نقد و برررسی شنود غیرمجاز در فضای سایبری

پریوش خلجی[1] دکتر محمود مالمیر[2] دکتر راضیه قاسمی[3]

تاریخ دریافت: ۹۹/۱۰/۰۳

تاریخ پذیرش:۹۹/۱۱/۲۵

چکیده

بحث فناوری اطلاعات و ارتباطات نوین ، که تجلی روشن آن فضای سایبر است مسأله جدیدی را با عنوان جرایم رایانه ای پیش روی قانون گذار قرار داده است که یکی از مصداق های آن بزه شنود غیر مجاز است. منظور از شنود اطلاع یافتن عمدی از محتوای در حال انتقال و ذخیره شده در سامانه های مختلف رایانه ای، مخابراتی، الکترومغناطیسی و نوری و در یک کلام الکترونیکی است. دسترسی به اطلاعات فردی، بازرگانی، تجاری و برهم ریختن امنیت اطلاعات از بدو تحول در تکنولوژی ارتباطات نگرانی هایی را پدید آورد. از این رو نیاز به داشتن قانونی خاص، در برخورد با مجرمان خفتهٔ سایبر بیشتر احساس شد. روش تحقیق در این طرح (تحلیلی/ توصیفی) و همچنین روش گردآوری مطالب به صورت کتابخانه ای می باشد و قلمرو این تحقیق را آخرین اطلاعات ثبت شده در کتاب‌ها، مقاله‌ها و مجلات تشکیل می دهد. در واقع هدف آگاهی نداشتن جامعه در مورد یکسری از جرم‌ها که به ظاهر ممکن است نوعی جرم به شمار نیایند و قابل لمس نباشند، بوده و آنچه در این زمینه باید به کار گرفته شود؛ افزایش آگاهی عمومی، ایجاد امنیت اطلاعاتی و اعمال شیوه های نظارتی از سوی نهاد های مسئول است.

کلید واژگان : فضای مجازی، شنود غیرمجاز، داده، جرم.

---

[1] دانشجوی کارشناسی ارشد حقوق- گرایش جزا و جرم شناسی

[2] دکتری حقوق علوم سیاسی

[3] عضو هیئت علمی دانشگاه شهید اشرفی اصفهانی در رشته حقوق

مقدمه :

در نیمه دوم قرن بیستم انقلابی دیگر رخ داد که به انقلاب اطلاعاتی موسوم است . هنگامی که تاریخ نگاران آینده ، نیمهٔ دوم قرن بیستم را مورد بررسی قرار می دهند ، در واقع به بازنگری انقلاب اطلاعاتی خواهند پرداخت ، بشر در ۵۰ سال گذشته از هر دوره دیگر ، تاریخ بیشتری داشته است یکی از دلایل این پیشرفت سریع تکنوژی ، کامپیوتر است (خبرنامه شورای عالی انفورماتیک ، ۱۳۷٦ ، ۲۰).

پیشرفت های جهانی رایانه های شخصی و تجاری ، افزایش قابلیت های ذخیره سازی و پردازش داده ها ، ادغام پردازش داده ها با فناوری های جدید ارتباطی اطلاعاتی همگی بیانگر تحول فعلی هستند که اغلب از آن به عنوان ورود به عصر اطلاعات یاد می شود . (زیبر ، ۱۳۸۳ ، ۱۷). بی تردید ، این دنیای نوین و گره گشا ، روی دیگری هم دارد که تیره و تار است . بزهکاران فضای سایبر آمادهٔ انجام تهدید های نوین و بی سر و صدا بر علیه رایانه و شبکه های رایانه ای می باشند . متأسفانه ، سرعت و شتاب موجود در رایانه ای نمودن حجم فراوان اطلاعات و استفاده از شبکه ، فرصت کافی برای توسعهٔ سیستم های دفاعی در مقابل هجوم و پیشگیری از آن را به ما نداده است (جی . آیکاو و همکاران ، ۱۳۸۳، ۲٤).

روند رو به رشد جرایم کامپیوتری موجب بروز چالش ها و تنش های گوناگونی در جوامع مدرن امروزی از جمله جوامع حقوقی گردیده است . جرایم از یک طرف می تواند شامل فعالیت های مجرمانه ای باشد که ماهیتی سنتی دارند مانند سرقت ، کلاهبرداری ، جعل و سوء استفاده مالی و یا اینکه ماهیتی کاملاً نوین و غیر قابل پیش بینی که توانسته است حقوق جزاء کلاسیک و آیین دادرسی را کاملاً به چالش انداخته و متحول نماید. (باستانی ،۱۳۸۳، ۱۳)

از جمله آن اعمالی که مورد مذمت ادیان الهی و اخلاق عمومی جوامع بوده ، ورود به اسرار مردم است که متأسفانه با گسترش عرصه فناوری اطلاعات و ارتباطات آفت های این پدیده شگرف نیز از پیچیدگی های خود برخوردار است . یکی از اشکال تجسس در امور شخصی مردم شنود غیر مجاز است که در کنار سایر جرایم مرتبط با فناوری ارتباطات توجه جوامع بین المللی و نیز حقوق داخلی کشورها را به خود معطوف داشته است . در کشور ما موضوع شنود غیرمجاز به طور پراکنده در برخی قوانین و در محدوده های خاص پیش بینی شده و بر لزوم شنود قانونی نیز توجه هایی صورت گرفته است اما در بسیاری از موارد نیز خلأ قانونی وجود دارد . در قانون جرایم رایانه ای که مهمترین قانون داخلی در این زمینه به شمار می آید ، به شنود غیرمجاز به عنوان یک جرم مستقل بدون توجه به فرد یا افراد خاص و با

در نظر گرفتن آن در محدوده تمامی مصادیق فناوری ارتباطات و اطلاعات اعم از رایانه ، مخابرات ، امواج الکترونیکی و نوری پرداخته شده و بحث شنود مجاز نیز مورد توجه قرار گرفته است.(امانی ، ۱۳۸۹ ، ٤)

چالش بین قوانین حقوقی و عملیات رایانه ای ، اساساً مانند سایر فناوری های روز می باشد . برای حفظ تعادل بین نیازهای جامعه و حقوق انفرادی اشخاص و حفظ امنیت جامعه ، قوانین حقوقی باید روش های جدیدی را که بررسی و مقابله با رفتار مجرمانه را مجاز می شمارد ، گسترش دهد . این روش ها بدون تردید ، روش های نوین ارتباطات هشدار دهنده و جست و جو در مجموعه عظیم داده ها را نیز شامل می شود . در عین حال ، قوانین حقوقی باید کمک کند تا از نادیده گرفتن حقوق اساسی و اولیه اشخاص ، شامل حفظ اسرار فردی آنان ، حق آزادی بیان و حق انتشار اطلاعاتشان ، جلوگیری شود . بنابراین باید پیش از پیش آمادگی حل این مشکلات را داشته باشیم زمان کمی برای هدر رفتن مانده است ، راهزنان در بزرگراه عظیم اطلاعات ، در کمین نشسته اند(جی . آیکاو و همکاران ،۱۳۸۳ ، ۲٦).

بیان مسأله :

انسان در مسیر پر فراز و نشیب زندگی خود شاهد تحولات و دگرگونی های زیادی است و عوامل مختلفی ممکن است در به وجود آمدن آن نقش داشته باشد که یکی از آنها پیشرفت های حاصل در عرصه های مختلف علوم و فناوری است اگرچه موجب ارتقای سطح زندگی و آسایش بشر است اما همین پیشرفت های سودمند می تواند مورد استفاده سوء قرار بگیرد امروزه در عصر رایانه و اینترنت پیشرفت های تکنیکی موجب پیدایش اشکال متنوع و جدید مجرمیت شده است که فرصت تازه ای برای قانون شکنی در اختیار مجرمان می گذارد . (حسینی خواه و رحمتی ، ۱۳۸۹ ، ١٤)

همچنین ارتقای تکنولوژی ، علم و دستیابی بشر به فناوری اطلاعات و استفاده از رایانه و پیدایش دنیای مجازی دارای پیامدهای مثبت و منفی فراوانی برای بشر بوده که از جمله پیامدهای منفی آن پیدایش جرایم رایانه ای بوده که اینگونه بیان شده : آن دسته از جرایم ، که با سوء استفاده از یک سیستم رایانه ای بر خلاف قانون ارتکاب می یابد . البته این دسته از جرایم را می توان شامل جرایم سنتی که به واسطه رایانه صورت می گیرد مانند سرقت ، کلاهبرداری و دسته جرایم نوظهور که با تولد رایانه پا به عرصه حیات گذاشته اند مانند ؛ جرایم علیه صحت و تمامیت داده ها و شنود غیرمجاز ، دانست.(طارمی ، ۱۳۸۷ ، ۸۸)

از جمله اعمالی که همیشه مورد مذمت واقع می شود ورود به اسرار مردم است که متأسفانه با

گسترش عرصه فناوری اطلاعات و ارتباطات آفت های این پدیده شگرف نیز از پیچیدگی های خود برخوردار شده است و افرادی که از رایانه برای این هدف یاری می گیرند مصداق این جمله اند ،دزد چون با چراغ آید گزیده تر برد کالا . (جی . آیکاو و همکاران ، ۱۳۸۳ ، ۱۵)

شنود عبارت است از عملیات غیرقانونی که با روش های فنی در ارتباط بین سیستم ها و یا شبکه های رایانه ای صورت می گیرد . شنود می تواند شامل هر نوع ارتباط رایانه ای شود و اغلب مربوط به انتقال اطلاعات از طریق سیستم های ارتباط راه دور شخصی یا عمومی می باشد که می تواند در یک سیستم منفرد یا بین دو سیستم انجام پذیرد همچنین شنود و دسترسی به محتوای در حال انتقال و ذخیره شده شامل مکالمات ، پیامک های نوشتاری و ارتباط از طریق اینترنت می باشد که این اطلاع یافتن عمدی از محتوا می تواند در سامانه های مختلف رایانه ای ، مخابراتی ، الکترومغناطیسی و نوری و در یک کلام الکترونیکی باشد (حسینی خواه و رحمتی ، ۱۳۸۹، ۷۷).

پس تلاش بر آن داریم که با آشنایی با این بزه و بیان راه های پیشگیری از به وجود آمدن خسارات مادی و معنوی جلوگیری نماییم تا کاربران با آسایش و امنیت مضاعفتری از پیشرفت های تکنولوژی بهره برند . این تحقیق به دنبال شناخت و یاری رساندن به قربانیان و بزه دیدگان فضای جدید و غیر ملموسی است که قربانیان آن ممکن است هیچگاه شناخته نشوند و جانیان و بزهکاران از این فناوری نوین با خیال آسوده تری برای شکار قربانیان بهره برند و با توجه به ورود فضای سایبری به تمام عرصه های زندگی افراد از موضوعات علمی گرفته تا کار و سرگرمی و اقتصاد و ارتباطات ، در صورتی که مهاجم بتواند دستیابی به اطلاعات سری افراد پیدا کند می تواند مورد استفاده سوء قرار دهد . دستیابی به این اطلاعات ممکن است از تخریب بنیان یک خانواده تا بر هم زدن امنیت یک کشور باشد . پس باید با شناخت و آشنایی کافی با این بزه بستری فراهم کرد تا راه بر جنایتکاران خفته این فضا بسته شود . با توجه به بیان مطالب مذکور باید اقدامات پیشگیرانه در دستور کار قرار گیرد .

سؤالات تحقیق :

۱. آیا تحصیل یک داده ملازمه با دسترسی غیرمجاز دارد؟

۲. آیا فضای سایبری عاملی برای شنود اطلاعات محرمانه محسوب می شود؟

۳ .آیا دسترسی غیرمجاز می تواند عامل تسهیل کننده در وقوع سایر جرایم رایانه ای محسوب شود؟

فرضیات تحقیق :

۱ .تحصیل داده یا هر نوع اطلاعات ، مرحله ای بعد از دسترسی غیرمجاز می باشد .

۲ . فضای سایبری می تواند به عنوان یک مکانیسم برای جرایم خاص و دسترسی بـه داده در سـامانه هـای مختلف محسوب شود .

۳ . در برخی موارد دسترسی غیرمجاز عامل تسهیل کننده در وقوع سایر جریم رایانه ای محسوب می شود.

روش تحقیق :

روش تحقیق به صورت توصیفی/ تحلیلی است و به معرفی و بیان ابعاد مختلف موضوع اصلی تحقیق می پردازد و روش گردآوری مطالب به صورت کتابخانه ای بوده و برای تطبیق مطالب از کتـب مختلـف و تحقیقات بنیادین گذشتگان و ترجمه متون و کتاب های مرتبط استفاده شده است.

ساماندهی (طرح) تحقیق :

این تحقیق به بررسی اقداماتی که در فضای سایبر به قصد دسترسی و شنود اطلاعات محرمانه صورت می گیرد می پردازد و از دو فصل کلی تشکیل شده است . فصل اول که شامل کلیات می باشد در خصوص تبیین فضای سایبری و ویژگی های خاص آن ، کلیات بحث شنود و بررسی مواد قانونی موجود و همچنین تفاوت شنود غیرمجاز با استراق سمع و بررسی جرایم رایانه ای که شنود غیرمجاز یکـی از عناصـر آن مـی باشد می پردازد ، سپس فصل دوم شنودهای غیرمجاز فضای سایبر در حقوق کیفری ایران را مورد بررسـی قرار می دهد ، این فصل به سه بخش با عناوین ، تعـاریف و عناصـر شـنود غیرمجـاز و تجـاوز بـه حـریم خصوصی ، ارکان تشکیل دهنده این بزه و پیشگیری از شنود با متدولوژی امنیت تقسیم می شود.

تعاریف و عناصر شنود غیرمجاز در فضای سایبر

شنود، گرچه این واژه بدون قرینه لفظی یا معنوی ، دلالت بر استماع مکالمه به صـورت حضـوری یـا پنهانی نمی کند، ولی در برخی از عرف های خاص بدون قرینه هم بر استماع مکالمه به طور پنهان بـه کـار رفته است. از این رو به کار بردن این واژه بر استماع پنهانی در صورتی صحیح است کـه قرینـه ای وجـود داشته باشد. (ترکی ، ۱۳۸۸ ، ۱۵)

قانون جرایم رایانه‌ای که با الهام از کنوانسیون جرایم سایبری و نیز کد جرایم اینترپل به تصویب رسیده و سعی شده است ویژگی های فرهنگی کشورمان نیز در آن لحاظ شود ، در سه مورد به بحث شنود پرداخته است . در بخش یکم که اختصاص به جرایم و مجازات ها دارد ، فصل یکم جرایم علیه محرمانگی داده ها و سامانه های رایانه‌ای و مخابراتی را مورد اشاره قرار داده و مبحث دوم آن که مشتمل بر ماده ۲ است ، به شنود غیرمجاز اختصاص داده شده است . این ماده مقرر می دارد :

A هرکس به طور غیرمجاز محتوای در حال انتقال ارتباطات غیرعمومی در سامانه های رایانه‌ای یا مخابراتی یا امواج الکترومغناطیسی یا نوری را شنود کند ، به حبس از شش ماه تا دو سال یا جزای نقدی از ده میلیون ریال تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد ≅ .

علاوه بر ماده ۲ در مبحث سوم از فصل یکم همان بخش و در زیر مجموعه جرایم علیه محرمانگی داده ها تحت عنوان « جاسوسی رایانه‌ای » بند (الف) ماده ۳ همان قانون به شنود محتوای سری در حال انتقال پرداخته است که به لحاظ طبقه بندی بودن محتوا و سری بودن آن عنوان جاسوسی رایانه‌ای پیدا می‌نماید . به موجب این بند شنود محتوای سری در حال انتقال یا ذخیره شده در سامانه های رایانه‌ای یا مخابراتی یا حامل های داده مستلزم تحمل حبس از یک تا سه سال یا جزای نقدی از بیست میلیون تا شصت میلیون ریال یا هر دو مجازات می باشد . در مبحث پنجم از فصل دوم قانون مذکور ماده ٤٨ به شنود مجاز و تبصرهٔ آن مربوط به دسترسی به محتوای ارتباطات غیرعمومی ذخیره شده است . (امانی ، ۱۳۸۹ ، ۵)

شنود غیرمجاز همچون دسترسی غیرمجاز ناشی از عدم رضایت دارنده واقعی یا قانونی داده یا محتوای در حال انتقال می باشد . همچنین شرط غیرقانونی بودن نیز به شرط رضایت اضافه می شود این جرم در واقع همان تعرض به حریم ارتباطات به وسیله شنود سنتی و ضبط مکالمات تلفنی افراد خواهد بود که به گونه ای دیگر بیان می شود . (جلالی فراهانی ، ۱۳۸۹ ، ۲۸)

مبحث اول : تجاوز به حریم خصوصی با دسترسی و شنود غیرمجاز

انسان جامعه جوست و همواره خواسته است در میان گروهی از هم نوعان خود زندگی کند و با همکاری آنان خواسته ها و نیازهای خود را برآورد . خواسته های آدمیان به حکم فطرت با هم شباهت زیادی دارند و همه می‌خواهند در رابطه با دیگران کمتر زیان ببینند و هرچه بیشتر سود ببرند پس طبیعی

است که نزاع و خصومت برای جلب منافع بیشتر و تأمین زندگی بهتر درگیرد .

لذا تن به قرارداد اجتماعی می دهند و از جمله موارد آن لزوم حمایت دولت از حقوق و آزادی های افراد است و انسان برای تأمین آزادی های فردی و آسایش خود ، رعایت حریم خصوصی خود را ضروری می داند ، او نمی‌خواهد زیر نظر باشد یا اطلاعات و اسرارش مورد تعرض واقع شود . حق حریم خصوصی حقی است که دولت و دیگر اشخاص را از مداخله و تعرض به حریم خصوصی شخص باز می‌دارد ، هم به واسطه اصول اخلاقی و هم از طریق حکم قانون .

Aحریم خصوصی≅ به عنوان یک ارزش اجتماعی و حق قانونی ، طیف گسترده‌ای از حقوق مربوط به استقلال شخصی را ؛ که به عنوان Aحق به حال خود گذاشتن≅ یا Aعدم مداخله در امور خصوصی دیگران≅ شناخته شده است ، را شامل می شود . اصول حریم خصوصی ، تاریخی طولانی دارد و با وصف تهدیدهای روز افزون فناوری های نوین به رشد و تکامل خود ادامه داده است .

از اواسط دهه ۱۹۷۰ موضوع حمایت از اطلاعات خصوصی ، بر محور رشد و توسعه فناوری رایانه‌ای ، از دغدغه های مهم مربوط به شبکه های اطلاع رسانی جهانی است .

با ورود به عصر فناوری اطلاعات به تدریج مسایل و دشواری های نوینی در ارتباط با حریم خصوصی اشخاص مطرح شده است که از مصادیق آن می توان به شنود و دستیابی اطلاعات شخصی و محرمانه افراد نام برد . (انصاری ، ۱۳۸۱ ، ١٤)

حقوق حمایت از داده ها همانا حمایت از حریم خصوصی در گستره الکترونیکی است وجهت نیل به این منظور نیازمند وضع قوانینی فراگیر در این زمینه هستیم . تا اینجا دانستیم که انسان به حکم طبیعت و سرشت باید دارای حریم خصوصی برای خود باشد و از آن باید در مقابل اشخاص محافظت نماید و بایستی نسبت به صیانت و رعایت حریم خصوصی سایرین نیز اقدام نماید . نقض حریم خصوصی در فضای مجازی یکی از مهمترین مسائل روز جامعه ماست . که از یک سو با پیشرفت روز افزون تکنولوژی و از سوی دیگر استفاده گسترده افراد از دنیای مجازی اطلاعات شخصی افراد ، که به عنوان حریم خصوصی آنان شناخته می شود در معرض خطر جدی قرار گرفته است . در این مبحث به تعریف حریم خصوصی و حوزه های این حریم اشاره خواهیم نمود .

گفتار اول : تعریف و تبیین حریم خصوصی

منظور از حریم خصوصی ، قلمرویی از زندگی اشخاص است که به هیچ وجه مایل نیستند دیگران بدون اجازه آنها وارد این قلمرو شوند یا از آن آگاهی پیدا کنند . به دیگر سخن ، آن بخش از زندگی اشخاص که آگاهی دیگران از آن به لحاظ کمیت و کیفیت در اختیار خود اشخاص می باشد حریم خصوصی نام دارد . (انصاری ، ۱۳۸۱ ، ۳۹)

حریم خصوصی مفهومی است ، زادهٔ نوگرایی و تجدید نظر در روابط انسانی از یک طرف و مقاومت در برابر پیشرفت های روز به روز تکنولوژی از طرف دیگر .

حریم خصوصی یکی از مصادیق آزادی های عمومی می باشد .A آزادی در زندگی و خصوصی یعنی مصون بودن شخص از دخالت دیگران در امور خانوادگی و کاری و نیز مصون بودن از تفتیش و تجسس دربارهٔ وضع جسمانی و احوال شخصی و سایر امور او≅ . استراق سمع گفتگوهای خصوصی فرد و ثبت آن به وسیله ضبط صوت و غیره و یا گرفتن عکس شخص و یا مونتاژ آن بدون اجازه او و انتشار آن ، مداخله در زندگی خصوصی فرد است که عرفاً ، شرعاً و قانوناً ممنوع اعلام شده است .

در کنگره حقوقدانان که در ۱۹۷۷ در استکهلم منعقد شده کنگره احترام زندگی خصوصی را برای سعادت بشر لازم می شمارد و از آنان تعریف جامعی بدست می دهد که حائز اهمیت است . در قطعنامه های این کنگره چنین آمده است :

حق زندگی حق فرد است ، که زندگی بکند همانطور که قصد دارد و حمایت بشود در مقابل :

الف – هرگونه مداخله در زندگی خصوصی خانوادگی و داخلی او .

ب – هرگونه تعرض به سلامت جسمی یا روحی و به آزادی اخلاقی یا مصنوعی او .

ج – هرگونه تعرض به شرافت و شهرت او .

د – هرگونه تفسیر مضری که از گفته ها و اعمال او بشود .

ه – افشای بی موقع امور ناراحت کننده مربوط به زندگی خصوصی او .

و – استفاده از اسم او ، هویت و عکس او .

ح – هرگونه فعالیت به منظور جاسوسی کردن دربارهٔ او .

ط – توقیف مکاتبات او .

ی – استفاده با سوء نیت از مخابرات کتبی یا شفاهی او .

ک ـ افشای اطلاعاتی که او داده یا گرفته برخلاف قاعده حفظ اسرار مربوط به شغل و حرفه شخص.
(یزدانی ، ۱۳۸۹ ، ٦٨)

حریم خصوصی افراد در ارتباطات اینترنتی و در فضای سایبر به ویژه از طریق شنود اطلاعات شخصی آنها در اینترنت نقض می شود . همچنین دسترسی غیرمجاز سایرین از طریق ارتباط اینترنتی به اطلاعات شخصی افراد مصداق دیگر نقض حریم خصوصی از طریق شبکه مذکور می باشد . فردی که به اطلاعات خصوصی دیگری نظیر نامه های شخصی ، فیلم ها یا عکس های خانوادگی دسترسی پیدا کرده است آنها را در اینترنت در دسترس عموم قرار می دهد . در این فرض ، عمل فرد مذکور همانند انتشار همان اطلاعات در یک روزنامه و تابع احکام آن است(انصاری ، ۱۳۸۱ ، ٤١).

لیکن در مجموع می توان بیان نمود :

حریم خصوصی یعنی A فرد آزادانه حق داشته باشد در خلوت خود اطلاعات مربوط به امور زندگی‌اش را پنهان نموده و بر آن کنترل داشته و مانع دسترسی دیگران به این اطلاعات گردد و تصمیم بگیرد که چه وقت و تا چه حد این اطلاعات را به دیگران منتقل نماید .

گفتار دوم : حوزه های گوناگون حریم خصوصی

حریم خصوصی نیز مانند سایر موارد دارای حوزه های گوناگونی است که هر حوزه به طور جداگانه و از دریچه و دیدگاه خود به این منظر می نگرد . حریم خصوصی را می توان در سه حوزهٔ مجزا ولی مرتبط مورد بررسی قرار داد ، که عبارتند از :

۱ . حریم خصوصی ارضی :

این حوزه از حریم خصوصی در برگیرنده یکی از ابتدایی ترین و سنتی ترین اشکال حق افراد بر لزوم محترم و مصون بودن از تعرض منازل مسکونی است . در باب حریم خصوصی اشخاص در منزل و اماکن تحت تصرف آنها ، اختلاف نظر قابل توجه میان اهل فن به چشم نمی خورد . این حق ریشه در حقوق اساسی افراد و همچنین حقوق بشر دارد و از فروع اصل کلی آزادی افراد در انتخاب مسکن و مصونیت از هرگونه تعرض است . مبنای این حق آن است که مسکن افراد و به تبع آن سایر اماکن مشابه نهان ترین نهان خانه ایشان بوده و اگر حقی برای افراد دایر بر پوشیده نگاه داشتن ابعاد شخصی و اسرار خود ، به رسمیت شناخته شده است (که چنین نیز هست) هیچ مکانی مناسب تر از مسکن برای اعمال این حق وجود ندارد البته این حق نیز همچون همه اشکال حق ، تنها به عنوان اصل ، پذیرفته شده است .

و نفوذ و اعتبار آن منافاتی با اعمال پاره‌ای استثناهای خاص و قانونی ندارد . از جمله این استثناها می توان به امکان تفتیش و بازرسی از قبیل اجرای حکم مقام صلاحیتدار و قضایی ، بازدید محل برای مسائل مالیاتی و عوارض قانونی و یا بهداشت محیط کار و مواردی چون جرم مشهود و امثال آن اشاره کرد . در خصوص وضعیت داخلی در این باب باید خاطر نشان کرد که هرچند قانون جامع و خاص در این حوزه تاکنون به تصویب نرسیده است لیکن از یکسو پاره‌ای آموزه های دینی بر این حق در جامعه ما بدیهی تلقی شده و اجرا می گردد و از سوی دیگر برخی متون قانونی به صورت کلی و گذرا برخی ابعاد این حق را مورد حمایت قرار داده‌اند از آن جمله می توان به اصل ۲۲ قانون اساسی و مادهٔ ۱۰٤ قانون آیین دادرسی دادگاه های عمومی و انقلاب در امور کیفری مصوب ۱۳۷۸ و همچنین مقررات قانون مجازات اسلامی در باب هتک حرمت منازل و املاک غیر مصوب ۱۳۷۵ اشاره نمود ، اصل مصونیت این اماکن از هرگونه تعرض با قید برخی استثنائات مقرر شده است . به نظر می رسد تدوین قانون جامع حمایت از حریم خصوصی اشخاص در منازل و اماکن خصوصی ضرورتی انکار ناپذیر است (نوری و نخجوانی ، ۱۳۸۳ ، ۳۲). که در فصل گذشته به طور مفصل به تفسیر مواد قانونی مذکور در این زمینه پرداختیم .

۲ . حریم خصوصی اطلاعاتی :

این حوزه از مباحث مربوط به حریم خصوصی که در برخی نظام های حقوقی تحت عنوان حمایت داده ها مورد بررسی قرار می گیرد در برگیرنده قواعد حاکم بر پردازش داده ها و اطلاعات مربوطه به اشخاص است . منظور از پردازش ، هرگونه تحصیل ، نگهداری ، سازماندهی ، ذخیره، هک و اصلاح ، افشاء ، انتقال ، انتشار و اقدامات مشابه در خصوص داده ها است . با این تعاریف روشن می‌شود که برخلاف تصور رایج اصل مباحث این حوزه فی نفسه ارتباطی به ظهور فناوری‌های اطلاعاتی و ارتباطی نداشته و پیش تر نیز امکان نقض این حق به صورت بالقوه و حتی بالفعل وجود داشته است ، لیکن پیدایش این فناوری ها موجب تسهیل و ترویج این قبیل اعمال در مقیاسی فوق تصور ، صورت گردید . و از همین رو جامعه امروز بیش از پیش نگران سوء استفاده های احتمالی از اطلاعات خصوصی اشخاص است .

همچنین باید دانست که منظور از اطلاعات خصوصی در این مبحث لزوماً اطلاعات سری دارای ماهیت محرمانه نیست بلکه هرگونه اطلاعات مربوط به اشخاص از جمله اطلاعات مربوط به علایق سلایق و اطلاعات مربوط به منابع مالی و اطلاعات مربوط به نیازهای شخصی ، اعتقادات ، خصوصیات فردی وابستگی های قومی ، نژادی ، هویت فرهنگی و به طور کلی هر قسم اطلاعاتی که بالقوه قابل استناد به

ضرر شخص موضوع اطلاعات یا حداقل بهبود اشخاص دیگر باشند را شامل می شود.(ایمانی،۱۳۸۲، ۸۲)

۳ . حریم خصوصی ارتباطاتی :

این جنبه از حریم خصوصی در برگیرنده حق اشخاص در امنیت و محرمانه باقی ماندن محتوای کلیه اشکال و صور مراسلات و مخابرات متعلق به ایشان است . این شق از حریم خصوصی به لحاظ قدمت و سابقه نسبی پست و مخابرات ، پذیرش و تداول بیشتری نسبت به مبحث مربوط به حریم خصوصی اطلاعات دارد . البته امروزه این حق با ظهور اشکال جدید مراسلات همچون پست الکترونیکی و ارتباطات ماهواره ای ، ارتباطات رایانه ای ، تلفن های بی‌سیم و امثال آن با مسائل جدیدتری روبرو شده و توسعهٔ مضاعف یافته است . از جمله مباحث قابل طرح ذیل این عنوان علاوه بر مصون بودن نامه ها و بسته های پستی از تفتیش و بازرسی ، امنیت و مصونیت مکالمات تلفنی از شنود ، محرمانه بودن قبوض و صورت حساب تلفن اشخاص که نشانگر فهرست تماس‌های آنهاست امنیت مراسلات داخل شبکه دیجیتالی از جمله اینترنت و شبکه های اینترنتی ، همچنین درج یا عدم درج نام شخص و شماره تلفن متعلق به او در دفترچه های راهنمای تلفن ، تماس های تلفنی ایمیل های ناخواسته و مزاحم هستند (ایمانی،۱۳۸۲ ، ۸۳).

امروزه به مدد فناوری ها ، مؤسسات عظیم تجاری و تولیدی می توانند اطلاعات فوق العاده ارزشمندی در خصوص سلایق مصرف کنندگان در نقاط مختلف دهکده جهانی و نیازهای بازار به دست آورند . اقتصاد و تجارت نوین در مفهوم امروزین آن بدون چنین اطلاعاتی قادر به حفظ عرصه‌های رقابتی نیست . به عنوان مثال از جمله ابزارهای مورد استفاده برای نیل به این اهداف A طعمه های اینترنتی≅ هستند . این مفهوم به آن معنا است که عرضه کنندگان خدمات اینترنتی یا اداره کنندگان یک سایت اینترنتی اطلاعات مختصری را از کاربر به هنگام عرضه خدماتی همچون استفاده از مطالب مندرج در سایت مطالعه می کنند . جمع آوری این اطلاعات به دارنده‌ی آن این امکان را می دهد که در قبال عرضه آنها به موسسات تجاری ذینفع (این نفع ممکن است ارسال پیام بازرگانی ناخواسته برای شخص ذیربط با در نظر گرفتن علایق ، سلایق و خصوصیات شخصی او باشد) مبالغ گزافی درآمد کسب نمایند .

امروزه این مبحث مطرح شده که گردآوری و عرضه این قبیل اطلاعات شخصی بدون اخذ رضایت شخص ذیربط ممنوع است و نقض این فن مسئولیت قانونی به دنبال خواهد داشت . در رابطه با وضعیت این شق از حریم خصوصی در حقوق داخلی علی رغم آنکه مقررات جامعی در این خصوص به ویژه در عرصه ارتباطات الکترونیکی و اینترنتی در حقوق ایران وجود ندارد ، لیکن اصل این حق ، به ویژه در باب

محرمانگی مراسلات پستی و همچنین مکالمات تلفنی مهم در اصل ۲۵ قانون اساسی و هم در ماده ۱۰۴ قانون آیین دادرسی دادگاه های عمومی و انقلاب در امور کیفری مورد تصریح قرار گرفته است . با این همه ، همچون سایر شقوق مورد بررسی ، تدوین قانون جامعی در این حوزه که به ویژه پاسخگوی چالش های حقوقی ناشی از ظهور فناوری های نوین باشد ضرورتی انکار ناپذیر است . (ایمانی ، ۱۳۸۲ ، ۸۴)

که این ضرورت عاملی شد در نگارش قانون جرایم رایانه ای که به تمامی موارد ذکر شده به طور اختصاصی پرداخته و آنها را مورد بررسی قرار داده و نگاه خاصی به حریم خصوصی افراد در فضای مجازی کرده است .

گفتار سوم : مصادیق نقض حریم خصوصی در فضای مجازی

نقض حریم خصوصی در فضای مجازی یکی از مهمترین مسائل روز جامعه ماست که از دو منظر قابل بررسی است یکی از جانب قربانیان نقض حریم خصوصی در فضای مجازی و دیگری از سوی ناقضین حریم خصوصی در فضای مجازی . بزه دیدگان در فضای مجازی نقش مهمی را در بروز جرایم ناقض حریم خصوصی ایفا می کنند و در عین حال می توانند در اقدامات پیشگیرانه علیه جرایم سایبری یا همان (cyber prevention) نقش آفرین باشند . بسیاری از بزه دیدگان جرایم سایبری و کسانی که حریم خصوصی آنان در فضای مجازی نقض می گردد ، استعدادی قابل توجه برای قربانی شدن[1] بروز می دهند و به راحتی طعمه بزهکاران سایبری می شوند بعضی کلاهبرداری های اینترنتی ناشی از کسب اطلاعات به روش های بسیار ساده و سوء استفاده از عکس ها و اسرار شخصی نمونه هایی از این موضوع می باشد .

اشخاص بایستی نسبت به صیانت از حریم خصوصی خود همت نمایند ، بسیاری اشخاص بدون رعایت مسائل امنیتی ، خصوصی ترین اطلاعات خود را بر روی سیستم رایانه‌ای و یا حامل های داده نظیر فلش و کارت های حافظه و تلفن همراه و سی‌دی ذخیره می نمایند و به نوعی دست بزهکار سایبری را در تعرض به حریم خصوصی باز می‌گذارند و این چنین استعداد قربانی شدن در فضای مجازی را از خود نشان می‌دهند . 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 می شوند در خیالی خام آن را ملک مطلق خود دانسته و اجازه هرگونه فعالیت و ورود به حریم خصوصی دیگران را به خود میدهند .

[1]. Im molate

در زیر به بعضی مصادیق نقض حریم خصوصی در فضای مجازی که در قانون جرایم رایانه ای جرم انگاری شده است می پردازیم :

۱- دسترسی غیرمجاز به داده های رایانه‌ای یا مخابراتی نظیر هک ایمیل یا اکانت اشخاص .

۲- شنود غیرمجاز محتوای در حال انتقال در سیستم های رایانه‌ای یا مخابراتی نظیر استفاده از نرم افزارهای شنود چت های اینترنتی .

۳- دسترسی غیرمجاز به داده های سری در حال انتقال در سیستم های رایانه‌ای یا مخابراتی یا حامل‌های داده یا تحصیل و شنود آن .

٤- در دسترس قرار دادن داده های سری در حال انتقال در سیستم های رایانه‌ای یا مخابراتی یا حامل های داده برای اشخاص فاقد صلاحیت .

۵- نقض تدابیر امنیتی سیستم های رایانه‌ای یا مخابراتی به قصد دسترسی به داده های سری در حال انتقال در سیستم های رایانه‌ای یا مخابراتی یا حامل های داده .

٦- حذف یا تخریب یا مختل یا غیرقابل پردازش نمودن داده های دیگری از سیستم های رایانه‌ای یا مخابراتی یا حامل های داده به طور غیرمجاز .

۷- از کار انداختن یا مختل نمودن سیستم های رایانه‌ای یا مخابراتی به طور غیرمجاز نظیر غیر فعال سازی دیتابیس تارنماها و ممانعت از دسترسی اشخاص به پایگاه اینترنتی های شخصی .

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

۹- ربودن داده های متعلق به دیگری به طور غیرمجاز .

۱۰- هتک حیثیت از طریق انتشار یافتن صوت و فیلم تحریف شده دیگری به وسیله سیستم های رایانه‌ای یا مخابراتی .

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

۱۲- فروش یا انتشار یا در دسترس قرار دادن گذرواژه یا هر داده ای که امکان دسترسی غیرمجاز به داده ها یا سیستم های رایانه ای یا مخابراتی متعلق به دیگری را فراهم کند .

۱۳- آموزش نحوه ارتکاب جرایم دسترسی غیرمجاز ، شنود غیرمجاز ، جاسوسی رایانه‌ای و تخریب و

اخلال در داده ها یا سیستم های رایانه‌ای و مخابراتی .

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

مبحث های آتی دو مورد از مهم ترین موارد نقض حریم خصوصی در فضای مجازی که شامل (دسترسی غیرمجاز و شنود غیرمجاز) و موارد مربوط به ارتکاب آن است را ، به طور کامل بررسی می نماید ، زیرا موارد بیان شده یعنی دسترسی غیرمجاز پیش زمینه ای است برای ارتکاب جرم شنود است ، پس بهتر آن است که با هر دو موارد نقض به طور کامل آشنا شویم . چراکه بررسی موردی تمام موارد مذکور از حوصلهٔ این بخش خارج می باشد .

مبحث دوم : دسترسی غیرمجاز

واژهٔ دسترسی از لحاظ لغوی به معنای قدرت و توانایی بیان شده است . (دهخدا ، ۱۳۷۷، ۱۰۸۵۷) . اولین رفتار فیزیکی که در جرم شنود در فضای سایبر مورد بررسی قرار می دهیم دسترسی غیرمجاز می باشد .دسترسی غیرمجاز به داده ها یا سامانه های رایانه ای و مخابراتی از جمله جرایم خاص رایانه ای می باشد که در محیط سایبر به وقوع می پیوندد . به همین دلیل آن را زیر مجموعهٔ جرایم رایانه ای محض می دانند . دسترسی غیرمجاز را به عنوان جرمی مادر تلقی می کنند زیرا دارای نقشی موثر در وقوع سایر جرایم رایانه ای می باشد . در برخی موارد دسترسی غیرمجاز عامل تسهیل کننده در وقوع سایر جرایم رایانه ای و حتی جرایم سنتی است و در برخی موارد دیگر به عنوان مقدمه ارتکاب جرم تلقی می شود . از نظر میزان وقوع و میزان خسارت هم در سطح بالایی قرار دارد . (زندی ، ۱۳۸۹ ، ۱۷۹)

واژهٔ دسترسی از بعد مفهومی ، عام است به نحوی که عناوینی همچون دستیابی و نفوذ غیر قانونی[1] را نیز در بر می گیرد . و در اصطلاح تخصصی رایانه ای دستیابی را عمل خواندن داده ها از حافظه یا نوشتن داده ها ذکر کرده اند (هیئت مولفان و ویراستاران انتشارات مایکروسافت ، ۱۳۸۱، ۲۰).

به این ترتیب ، دسترسی غیرمجاز عبارت است از :

A دسترسی بدون مجوز به سیستم ها یا داده های رایانه‌ای (جزئاً یا کلاً) بدون نقض تدابیر ایمنی یا

[1] Cracking.

حفاظتی آنها ≅ . (تحیری ، ۱۳۸۹ ، ۱۸)

همچنین در بند ٦ ماده ۲ لایحهٔ حمایت از حریم خصوصی در تبیین دسترسی به اطلاعات بیان می شود : دسترسی به اطلاعات اعم است از مشاهده سند یا هر وسیله یا هر چیز دیگری که اطلاعات در آن ثبت یا ذخیره شده است و اطلاع از محتوای آن از طریق مطالعه یا استنساخ یا تکثیر تمام یا برخی قسمت ها و یا با تهیه یک رونوشت کامل از آن . (آقایی نیا ، ۱۳۸٦ ، ۲٤۷)

طرح های نوین قانونی مربوط به استراق سمع و دسترسی غیرمجاز به سیستم های ارتباطی و داده پردازی ، رویکرد گوناگونی در بردارد . در برخی از این طرح ها A صرف ≅ دسترسی به سیستم های داده پردازی جرم تلقی شده و در برخی دیگر آن دسته از دسترسی ها قابل مجازات دانسته شده که متضمن تحصیل ، تغییر یا صدمه دیدن اطلاعات باشد . اولین قانونی که A صرف ≅ دسترسی را جرم تلقی کرد ، قانون داده های سوید مصوب آوریل ۱۹۷۳بود که در مادهٔ ۲۱ اینگونه بیان کرده هرکسی را که به داده های رایانه ای ذخیره شده دسترسی پیدا کند قابل مجازات می داند . (زیبر ، ۱۳۸۳ ، ۱۵۸)

تشخیص بین دسترسی غیرقانونی و جرایم بعدی مهم است ، به طوری که پیش بینی های قانونی تعریف متفاوتی روی حفاظت دارند . در بیشتر موارد ، دسترسی غیرقانونی (جایی که قانون دنبال حفاظت از صحت و سقم خود رایانه می باشد) هدف نهایی نمی باشد ، بلکه اولین گام به سمت جرایم دیگر است ، مثل تغییر دادن یا بدست آوردن اطلاعات ذخیره شده .

سؤال این است که آیا دسترسی غیرقانونی را باید ، همراه با جرایم بعدی جرم به شمار آورد ؟ تجزیه و تحلیل رویکرد های مختلف برای جرم به حساب آوردن دسترسی غیرقانونی به رایانه در سطح ملی نشان می دهد که گاهی اوقات ماده های قانونی وضع شده دسترسی غیرقانونی با جرایم بعدی را با هم اشتباه می گیرد ، یا دنبال محدود کردن جرم دانستن دسترسی غیرقانونی تنها به جرایم خیلی مهم می باشد . برخی کشورها دسترسی صرف را جرم می دانند ، در حالی که کشورهای دیگر تخلف را تنها محدود به مواردی می دانند که سامانه مورد دسترسی با اعمال امنیتی حفاظت شده است ، یا مواردی که مجرم نیت خطرناک دارد ، یا مواردی که داده ها را به چنگ بیاورد ، تغییر دهد یا از بین ببرد . مخالفان جرم دانستن دسترسی غیرقانونی اشاره به موقعیت هایی که هیچ خطری توسط دسترسی صرف ایجاد نمی شود دارند ، یا مواردی که هک کردن منجر به شناسایی ضعف ها و روزنه ها در امنیت رایانه مورد هدف می شود .

کنوانسیون جرایم سایبری دارای ماده ای است که دسترسی غیرقانونی به رایانه های حفاظت شده را زمانی

جرم تلقی می کند که فرد اطلاع از دسترسی غیرمجاز به سامانه را داشته باشد (گرکی ، ۱۳۸۹ ، ۲۴۲).

و در آخر متخصصین حقوق کیفری رایانه نیز از عباراتی دیگر مانند نفوذ غیرمجاز ، ورود غیرمجاز و دستیابی غیرمجاز استفاده می‌کنند که به زعم ما همه آنها در زیر مجموعه دسترسی غیرمجاز قرار می گیرند.

گفتار اول : داده ها موضوع ارتکاب جرم دسترسی غیرمجاز

داده در لغت به معنای اطلاعات ، مفروضات ، دانسته ها و سوابق آمده است . (حییم ، ۱۳۷۷ ، ۱۲۵)

داده را می توان دارای اقسامی دانست داده رایانه ای ، داده مخابراتی ، داده موجود روی کارت های اعتباری ، داده موجود روی تراشه های مغناطیسی اما به طور کلی عبارت است از اطلاعاتی که در قالبی خاص ایجاد ، ذخیره و نگهداری می شوند . آنچه موضوع جرایم رایانه ای واقع می شود ، غالباً داده های رایانه ای هستند . البته اقسام دیگر نام برده شده از داده را می توان به نوعی داده رایانه ای دانست ، چراکه امروزه با در هم آمیختن تجهیزات مخابراتی و سیستم های رایانه ای دیگر عملاً تفکیک این فضاها از یکدیگر میسر نیست . داده های موجود روی کارت ها و تراشه ها نیز به وسیلهٔ رایانه قابل ایجاد ، ذخیره و پردازش است . لذا دادهٔ رایانه ای دارای مفهوم عامی است که سایر انواع یاد شده ، زیر مجموعه های آن هستند . به همین علت کنوانسیون جرایم سایبر در بند Aب≅ ماده یک خود داده رایانه ای را اینگونه تعریف کرده است :

A به معنای هر نمادی از واقعیات ، اطلاعات یا مفاهیم است که به شکلی که برای پردازش در سیستم رایانه ای که حاوی برنامه ای مناسب برای واداشتن یک سیستم رایانه ای به انجام یک وظیفه است ، مفید باشد ≅ .

بنابراین نکتهٔ مهم در داده رایانه ای قابلیت پردازش توسط رایانه است . (جاویدنیا ، ۱۳۸۷ ، ۵۹)

برای اینکه تمامی انواع داده ها مورد توجه قرار گیرند ، آنها را به دو گروه اصلی تقسیم کرده اند :

۱ . داده های رایانه ای ذخیره شده

۲ . داده های در جریان ارتباطات

سپس داده های در جریان ارتباطات که در واقع می توان از آنها به داده های شبکه ای یاد کرد را در دو شاخه قرار داده اند که عبارتند از :

۱ . داده ترافیک ۲ . داده محتوا

مضافاً اینکه گروه دیگری از اطلاعات هستند که حالت بینابین دارند ، یعنی علاوه بر اینکه اطلاعات شبکه ای محسوب می شوند ، اما در حالت ذخیره شده قرار دارند و در جریان نیستند از آنها به اطلاعات راجع به مشترک یاد می شود . (جلالی فراهانی ، ۱۳۸٦ ، ۲۵۸)

نکتهٔ جالب توجه دیگری که مدنظر قرار گرفته است تفکیک دو اقدام حفظ داده ها و نگهداری داده ها از یکدیگر است . با اینکه این دو اصطلاح رایج تقریباً به یک معنا هستند ، اما در حوزه کامپیوتر از معانی متمایزی برخوردارند . منظور از حفظ داده ها ، مراقبت از داده هایی است که هم اکنون در قالب ذخیره وجود دارند و از آنها در برابر هرگونه تغییر یا ایجاد خدشه در کیفیت یا وضعیت کنونی جلوگیری می شود . منظور از نگهداری داده ها ، در اختیار داشتن داده هایی است که هم اکنون ایجاد می شوند و در آینده در تصرف یک شخص قرار خواهد گرفت . به این ترتیب ، نگهداری داده ها این مفهوم را به ذهن متبادر می گرداند که هم اکنون حجمی از داده ها تولید می شوند تا در آینده تحت تصرف یک شخص برای مدتی نگهداری شود . در واقع نگهداری داده ها فرآیند ذخیره سازی آنهاست . اما حفظ داده ها اقدام برای ایمن و سالم نگه داشتن داده های ذخیره شده است . (جلالی فراهانی ، ۱۳۸٦ ، ۲٦۰)

به طور کلی هرگونه اطلاعاتی که از طریق دستگاه ورودی به درون رایانه وارد می شود تا عملیاتی روی آن به اجرا در آید داده گفته می شود و جمع آنها داده هاست ، به عبارت دیگر به اطلاعات خاصی که وارد رایانه می شوند تا پردازشی روی آنها صورت گیرد داده اطلاق می شود و به نتیجه ای که حاصل پردازش بر روی داده های خام می باشد اطلاعات گفته می شود ، یعنی اطلاعات شکل تغییر یافته داده هاست . اطلاق کلمه داده ها ، شامل همه نوع داده ای می شود . لذا ارزشمند بودن یا بی ارزش بودن ، قابل استفاده غیرقانونی بودن یا نبودن داده ها ، مورد نظر نبوده و دسترسی غیرمجاز و عمدی همراه با نقض تدابیر حفاظتی (که بر عنوان هک کاملاً منطبق است) به همه نوع داده ها ، اعم از تجاری ، سیاسی و غیره جرم شمرده شده است ؛ چراکه صرف ارتکاب دسترسی غیرمجاز به داده ها موجب نقض اصل محرمانه بودن داده ها و اطلاعات می گردد . (شیرزاد ، ۱۳۸۸ ، ۸۰)

گفتار دوم : هکرها[1] و دسترسی غیرمجاز فنی

شیوه های دسترسی غیرمجاز را می توان به شیوه های فنی (از جمله ؛ دسترسی بر گذرواژه ها ، دسترسی از رهگذر درهای پشتی ، دسترسی از طریق مودم) و شیوه های غیرفنی (شامل شیوه های مبتنی بر دانش مهندسی اجتماعی ، اشغال گردی ، برقراری ارتباط دوستانه با مدیر سیستم ، جعل عنوان) تقسیم کرد . مرحله های ارتکاب را می توان به منزلهٔ یک فرایند از لحظه شروع تا پایان از نظر فنی و حقوقی تقسیم نمود . از نظر فنی ، این مراحل در برگیرنده گزینش هدف ، گردآوری اطلاعات و سازماندهی آنها و طرح ریزی ، اجرا و پاکسازی حمله است . از نظر حقوقی نیز این مراحل عبارتند از قصد ارتکاب ، اجرای عملیات مقدماتی ، شروع به جرم و اجرای آن . از لحاظ فنی مرتکبین این جرم به A هکرها ≅ معروف می باشند . (حسینی خواه و رحمتی ، ۱۳۸۹ ، ۵۷)

دسترسی به سامانه های رایانه ای و مخابراتی باید همراه با نقض تدابیر ایمنی و حفاظتی باشد و إلا نمی توان عمل را جرم دانست . در واقع سامانه های بدون محافظ از حمایت کیفری خارج شده اند . ماده ۷۲۹ و تبصره ۲ ماده ۷۳۱ بیان کننده این شرط می باشند . منظور از تدابیر ایمنی و حفاظتی کلیه روش های فنی و مهندسی ، اعم از سخت افزاری یا نرم افزاری اتخاذ شده برای جلوگیری از دسترسی غیرمجاز است . در ضمن منظور از دسترسی اعم است از تحت کنترل قرار دادن (شنود ـ رهگیری) نظارت و یا در اختیار گرفتن داده یا سامانه رایانه ای و یا استفاده از آنها با روش های ویژه فنی ـ مهندسی اعم از اینکه صاحب ، متصرف ، دارنده یا ذی حق را از اعمال حق نسبت به آنها باز دارد یا خیر . (زندی ، ۱۳۸۹ ، ۱۷۳)

در میان متخصصان اعم از فنی و حقوقی نسبت به مفهوم دسترسی غیرمجاز وحدت نظر وجود ندارد . متخصصان فنی از عبارت هکینگ استفاده کرده و منظور از آن را هر نوع حمله به سامانه های ایمنی بیان می کنند . برخی دیگر هکینگ را در معنای محدودتر ، نفوذیابی یا نفوذگری ترجمه می کنند . (شهیدی ، ۱۳۷٤ ، ۸۸). اما همچنین Aنفوذگری≅ یا Aنفوذیافتگی≅ را نیز نمی‌توان معادل یا ترجمه A هکینگ ≅ دانست. زیرا همانطور که بیان نمودیم هکینگ تنها شامل صرف دسترسی غیرمجاز به سیستم های ایمن (نفوذ) نمی باشد . بلکه هرگونه تهاجم و حمله به سیستم های ایمن را در بر می‌گیرد . به همین دلیل در ترجمه هکینگ ، به جای عبارت A نفوذگری ≅ پیشنهاد می‌نماییم از عبارت A تجاوزگری ≅ ، استفاده شود (تحیری ، ۱۳۸۹ ، ۳۵). و برخی دیگر هکینگ را مترادف با دسترسی غیرمجاز می دانند ولی باید بیان

[1]. Hackers

نمود که هکینگ را نمی توان مترادف با دسترسی غیرمجاز انگاشت زیرا هکینگ چه در عنوان و چه در آماج و چه در نوع سامانه بر حسب ایمن یا غیرایمن بودن و چه در وسعت شمول افعال مادی با دسترسی غیرمجاز متفاوت است (زندی، ۱۳۸۹ ، ۱۷٤) .

HackA به زبان ساده و شاید عامیانه ترین تعبیر آن دزدیده شدن کلمه عبور یک سیستم می باشد. هکر شخصی باهوش ، فرصت طلب ، دارای معلومات بالا با افکار سازنده و مطمئناً با وجدان است . لازم به ذکر است که هکرها با دزدان اینترنتی و یا الکترونیکی تفاوت دارند هکرهای واقعی در میان خود دارای مرام نامه ای هستند که همه پایبند به آن می باشند (ضیایی پرور ، ۱۳۸۳ ، ۵۰).

در دهۀ ۱۹۷۰ واژه هکر به شخصی اطلاق می شد که در برنامه نویسی بسیار ماهر و باهوش باشد . بعدها در دهۀ ۱۹۸۰ این واژه به معنی شخصی بود که در " نفوذ " به سیستم های جدید به صورت ناشناس تبحر داشته باشد . امروزه بیشتر با هدف ترساندن هکرها ، رسانه ها و مقامات مسئول مانند آژانس های دولتی و ادارات پلیس، این واژه را به هر شخصی که مرتکب یک جرم مرتبط با فناوری شود اطلاق می دهند (معاونت اجتماعی فرماندهی انتظامی ، ۱۳۸٤ ، ۱۰۲).

تمرکز هکرها روی رایانه های شخصی جالب است . دو رویکرد برای بدست آوردن اطلاعات وجود دارد :

ـ دسترسی به رایانه یا وسیله ذخیره داده ها و استخراج اطلاعات

ـ استفاده از عملی که منجر به آشکار کردن اطلاعات یا کدهای دسترسی کاربران شود که مجرمان را در دسترسی به اطلاعات قادر می سازد .

مجرمان اغلب از ابزارهای نصب شده روی رایانه قربانی یا نرم افزارهای مخرب که خفا ابزار نامیده می شود برای ارسال اطلاعات به آنها استفاده می کنند . انواع متفاوتی از خفا افزارها در طول سالیان اخیر کشف شده است از قبیل لاگرها ابزارهای نرم افزاری هستند که هر فشار کلیدی را روی صفحه کلید رایانه ویروسی شده ثبت می کنند . برخی لاگرها به محض اینکه رایانه به اینترنت وصل شود ، همه اطلاعات ثبت شده را برای متخلف می فرستند (گرکی ، ۱۳۸۹ ، ٤۷)

کارهایی که هکرها انجام می دهند معمولاً از روی بد خواهی نیست . انگیزۀ بیشتر هکرها برای این کار ، تمایل شدید به یادگیری نحوه کار سیستم رایانه ، یافتن راهی برای ورود مخفیانه به آنها و پیدا کردن سوراخ های امنیتی این سیستم ها است . هیجان خواندن اطلاعاتی که می دانند اجازۀ دیدن آنها را ندارد یا

انجام کاری که می دانند قانونی نیست به لذت دست زدن به چنین تجاربی توسط هکرها به عنوان سرگرمی می افزاید(معاونت اجتماعی فرماندهی انتظامی ، ۱۳۸٤ ، ۱۰۲)

هک کننده که فاعلی قاصد است ، با صرف وقت بسیار ، حفره های حفاظتی داده ها و سیستم های رایانه ای و مخابراتی را می یابد ، بدان نفوذ می کند و امنیت اطلاعات را به باد سخره می گیرد . هک کنندگان گاه به عنوان تفریح و خودنمایی و گاه با هدف باج گیری یا تهدید صاحبان داده ها یا سیستم ها و گاه با هدف جاسوسی ، اطلاعاتی را که مجاز به دسترسی بدان نیستند را مشاهده می کنند . دسترسی غیرمجاز از یک سو امنیت اطلاعاتی شهروندان جامعه اطلاعاتی را تهدید می کند و منجر به ناامنی و غیر قابل اعتماد بودن یکی از مفیدترین فناوری قرن اطلاعات؛ یعنی اطلاعات الکترونیکی می شود(طارمی ، ۱۳۸۷ ، ۱٦)

هک، دنیای پیچیده ای است ، اما فرهنگ هک تقسیم بندی ساده ای برای انواع هکرها دارد :

۱ . هکرهای کلاه سفید :

هکرهای کلاه سفید متخصصان و کامپیوتر دوستانی هستند که سعی می کنند عیوب امنیتی در یک سیستم کامپیوتری را پیدا کرده و آنها را برطرف سازند . بسیاری از شرکت ها ، هکرهای کلاه سفید را برای آزمایش شبکه های کامپیوتری و خدمات اینترنتی خود استخدام می کنند(ضیایی پرور ، ۱۳۸۳ ، ٥٤)

این افراد سعی در بی اعتبار کردن و نابودی سیستم های رایانه ای دارند . این هکرهای کلاه سفید به صورت غیرقانونی به سیستم ها نفوذ می کنند . در صورت موفقیت یک حفرهٔ امنیتی و یک نقطه آسیب پذیر سیستم را تشخیص می دهند و از این راه از مدیران سیستم ها پول می گیرند تا در رفع آن به مدیر سیستم کمک کنند . (حسینی خواه و رحمتی ، ۱۳۸۹ ، ۵۷)

و در نهایت هکرهای کلاه سفید به افرادی گفته می شود که به پیشرفت امنیت در دنیای دیجیتال فکر می کنند .

۲ . هکرهای کلاه سیاه :

اما کلاه هکرهای کلاه سیاه واقعاً سیاه هستند ، چون آنها سوء نیت دارند . هکر کلاه سیاه به فردی اطلاق می شود که به منظور صدمه زدن وارد یک سیستم می شود . هکرهای کلاه سیاه به روش های مختلفی کار می کنند . بهترین عمل هکر کلاه سیاه ، شامل دزدی و اخاذی می شود . هکرهای کلاه سیاه معمولاً اطلاعات خود را درباره حفره های امنیتی از طریق اینترنت به سایر هکرهای کلاه سیاه در سراسر

دنیا انتقال می دهند . (ضیایی پرور ، ۱۳۸۳ ، ٥٦) . هکرهای کلاه سیاه افرادی هستند که امیدوارند از ضعف های سیستم های دیگران به نفع خود بهره برند . نفوذ این کلاه سیاه ها ، سبب بروز اشکال در ارائه برخی سرویس ها ، به خطر افتادن داده ها و از دست دادن صدها هزار دلار در سال می شود . (حسینی خواه و رحمتی ، ۱۳۸۹ ، ۵۸). این اصطلاحات از سینمای وسترن گرفته شده که در آنها آدم های خوب ، کلاه سفید و آدم های بد کلاه سیاه بودند .

گفتار سوم : دسترسی و تحصیل داده

تحصیل داده ملازمه با جرایمی همچون دسترسی غیرمجاز و شنود غیرمجاز دارد . هرچند که به زعم برخی دستیابی غیرمجازی که در ماده ۷۵ قانون تجارت الکترونیک بیان شده همهٔ این عناوین را در بر می گیرد . (جاوید نیا ،۱۳۸۷ ، ۲۷٦) باید بیان نمود که معمولاً تحصیل داده یا هر نوع اطلاعات مرحله ای بعد از دسترسی غیرمجاز می باشد ، با این توضیح که شخصی که می خواهد به صورت غیرمجاز داده ای را تحصیل کند ، ابتدا باید به آن دسترسی پیدا کرده و سپس آن را تحصیل یا کسب کند ، به خاطر همین بیان شده است که تحصیل یک داده ملازمه با دسترسی غیرمجاز دارد .

مبحث سوم : شنود غیرمجاز در فضای سایبر

یکی از اشکال تجسس در امور شخصی مردم شنود غیرمجاز است که در کنار سایر جرایم مرتبط با فناوری ارتباطات توجه جوامع بین المللی و نیز حقوق داخلی کشورها را به خود معطوف داشته است .

گرچه لفظ شنود متبادر در دریافت فایل های صوتی است ، اما در حقیقت منظور صرف فایل های صوتی یا مخابراتی نبوده ، شامل هر نوع داده در حال انتقالی است . در حقیقت هر نوع پردازش، مشاهده ، شنود ، دریافت یا ذخیره غیرقانونی اطلاعات در حال انتقال و ذخیره شده ای ، را شامل می شود که مجرم مجاز به دریافت یا شنود آن نیست ، آنجایی که داده غیرعمومی و خصوصی است . در صورتی که غیرعمومی باشد ، مشمول ماده ۲ قانون مجازات جرایم رایانه ای می شود . اما اگر عمومی و جزء اطلاعات سری باشد ، مشمول ماده ۳ قانون مجازات جرایم رایانه ای است . ما در این مبحث به دو نمونه از مهمترین مصداق های شنود غیرمجاز در فضای سایبری اشاره خواهیم کرد که عبارتند از :

ـ شنود اطلاعات از طریق پست الکترونیکی

ـ شنود و دستیابی به اطلاعات از طریق فیشینگ[1]

[1].Phishing

نتیجه گیری :

پیشرفت تکنولوژی کامپیوتر و توسعهٔ کاربرد آن ، وابستگی تنگاتنگ زندگی مدرن امروزی به این فناوری را در تمامی زمینه های مختلف به ارمغان آورده است . به طوری که امروزه عملاً بدون وجود کامپیوتر ، حیات جامعهٔ جهانی مختل خواهد شد . بطور طبیعی هر نوآوری در زمینهٔ تکنولوژی و علوم به تبع خود توجه افراد سودجو و بزهکاران را نیز جلب می نماید و این افراد ، امکاناتی را که می تواند در جهت اعتلای تمدن بشری و امنیت و رفاه بکار رود ، در جهت منافع خود و ارضاء حوائج شخصی بکار می برند ، به طوری که جرایم مربوط به تکنولوژی کامپیوتری امروزه توجه حقوقدانان ، جرم شناسان ، متخصصین کامپیوتر و پلیس های جهان را به خود معطوف کرده است .

خصوصاً در دههٔ ۹۰ ، جرایمی در محیط سایبر تجلی نمود که آن حاصل تکنولوژی ارتباطاتی ، مخابراتی و پیدایش شبکه های بین المللی بوده و با توجه به خصوصیت غیرملموس و مجازی بودن محیط سایبر ، مسایل جزایی آن به گونه ای متفاوت تر نسبت به جرایم کامپیوتری نسل های قبل بیان می شود . چراکه از سویی فضای سایبر همچون بستری برای ارتکاب جرایم نوظهور مانند شنود غیرمجاز و دستیابی به اطلاعات محرمانه می باشد و از سوی دیگر همانطور که می دانیم یکی از عناصر اصلی و ارزشمند کاربران ، اطلاعاتی است که در فضای سایبر آن را مدیریت می کنند . چه آن اطلاعات محرمانهٔ سازمانی باشد یا اطلاعات شخصی کاربران .

پیشرفت تکنولوژی کامپیوتری و اطلاعاتی به خصوص در زمینهٔ تبادل اطلاعات در سطح بین المللی و بروز جرایم پیچیده تر و تخصصی تر مرتبط با این فناوری (جرایم سایبر) ، مشکلات و معضلات بسیاری را برای کاربران کامپیوتر و اینترنت بوجود آورده است . مجرمان کامپیوتر بدون هراس از احتمال دستگیری یا تعقیب قانونی ، در شبکه اینترنت به کمین نشسته اند و به عنوان تهدیدی جدی برای سلامت مالی شرکت های تجاری ، مشتریان و کاربران شبکه و امنیت کشورها مطرح هستند .

بطور کلی جرایم کامپیوتری و شبکه ای با اغلب جرایم متعارف و کلاسیک در چند مورد اختلاف اساسی دارند :

اولاً شیوه ارتکاب آنها تقریباً آسان است ، ثانیاً با منابعی اندک ، خسارتی هنگفت می توانند وارد کنند، ثالثاً می توان بدون حضور فیزیکی در یک حوزهٔ قضایی معین ، در آن حوزه مرتکب اینگونه جرایم شد . رابعاً در اغلب موارد (به خصوص جرایم سایبر) غیرقانونی بودن و منشأ آنها روشن و آشکار نیست و خامساً

امروزه جرایم کامپیوتری و اینترنتی غالباً در ابعاد بین المللی به وقوع می پیوندد .

حال با توجه به خصوصیات فوق و این مسئله که تکنولوژی کامپیوتر و اینترنت امروزه با تغییر ماهیت از موضوعات ملموس و عینی به موضوعات نوینی همچون داده ها و اطلاعات غیرفیزیکی مطرح می باشد ، جرایمی همچون دسترسی غیرمجاز و شنود غیرمجاز در اولویت بحث قرار می گیرند .

قبل از افزایش و گسترش به کار گیری فناوری جدید ، و بروز جرایم سایبر ، قوانین سنتی نیز در محدوده های خاص خود به صورت پراکنده به بزه شنود پرداخته بودند . (ماده ۲۵ قانون اساسی) با پیشرفت حیرت آور فناوری اطلاعات و به تبع آن ظهور بی تقوایی ها ، انحراف ها و تخلفاتی که عواقب آن دامنگیر افراد ، خانواده ها و جامعهٔ بشری می شود ، ضرورت قانونگذاری و جرم انگاری این جرایم پیش از پیش احساس شد . به همین ترتیب قانون جرایم رایانه ای با نگرشی نو پا به عرصه نهاد تا پاسخگوی فناوری جدید باشد . از این رو در ماده ۲ و تبصره ٤٨ قانون جرایم رایانه ای ، انواع شنود محتوای در حال انتقال اعم از رایانه ای ، مخابراتی و امواج الکترومغناطیسی و نوری را در خود گنجانید و حتی می توان گفت از عنوان قانون که A جرایم رایانه ای ≅ بود ، فراتر رفت .

همانطور که بیان شد اولین گام در بزه شنود و جرایم زاده فضای سایبر ، دسترسی به اطلاعات می باشد ؛

دسترسی غیرمجاز ، به عنوان یکی از جرایم رایانه‌ای محض ، از جمله جرایمی می باشد که دارای نقشی زاینده در ارتکاب سایر جرایم رایانه‌ای ، خصوصاً جرایم رایانه‌ای محض می باشد . به همین دلیل در محیط سایبر ، جرمی مادر تلقی می‌شود و عاملی تسهیل کننده در وقوع سایر جرایم از قبیل شنود غیرمجاز به حساب می آید . بعد از دسترسی به اطلاعات در بزه شنود ، بحث تحصیل داده مطرح می شود اما باید بیان نمود که معمولاً تحصیل داده یا هر نوع اطلاعات مرحله ای بعد از دسترسی می باشد ، یعنی شخص در ابتدا باید به صورت غیرمجاز به داده دسترسی پیدا کند و سپس آن را کسب کند . حال اگر بعد از کسب داده ، آن را تخریب یا دستکاری کند می توان آن را به هر دو مجازات محکوم نمود ؛ اول به دلیل دسترسی و تحصیل داده و دوم به دلیل تخریب اطلاعات .

شنود اطلاعات محرمانهٔ افراد در فضای سایبر ، با هک و نفوذ به سامانه های رایانه ای و مخابراتی با نیت و قصد مجرمانه ای که در قانون جرایم رایانه ای تعریف شده است ، جرم تلقی می شود . شنود در فضای سایبر ، شیوه نفوذ به داخل سامانه از طریق لایه های زیرین شبکه به دلیل انعطاف زیاد ، بیشتر مورد

توجه نفوذگران حرفه ای است و نفوذ به داخل سامانه به این صورت بسیار مخرب وخطرناک است چراکه شنود اطلاعات می تواند شامل داده ، متن ، تصویر ، صدا ، کد ، پایگاه داده ای ، هرگونه نرم افزار ایجاد شده یا انتقال دادنی یا ذخیره شدنی باشد پس بنابراین شنود می تواند برای کاربران دنیای مجازی بسیار صدمات جبران ناپذیری را به همراه داشته باشد . اما اگر در بحث شنود جرایمی همچون دسترسی غیرمجاز ، شنود و جاسوسی رایانه ای به موازات یکدیگر اتفاق بیافتد باید براساس قاعدهٔ تعدد معنوی نسبت به آن عمل کرد .

در نتیجه با توجه به تمامی مطالب مذکور ، چالش بین قوانین حقوقی و عملیات رایانه ای ، اساساً مانند سایر فناوری های روز می باشد . برای حفظ تعادل بین نیازهای جامعه و حقوق انفرادی اشخاص و حفظ امنیت جامعه ، قوانین حقوقی باید روش های جدیدی را که به بررسی و مقابله با رفتار مجرمانه را مجاز می شمارد ، گسترش دهد . این روش ها بدون تردید ، روش های نوین ارتباطات هشدار دهنده و جست و جو در مجموعهٔ عظیم داده ها را نیز شامل می شود . جامعه نمی تواند به رفتارهای ضد اجتماعی یا رفتارهای خشن به سادگی اجازه بروز دهد زیرا باعث بروز مشکلات پیچیده دیگری در جامعه می شود .

اما بهترین راه برای جلوگیری از وقوع اکثر جرایم رایانه‌ای به آگاهی ما بستگی دارد و از سوی دیگر مبارزه با این جرم رایانه ای همانند سایر جرایم با پیشگیری شروع می شود که بهترین راه حل در پیشگیری برقراری امنیت در این فضا می باشد . و نیز اگر تعداد بیشتری از مردم از اشکال و روش‌های فعلی جرایم سایبر آگاهی یابند ، تعداد قربانیان کاهش خواهد یافت . تنها هدف از نگارش این پایان نامه آشنایی کاربران با جرم خطرناک و پر آسیب ، شنود غیرمجاز بوده تا باشد ، که افراد کمتری به دام نفوذگران سایبری گرفتار شوند .

منابع

انصاری ، باقر ، ۱۳۸۲ ، **مقدمه ای بر مسئولیت مدنی ناشی از ارتباطات اینترنتی** ، مجله دانشکده حقوق و علوم سیاسی تهران ، شماره شصت و دو .

ایمانی , عباس ، ۱۳۸۲ ، **حمایت از حق خلوت آدمیان در عصر اطلاعات** ، مجله پژوهش های حقوقی ، موسسه مطالعات و پژوهش های نشر دانش ، شماره دو .

امانی ، حمید رضا ، ۱۳۸۹ ، **بررسی ابعاد کیفری شنود غیر مجاز در عرصه فن آوری اطلاعات و ارتباطات** ، نشریهٔ داخلی قوه قضاییه مأوی ، شماره های ۹۱۹ ، ۹۲۰ ، ۹۲۱ ، ۹۲۲ ، ۹۲۳ ، تهران .

آقایی نیا ، حسین ، ۱۳۸٦ ، **جرایم علیه اشخاص (شخصیت معنوی)** ، چاپ دوم ، تهران ، انتشارات میزان .

باستانی ، برومند ، ۱۳۸۳ ، **جرایم کامپیوتری و اینترنتی جلوه ای نوین از بزهکاری** ، چاپ اول ، تهران انتشارات بهنامی

جلالی فراهانی ، امیر حسین ، ۱۳۸۹ ، **کنوانسیون جرایم سایبر و پروتکل الحاقی آن** ، چاپ اول ، تهران ، انتشارات خرسندی .

جی آیکاو ، دیوید ، کارل ای . سیگر ، ویلیام آر . وان استروچ ، ۱۳۸۳ ، **راهکارهای پیشگیری و مقابله با جرایم رایانه ای** ، مترجمان : اکبر استرکی ، تورج ریحانی ، محمد صادق روزبهانی ، راحله الیاسی ، چاپ اول ، تهران ، انتشارات دانشگاه علوم انتظامی (معاونت پژوهشی)

حسینی خواه ، نورالله ، رحمتی ، داریوش ، ۱۳۸۹ ، **پلیس و جرایم رایانه ای** ، چاپ اول ، تهران ، ناشر معاونت تربیت و آموزش ناجا .

زیبر ، اولریش ، ۱۳۸۳ ، **جرایم رایانه ای** ، مترجمان : محمد علی نوری ، رضا نخجوانی ، مصطفی بختیاروند ، احمد رحیمی مقدم ، چاپ اول ، تهران ، انتشارات گنج دانش .

طارمی ، محمد حسین ، ۱۳۸۷ ، **طبقه بندی و آسیب شناسی جرایم رایانه ای** ، دو هفته نامه پگاه حوزه ، قم ، شماره دویست و سی و پنج .

خبرنامه شورای عالی انفورماتیک کشور ، ۱۳۷٦ ، **خلاصه مقالات سمپوزیوم بین المللی دربارهٔ جلوگیری و تعقیب جرایم کامپیوتری** ، ترجمه محمد حسن دزیانی ، جلد اول ، بنیاد محاسبات کامپیوتر.

یزدانی ، بهروز ، ۱۳۸۹ ، **نگاهی حقوقی به حریم خصوصی** ، طرح تحقیقاتی کارشناسی حقوق ، تهران ، دانشگاه آزاد اسلامی .

حییم ، سلیمان ، ۱۳۷۷ ، **فرهنگ کوچک انگلیسی ـ فارسی** ، چاپ پانزدهم ، تهران ، انتشارات فرهنگ معاصر.

شیرزاد ، کامران ، ۱۳۸۸ ، **جرایم رایانه ای از دیدگاه حقوق جزای ایران و بین الملل** ، چاپ اول ، تهران ، نشر بهینه فراگیر

ضیایی پرور ، حمید ، ۱۳۸۳ ، **جنگ نرم ۱ : ویژه جنگ رایانه ای** ، تهران ، چاپ اول ، انتشارات موسسه فرهنگی و تحقیقاتی ابرار

معاونت اجتماعی فرماندهی انتظامی ، ۱۳۸٤ ، **مروری بر آسیب های فضای مجازی در عصر فناوری اطلاعات** ، چاپ اول ، اصفهان ، ناشر معاونت اجتماعی انتظامی استان اصفهان .