاعات و ارتباطات با آشنایی کامل به قوانین است، تا با رعایت جوانب احتیاط و با حکم مقام قضایی اقدام کنند و در صورت تحقق شرایط بالا پیشگیری و کشف جرم امکان پذیر خواهد بود . در غیر این صورت پیشگیری از جرم و کشف جرم، موجب نقض حریم خصوصی مجازی افراد و ایجاد چالشی بزرگ فرا روی ناجا خواهد بود .ناگفته نماند که نقش کاربران در حفظ حریم خصوصی خود و آگاهی آنان نسبت به آن بسیار مفید خواهد بود، به طوری که با ایجاد امنیت تبادل اطلاعات و عدم اتصال به سایت های غیر مجاز این امر ممکن خواهد بود.

۶- منابع و مآخذ

۱-آقابابایی، حسین،۱۳۸۹، قلمرو امنیت در حقوق کیفری، چاپ اول،تهران،انتشارات پژوهشگاه فرهنگ و اندیشه اسلامی.

۲-باستانی، برومند،۱۳۸۳،جرائم کامپیوتری و اینترنتی، تهران ،انتشارات بهنامی.

۳-جاوید نیا، جواد،۱۳۸۷، جرایم تجارت الکترونیکی، چاپ اول، تهران، انتشارات خرسندی.

۴-جعفری، عباس،۱۳۸۵، بررسی حق حریم خصوصی ،مجله ی تعالی حقوق، شماره ی1 .

۵-جلالی فراهانی، امیر حسین،۱۳۸۴، پیشگیری وضعی از جرائم مجازی در پرتو موازین حقوق بشر، مجله ی حقوقیِ فقه و حقوق، شماره6 .

۶-حسن بیگی ، ابراهیم،۱۳۸۴، حقوق و امنیت در فضای سایبر» تهران ،انتشارات ، مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار.

۷-حسن بیگی، ابراهیم، ۱۳۸۴، حقوق و اینترنت در فضای سایبر، چاپ اول، تهران ، انتشارات مؤسسه فرهنگی مطالعات و تحقیقات بین المللی ابرار معاصر.

۸-حسنی، جعفر، ۱۳۸۵، حمایت کیفری از حریم خصوصی در فضای سایبر، پایان نامه ی کارشناسی ارشد حقوق جزا و جرم شناسی، دانشکده حقوق، دانشگاه شهید بهشتی.

۹-رحم دل، منصور،۱۳۸۴،حق انسان بر حریم خصوصی، مجله ی حقوقیِ دانشکده حقوق و علوم سیاسی دانشگاه تهران، شماره 70.

۱۰-زیبر، اولریش،۱۳۸۴، جرایم رایانه ای، ترجمه ی محمدعلی نوری -رضا نخجوانی -مصطفی بختیاروند -احمد رحیمی مقدم، تهران،انتشارات گنج دانش.

---

[1] - رمزنگاري عملي است كه براي حفظ محرمانگي اطلاعات به كار گرفته م ي شود . در اين روش اطلاعات كد مي شود يا به عبارتي اطلاعات، به اطلاعاتي نامفهوم تبديل م ي شود و در مقصد بعد از دريافت اطلاعات، كد آن شكسته مي شود تا به اطلاعات با معني و همانند قبل، تبديل شود.

۱۱-نمک دوست، حسن، ۱۳۸۵، اخلاق حرفه ای، حریم خصوصی و حق دسترسی به اطلاعات، مجله ی اطلاع رسانی و کتابداری، شماره66 .