فصلنامه مطالعات قرآنی، سال دهم، شماره ۳۹، پاییز ۱۳۹۸، صص ۲۲۱-۲۴۲

نقش دولت با محوریت اخلاق دینی در پیشگیری از نقض محرمانگی داده‌ها در فضای مجازی

نفیسه نکویی مهر *
عاطفه حسینی فرد **
رضا سلطانی ***

تاریخ دریافت: ۹۷/۱/۱۷
تاریخ پذیرش: ۹۷/۶/۲۱

چکیده

حریم خصوصی یکی از بسترهای جرم‌خیز در فضای مجازی است. این حریم، از جمله مهم‌ترین حقوق فردی است که هم از نگاه شرع مقدس اسلام و هم از دید قوانین کشورها و اسناد بین المللی، محترم و مصون از تعرض است. اما نقض حریم خصوصی و حفظ امنیت و سلامت کاربر در جامعه ما کم‌تر مورد توجه قرار گرفته است. از همین رو در این نوشتار با پرداختن به حوزه اخلاق دینی، که هم پشتوانه‌های استدلالی اخلاق کاربران را تحکیم می‌بخشد و هم ضمانت اجرای کارآمدی در اختیار قرار می‌دهد و نیز شرط مکمل راهبرد فردی- اخلاقی جامعه پذیری دینی، تقویت روحیه خود دیگرپنداری، آشناسازی با پیامد منطقی رفتار کاربران و نهادینه سازی امر به معروف و نهی از منکر است سعی در آموزش و بالابردن فرهنگ اجتماعی در خصوص جرایم سایبری شده است. همچنین به لحاظ اهمیت محرمانگی داده‌ها و حفظ حریم خصوصی افراد در فضای مجازی به تعریف این عامل و نقشی که دولت در آموزش اخلاق دینی به جامعه دارد پرداخته شده تا شاید نواقضی که در این زمینه وجود دارد، برطرف گردد.

کلیدواژگان: محرمانگی داده‌ها، فضای مجازی، نقض حقوق، حریم خصوصی.

* دانشجوی دکتری حقوق،گروه حقوق عمومی، واحد نجف آباد، دانشگاه آزاداسلامی، نجف‌آباد، ایران.
nafas.nekouimehr@gmail.com
** دانشجوی دکتری، گروه فقه و حقوق، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران.
atefehoseinifard@gmail.com
*** عضو هیأت علمی، گروه فقه و حقوق، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران.
نویسنده مسئول: نفیسه نکویی مهر

مقدمه

اکثر جرایم رایانه‌ای که از طریق اینترنت صورت می‌گیرند بسیار جدیدند لذا همین امر باعث شده است که بسیاری از مشکلاتی که به صورت تبعی با خود همراه آورده است نیز نیاز به انجام بعضی از کنترل‌های اجتماعی‌ای داشته باشند که از طریق فضای اینترنت بایستی صورت بگیرد.

به طور مثال به خاطر مشکلات پیش آمده در زمینه حملات سایبری به سازمان‌های تجاری و یا شرکت‌های اقتصادی، بسیاری از جوامع دنیا برای کنترل این اتفاقات و حفاظت از این نوع سازمان‌ها، در قوانین خود محدودیت‌ها و نیز مجازاتی در نظر گرفته‌اند.تا قرن بیستم، جرم‌شناسان دلایل مختلفی را برای ارتکاب یک جرم قائل شده‌اند ولی بعضی از این دلایل تقریباً برای اکثریت جوامع ثابت‌اند که بودن یا نبودن آن، خود باعث ارتکاب یک جرم و یا جلوگیری از وقوع آن می‌شود. به طور مثال فرهنگ (ارزش‌های خانوادگی و دینی)، اقتصاد و سیستم تعلیم و تربیت جزء عواملی هستند که خود می‌توانند در وقوع یا عدم وقوع یک جرم تأثیرگذار باشند. اما در این میان شاید بتوان جایگاه تعلیم و تربیت و نیز فرهنگ را از بقیه موارد مهم‌تر دانست. که البته این دو مورد، خود در دو زیرشاخه پیشگیری و یا درمانی(تدافعی) قابل بررسی هستند. آشنابودن خانواده‌ها با انواع بسترها و زیرشاخه‌های فضای سایبر، تأثیر بسزایی در تعلیم و تربیت کودکان و نوجوانان در جهت جلوگیری از ورود آن‌ها به فضای جرایم سایبری دارد.

در این میان نقش دین بسیار مهم است و اخلاق که بستر اصلی ادیان مختلف (خصوصاً دین اسلام) می‌باشد نیز خود تأثیری بسیار بر انجام یک تعلیم و تربیت درست خواهد داشت. بسیاری از اشتباهاتی که از یک انسان سر می‌زند را شاید بتوان در ساختار قانونی بدون اشکال دانست اما اگر هر فرد خود متعهد(مُتَخَلّق) به اخلاق دینی باشد بسیاری از اشتباهات به حیطه رفتار انسان نیز وارد نمی‌شود که حال بخواهیم آن را در حیطه جرم‌ها و سپس در ساختار جرایم سایبری بررسی کنیم.

شاید با گفتن معنای جرم در شریعت اسلام به این نکته پی‌ببریم که چگونه تمامی مطالب گفته شده تا به حال در این تعریف به صورت کاملاً واضح و مختصر نهفته شده است؛ تعریفی که نگاه جامعه‌شناسانه و روان‌شناسانه به طور کامل در آن پیداست. تعریف

جرم در شریعت اسلام: «مخالفت با اوامر و نواهی کتاب و سنّت، یا ارتکاب عملی که به تباهی فرد و یا جامعه بینجامد». هنگامی که تعلیم و تربیت درست، به صورت جمعی صورت بگیرد؛ باعث خواهد شد که یک جامعه فرهنگ سایبری درست داشته باشد و لذا در دیدگاه پیشگیرانه بسیار قوی عمل کند و زمینه بسیاری از مشکلات اجتماعی بعدی پیش نیاید. جنبه بعدی که جنبه درمانی است، همواره از گام اول سخت‌تر و هزینه‌برتر است اما در بعضی جوامع به دلیل اغفال صورت‌گرفته گاه ممکن است که جامعه، اکثراً درگیر این بخش از جرایم سایبری در فضای جامعه باشد.

این اغفال گاه در زمینه علمی قابل بررسی است یعنی جامعه علمی کشوری همگام با سایر جوامع دنیا در زمینه‌های تکنولوژی سایبری پیش نمی‌رود و همین امر باعث می‌شود که یک تکنولوژی به جامعه‌ای وارد شود پیش از آنکه در کنار اثرات مفید و سودبخش؛ اثرات منفی و مضر آن بررسی شده باشد. گاه اغفال صورت گرفته در مرحله پیشگیری؛ یعنی اغفال در تعلیم و تربیت مناسب و اشاعه فرهنگ سایبری درست، باعث می‌شود که یک تکنولوژی به جامعه‌ای وارد شود و قشر کم تجربه‌تر یعنی جامعه کودک، نوجوان و جوان به سمت استفاده از نکات منفی این تکنولوژی سوق پیدا کند. لذا در این مرحله باز هم نگاه درمانی درست که می‌توان آن را در یک نگاه مبتنی بر تکنولوژی و نیز اخلاق دانست، راهگشاست.

در مجموع می‌توان گفت که با به‌روز بودن جامعه علمی یک کشور در تمامی عرصه‌های سایبری و نیز همکاری‌کردن آن‌ها با ساختار تعلیم و تربیت جامعه که شامل آموزش و پرورش، دانشگاه‌ها و نیز جوامع دینی می‌شود می‌توان از ورود جامعه به این عرصه جلوگیری کرد و همچنین تکنولوژی‌ای را در اختیار داشت که متناسب با معیارهای فرهنگی آن جامعه باشد. طبق اصول ۲۲و ۲۳و۲۵ قانون اساسی جمهوری اسلامی ایران هرگونه تعرض به آبرو و جان و مال و حقوق و مسکن و پیشه و عقاید و اطلاعات خصوصی افراد ممنوع اعلام شده است. تعریف حریم خصوصی را می‌توان اینگونه بیان نمود که حریم خصوصی از آن دست مفاهیمی است که همه آن را درک می‌کنند(شورای عالی انفورماتیک، شماره ۵۲: ۷۲). ولی از آنجا که نمی‌توان تعریف جامع و کاملی از آن ارائه کرد لذا در بسیاری از موارد ما شاهد نوعی تعارض و یا حتی چالش

در زمینه مسائل مربوط به حریم خصوصی هستیم لکن در مجموع می‌توان بیان نمود که حریم خصوصی یعنی فرد آزادانه حق داشته باشد در خلوت خود اطلاعات مربوط به امور زندگی‌اش را پنهان نموده، و بر آن کنترل و تسلط داشته باشد 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. در تعالیم دینی ما نیز به این موضوع اشاره شده که امام معصوم می‌فرماید چند چیز خود را از دیگران پنهان نما! اینکه چقدر مال داری؟ اینکه کجا می‌روی؟ و اینکه مشرب فکری و مذهبی شما چیست؟

نقض حریم خصوصی در فضای مجازی این موضوع یکی از مهم‌ترین مسائل روز جامعه ماست که از دو دیدگاه قابل بررسی است؛ یکی از جانب قربانیان نقض حریم خصوصی در این فضا و دیگری از سوی ناقضین حریم خصوصی در فضای مجازی... در این رابطه همیشه بزه دیدگان در این فضا نقش مهمی را در بروز جرائم ناقض حریم خصوصی ایفا می‌کنند. در عین حال می‌توانند در اقدامات پیشگیرانه علیه جرائم سایبری نقش آفرین باشند(Casey, 2001: 8).

بسیاری از بزه دیدگان جرایم سایبری و کسانی که حریم خصوصی آنان در فضای مجازی نقض می‌شود استعدادی قابل توجه برای قربانی‌شدن بروز می‌دهند و به راحتی طعمه بزهکاران سایبری می‌شوند برخی کلاهبرداری‌های اینترنتی ناشی از کسب اطلاعات به روش‌های ساده و سوء استفاده از عکس‌های شخصی نمونه‌هایی از این موضوع می‌باشد. ضعف شخصیتی، فقدان اطلاعات کافی در رابطه با محیط مجازی و عدم دقت در محافظت از داده‌ها و... مواردی است که قربانی بزه سایبری را در قربانی‌شدن‌اش مساعدت می‌کند. بسیاری از افراد بدون رعایت مسائل امنیتی خصوصی‌ترین اطلاعات خود را روی سیستم رایانه‌ای و تلفن همراه و... ذخیره می‌نمایند و به نوعی دست بزهکار سایبری را در تعرض به حریم خصوصی باز می‌گذارند؛ بنابراین می‌توان گفت که در فضای مجازی از اطلاعات شخصی و حریم خصوصی خود محافظت نمائیم تا مجبور نباشیم به دنبال مجرم بگردیم هرچند این مطلب به معنای توجیه عملکرد بزهکار سایبری نیست. یعنی اگر افراد در محافظت از حریم خصوصی خود کوتاهی نمایند دلیل بر این نیست که ما خود را مجاز به تعرض به حریم خصوصی افراد بدانیم جنبه دیگر

موضوع مربوط به ناقضان حریم خصوصی در فضای مجازی می‌باشد. این افراد زمانی که وارد فضای مجازی می‌شوند به خود اجازه هرگونه فعالیت و ورود به حریم شخصی دیگران را می‌دهند که به چند موضوع مهم و به روز جامعه می‌توان اشاره نمود که از جمله:

- دسترسی غیر مجاز به داده‌های رایانه‌ای یا مخابراتی مثل هک نمودن ایمیل
- شنود غیر مجاز مخابراتی
- نقض تدابیر امنیتی سیستم‌های رایانه‌ای
- مختل نمودن و یا تخریب داده‌های دیگری از سیستم‌های رایانه‌ای یا مخابراتی
- غیر فعال نمودن دیتا بیس و ممانعت از دسترسی افراد به سایت‌های شخصی
- هتک حرمت و حیثیت از طریق انتشار صوت و فیلم
- نشر اکاذیب از طریق سیستم‌های رایانه‌ای

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

اخلاق دینی، هم پشتوانه‌های استدلالی اخلاق کاربران را تحکیم می‌بخشد و هم ضمانت اجرای کارآمدی در اختیار قرار می‌دهد. شرط مکمل راهبرد فردی- اخلاقی جامعه پذیری دینی، تقویت روحیه خود دیگرپنداری، آشناسازی با پیامد منطقی رفتار کاربران و نهادینه سازی امر به معروف و نهی از منکر است.

تعریف حریم خصوصی

به زبان ساده می‌توان گفت حریم خصوصی از آن دست مفاهیمی است که همه آن را می‌فهمند و درک می‌کنند لکن نمی‌توانند تعریفی جامع و کامل از آن ارائه نمایند، لذا در بسیاری موارد ما شاهد نوعی تعارض و یا حتی چالش در زمینه مسائل مربوط به حریم خصوصی هستیم. به طور مثال زمانی سخن از نصب دوربین‌های مداربسته در کافی‌نت‌ها به میان آمده بود که مخالفین این طرح آن را معارض با حریم خصوصی اشخاص می‌دانستند و بعضی دیگر همچون نگارنده این مطلب آن را غیر مرتبط با حریم

خصوصی اشخاص تلقی می‌کردند(نیازپور، ۱۳۸۲: ۱۲۴). چنین اختلافاتی بعضاً ناشی از آن است که تعریف ترمینولژیکی از حریم خصوصی ارائه نشده است لکن در مجموع می‌توان بیان نمود: حریم خصوصی یعنی 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(صدیق بنای، ۱۳۸۹:۱۱).

نقض حریم خصوصی در فضای مجازی

تا اینجا دانستیم که انسان به حکم طبیعت و سرشت باید دارای حریم خصوصی برای خود باشد و از آن محافظت نماید در مقابل اشخاص بایستی نسبت به صیانت و رعایت حریم خصوصی سایرین اقدام نمایند. 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(نجفی ابرندآبادی، ۱۳۸۲: ۱۲۰۸).

بزه دیدگان در فضای مجازی نقش مهمی را در بروز جرایم ناقض حریم خصوصی ایفا می‌کنند و در عین حال می‌توانند در اقدامات پیشگیرانه علیه جرایم سایبری یا همان Cyber Prevention نقش‌آفرین باشند. بسیاری از بزه دیدگان جرایم سایبری و کسانی که حریم خصوصی آنان در فضای مجازی نقض می‌گردد، استعدادی قابل توجه برای قربانی شدن(Immolate) بروز می‌دهند و به راحتی طعمه بزهکاران سایبری می‌شوند. بعضی کلاهبرداری‌های اینترنتی ناشی از کسب اطلاعات به روش‌های بسیار ساده و سوء استفاده از عکس‌ها و اسرار شخصی نمونه‌هایی از این موضوع می‌باشد(نجفی ابرندآبادی، ۱۳۸۳: ۵۵۹).

ضعف شخصیتی، فقدان اطلاعات کافی در رابطه با محیط مجازی و عدم دقت در محافظت از داده‌ها و... مواردی است که قربانی بزه سایبری را در قربانی شدن‌اش مساعدت می‌کند. اشخاص بایستی نسبت به صیانت از حریم خصوصی خود همت نمایند، بسیاری اشخاص بدون رعایت مسائل امنیتی، خصوصی‌ترین اطلاعات خود را بر روی

سیستم رایانه‌ای و یا حامل‌های داده نظیر فلش و کارت‌های حافظه و تلفن همراه و سی‌دی و... ذخیره نماید و به نوعی دست بزهکار سایبری را در تعرض به حریم خصوصی باز می‌گذارند و اینچنین استعداد قربانی شدن در فضای مجازی را از خود نشان می‌دهند (معتمدنژاد، ۱۳۸۳: ۴۲).

مصادیق نقض حریم خصوصی در فضای مجازی

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 آن را "ملک طلق" خود دانسته و اجازه هرگونه فعالیت و ورود به حریم خصوصی دیگران را به خود می‌دهند. در زیر به بعضی مصادیق نقض حریم خصوصی در فضای مجازی که در قانون جرایم رایانه‌ای جرم انگاری شده است می‌پردازیم:

- دسترسی غیر مجاز به داده‌های رایانه‌ای یا مخابراتی نظیر هک ایمیل یا اکانت اشخاص
- شنود غیر مجاز محتوای در حال انتقال در سیستم‌های رایانه‌ای یا مخابراتی نظیر استفاده از نرم افزارهای شنود چت‌های اینترنتی
- دسترسی غیر مجازبه داده‌های سری در حال انتقال در سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده یا تحصیل و شنود آن
- در دسترس قرار دادن داده‌های سری در حال انتقال در سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده برای اشخاص فاقد صلاحیت
- نقض تدابیر امنیتی سیستم‌های رایانه‌ای یا مخابراتی به قصد دسترسی به داده‌های سری در حال انتقال در سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده
- حذف یا تخریب یا مختل یا غیر قابل پردازش نمودن داده‌های دیگری از سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده به طور غیر مجاز

- از کار انداختن یا مختل نمودن سیستم‌های رایانه‌ای یا مخابراتی به طور غیر مجاز نظیر غیر فعال سازی دیتابیس تارنماها و ممانعت از دسترسی اشخاص به پایگاه‌های اینترنتی شخصی
- ممانعت از دسترسی اشخاص مجاز به داده‌های یا سیستم‌های رایانه‌ای یا مخابراتی به طور غیر مجاز
- ربودن داده‌های متعلق به دیگری به طور غیر مجاز
- هتک حیثیت از طریق انتشار یافتن صوت و فیلم تحریف شده دیگری به وسیله سیستم‌های رایانه‌ای یا مخابراتی
- نشر اکاذیب از طریق سیستم‌های رایانه‌ای یا مخابراتی به قصد اضرار به غیر یا تشویش اذهان عمومی
- فروش یا انتشار یافتن یا در دسترس قرار دادن گذرواژه یا هر داده‌ای که امکان دسترسی غیر مجاز به داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتی متعلق به دیگری را فراهم می‌کند.
- آموزش نحوه ارتکاب جرایم دسترسی غیر مجاز، شنود غیر مجاز، 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 اشخاص وارد می‌سازند.

نقش دولت در پیشگیری از جرم نقض محرمانگی داده‌ها در فضای مجازی

۱.مجازات‌های ورود به حریم خصوصی افراد در فضای مجازی

در اصولی نظیر ۱۹-۲۰-۲۲-۴۰ و ۴۲ قانون اساسی جمهوری اسلامی ایران هرگونه تعرض به آبرو جان، مال، حقوق، مسکن، عقائد، پیشه و اطلاعات خصوصی افراد ممنوع اعلام شده است. همچنین در قانون جرائم رایانه‌ای و مصادیق محتوای مجرمانه در فضای

مجازی حریم خصوصی مورد تأکید و مجازات‌های متفاوتی برای اخلال 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 که هر کس به طور غیر مجاز به داده‌ها با 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 قانون جرائم رایانه‌ای 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 و اگر کسی به طور غیر مجاز داده‌های شما را از سیستم رایانه‌ای شما حذف یا تخریب یا غیر قابل 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 می‌شوند. همچنین اعمالی مانند واردکردن، انتقال دادن، پخش کردن، 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 گذرواژه‌ها 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. برابر ماده ۱۲ قانون جرائم رایانه‌ای و مصادیق محتوای مجرمانه در فضای مجازی این افراد به جزای نقدی از یک تا بیست میلیون ریال و در غیر این صورت به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج تا بیست میلیون ریال یا هر دو مجازات محکوم خواهند شد. البته در این میان قانون درباره هتک حرمت اینگونه برخورد کرده است و هر کس 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 دو مجازات مقرر محکوم

می‌شود. اگر حریم شما نقض شد و یا به حریم خصوصی شما تعدی صورت گرفت راهکار آن در قدم اول در جریان قرار دادن پلیس فتا می‌باشد که این پلیس به طور تخصصی به بررسی جرائم اینترنتی می‌پردازد، دادسرای مبارزه با جرائم رایانه‌ای نیز محل مناسبی برای طرح شکایت و احقاق حق می‌باشد، و اینکه جرائمی مثل نفوذ به اطلاعات شخصی و تهدید به افشا و انتشار که آگهی‌های کلاهبرداری اینترنتی، خرید و فروش کالاهای غیر مجاز اینترنتی، فعالیت اقتصادی مجرمانه نظیر شرکت‌های هرمی، تهیه و توزیع اینترنتی مواد مخدر و قرص‌های روانگردان، انجام جاسوسی اینترنتی روی فرد خاص، ایجاد اخلال در سیستم‌های رایانه‌ای شخص حقیقی و یا حقوقی و کلاهبرداری و اغفال از طریق جادوگری، رمالی، کف بینی اگر در بستر فضای مجازی شکل بگیرد.

همچنین تبلیغ و فروش محصولات جنسی نامشروع و غیر مجاز، جرائمی است که می‌توان به دادسرای مبارزه با جرائم رایانه‌ای مراجعه کرد. در پایان از این مبحث نتیجه گرفته می‌شود که حفظ حریم خصوصی هر شخص در فضای مجازی توسط کاربران الزامی بوده و سعی بر آن باشدکه در حفظ و نگهداری این فضا اقدامات حفاظتی کامل صورت پذیرد تا ناقضین بر این فضا حتی به خود اجازه ورود به آن را ندهند(دزیانی، ۱۳۸۴: ۷).

۲.مراجع رسیدگی به جرم نقض محرمانگی داده‌ها در فضای مجازی

یادتان باشد اگر به هر طریقی در فضای مجازی به حریم خصوصی شما تعدی شد راهکار بسیار ساده است. در قدم اول شما می‌توانید به پلیس فتا مراجعه کنید. این پلیس به طور تخصصی به بررسی جرایم اینترنتی می‌پردازد. دادسرای مبارزه با جرایم رایانه‌ای نیز محل مناسبی برای طرح شکایت و احقاق حق‌تان است. یادتان باشد نفوذ به اطلاعات شخصی و تهدید به افشا و انتشار آن، انتشار آگهی‌های کلاهبرداری اینترنتی، خرید و فروش کالاهای غیر مجاز اینترنتی، فعالیت اقتصادی مجرمانه نظیر شرکت‌های هرمی، تهیه و توزیع اینترنتی مواد مخدر و روانگردان‌ها، انجام جاسوسی اینترنتی روی فرد خاص، ایجاد اخلال در سیستم‌های رایانه‌ای شخص حقیقی یا حقوقی، کلاهبرداری و اغفال از طریق جادوگری، رمالی، کف‌بینی و... اگر در بستر فضای مجازی شکل بگیرد.

همچنین تبلیغ و فروش محصولات جنسی نامشروع و غیر مجاز، مواردی است که کاربران محترم به محض مواجه شدن با آن‌ها باید به دادسرای مبارزه با جرایم رایانه‌ای مراجعه کنید(دزیانی، ۱۳۷۶: ۷۴).

روش‌های پیشگیری از جرم نقض محرمانگی داده‌ها در فضای مجازی

۱.روش‌های ملی و بین المللی

توماس بابینگتون می‌گوید: «بهترین ملاک ارزیابی شخصیت یک فرد این است که ببینیم در هنگامی که می‌داند هیچ کس از هویت او باخبر نمی‌شود، چه کارهایی انجام می‌دهد»(Berson,2004). این جمله بسیار زیبایی است، خصوصاً وقتی از منظر یک شهروند به آن نگاه کنیم. محیط مجازی به افراد این امکان را می‌دهد تا به صورت ناشناس فعالیت کنند، شاخصه‌ای که در محیط فیزیکی کم‌تر با آن مواجه هستیم. همین فعالیت ناشناس زمینه را برای مواجهه با مسائلی جدید در قالب شهروندی مجازی مهیا می‌کند. جوانان تصور می‌کنند که در فضای مجازی می‌توانند به صورت ناشناس فعالیت کنند و هیچ عواقبی نیز در انتظار فعالیت‌های نامشروع و غیر قانونی آن‌ها نیست و بعضاً شاهد اعمالی هستیم که از آن‌ها در محیط اجتماع سر نمی‌زند(همان).

در دنیای تکنولوژی‌های جدید و اینترنت، تعداد رو به رشدی از افراد برای تقریباً تمام امور زندگی خود وابسته به اینترنت هستند و این حتی شامل رابطه شهروندان با دولت نیز می‌شود چراکه دولت زیرساخت‌های فنی لازم برای استفاده‌های گوناگون از اینترنت را در دست داشته و در نتیجه قدرت زیادی نیز در اختیار دارد. در واقع می‌توان گفت که تکنولوژی‌های شبکه‌ای به دولت‌ها و شهروندان در سراسر دنیا قدرت داده‌اند. مثلاً کشور چین نمونه کشوری است که دولت از قدرت اعمال سانسور و نظارت بالایی بر روی شهروندان برخوردار است. به نظر *ربکا مک کنین* در سلسله گزارش‌ها و مقالات‌اش درباره شهروندی اینترنتی، این مورد در کشور چین به خاطر عدم احاطه شهروندان بر حقوق خود در فضای مجازی و عدم تلاش برای احقاق حقوق‌شان است. او عنوان می‌کند که این نمونه نه‌تنها درسی برای خود چینی‌هاست بلکه برای هر کسی است که هر جای دنیا از اینترنت استفاده می‌کند. اگر ما می‌خواهیم تا حقوق‌مان حفظ شود دیگر تنها احاطه بر

حقوق شهروندی در محیط فیزیکی کافی نیست بلکه بایستی اصول شهروندی مجـازی را نیز یاد بگیریم، تمرین کنیم(Mackinnon, 2012).

در واقع مسأله قدرت مجازی همانند فضای فیزیکی بایستی به تـوازن برسـد و تحـت کنترل قرار گیرد تا از هرگونه دستکاری و سوء اسـتفاده مصـون بمانـد و ایـن بسـته بـه انتخاب هر فردی است که به نوعی از تکنولوژی و به ویژه اینترنت اسـتفاده مـی‌کنـد. تـا زمانی‌که ما از تصمیماتی که در اطراف‌مان گرفته می‌شود آگاهی نداشته باشـیم و کـاری در قبال آن‌ها نکنیم، آزادی و حریم خصوصی‌مان در خطر است. *مک کنین* معتقد اسـت که ۳ اهرم قدرت در فضای مجازی وجود دارد: دولت، شرکت ها و شهروندان الکترونیـک (همان). در شرایط امروزی، قدرت شهروندی مجازی بایستی توانمند شود تا توازن میـان این سه قدرت برقرار شود(United Nations, 1992). ما می‌دانیم که شرکت‌ها و دولت‌هـا در فضای مجازی قدرت زیادی دارند. بنابراین ما باید جنبش شـهروندی مجـازی داشـته باشیم که اولاً افراد را از حقوق‌شان آگاه کند و ثانیاً با ایجاد امکانات دسترسی بـه فضـای مجازی جدای از مجرای دولت امکان بیش‌تری برای فعالیت و خلاقیت افراد در این فضـا ایجـاد کنـد(Usdoj, 2002: 52). اقـدامات لازم بـرای ایجـاد محـیط مجـازی مناسـب فعالیت‌های شهروندی در دو سطح است: اول اموری که مربـوط بـه دولـت‌هاسـت و دوم اموری که در ارتباط با شرکت‌ها است:

در سطح کشور-دولت: ما به عنوان شهروندان اینترنتی باید این درخواست‌هـا را از دولت ملی داشته باشیم:

- تمامی قانونگذاری‌های مربوط به اینترنت بایستی هم‌گام با قواعد جهانی آزادی بیان و حریم خصوصی باشد. به عبارت دیگـر قـوانینی کـه در جهـت حـل مسـائلی همچـون استثمار کودکان و جرائم هستند نباید متکی بر راه حل‌هایی باشند که ممکن است منجر به حذف امکان شهروندان در استفاده از زیرساخت‌های دیجیتال در کاربردهای معقـول و منطقی مانند مشارکت سیاسی شود(حسینی، ۱۳۸۲: ۷۵).

- دولت بایستی متعهـد شـود تـا در زمینـه چگـونگی اعمـال سانسـور و نظـارت بـر شرکت‌هـای ارائـه کننـده زیرسـاخت‌هـای تکنولوژیـک، و شـبکه‌هـایی کـه ارتباطـات و خلاقیت‌های ارتباطی ما را مهیا می‌کنند، شفاف عمل کند.

در سطح شرکت‌ها: به عنوان شهروندان الکترونیک باید نظارت خصوصی بـر فضـای مجازی را ترغیب و تشویق کنیم تا به حقوق ما احترام بگذارنـد(جلالی فراهـانی، ۱۳۸۴: ۱۰۹).

- به عنوان استفاده یا مصرف کننده‌های شرکت‌های ارائه دهنده سرویس، شـهروندان اینترنتی باید بخواهند تا شرکت‌ها چگونگی اشتراک اطلاعات خود را با دولت‌هـا و پاسـخ به نیاز های سانسوری آن‌ها را افشا کنند.

- شهروندان اینترنتی می‌توانند اتحادیه استفاده کنندگان یا مشتریان را تشکیل دهند تا درگیر مسائل شرکت‌ها شده و مطمئن شوند که فعالیت‌های تجاری شرکت‌هـا آسـیبی به حقوق سیاسی و شهروندی آن‌ها در فضای مجازی وارد نمی‌کند.

- شرکت‌هایی که موافق استانداردهای پایه‌ای آزادی بیان و حریم خصوصی هستند و همچنین موافق این هستند که رعایت این اسـتانداردها توسـط یـک ارگـان ثالـث مـورد ارزیابی قرار بگیرد، باید توسط مشتریان، استفاده کنندگان و سرمایه گذاران مورد تشویق قرار بگیرند و شرکت‌هایی که مخالف این موضوع هستند و حریم خصوصی شـهروندان را نقض کرده و حقوق آن‌ها را رعایت نمی‌کنند بایستی عواقب کار خود را به طریقی ببینند (Mackinnon, 2012).

۲.راهکارهای فردی و اخلاقی

با توجه به چالش‌های یادشده بر سر راه اقدامات حکومتی و بین المللی بـرای کنتـرل جرایم سایبری، مؤثرترین اقدام، مراعـات کـردن مسـائل ایمنـی و اخلاقـی توسـط خـود کاربران است. در این روش که به روش «کنترل فردی» موسوم است، تمام تضـمین‌هـای اجرایی، درون فردی بوده و شخص با بهره گیری از وجدان فردی و مبانی اخلاقی و تعهد دینی، مراقبت‌های لازم را در خصوص طرز استفاده از شبکه‌های جهانی به عمل می‌آورد. اهمیت این روش در مقایسه با دیگر روش‌ها این است که در سطوح مختلف زندگی قابل اعمال بوده و ظرفیت تأثیرگذاری بر اطرافیان کاربر را نیز دارد.

با توجه به کارآمدی این روش، کشـورهای پیشـرفته در کنـار اقـدامات بـین المللـی، اجرای اصول اخلاقی را یکی از راه‌های مفید برای کنترل جرایم در نظر گرفته‌اند. یکی از

موارد عملی تدبیر اخلاقی، نهادینه شدن اصول اخلاقی روزنامه نگاری است که بر اساس آن کشورها سعی می‌کنند در گزارش‌های خبری خود به اصولی به عنوان اصول اخلاقی توجه نمایند. نمونه دیگر، منشور اخلاقی رایانه است که در سال ۱۹۹۲م توسط انجمن ماشین آلات رایانه تأیید شده و ۲۴ فرمان و رهنمود اخلاقی در آن ذکر شده است. اقدام فردی که به جهت گیری اخلاقی افراد وابسته است و با باورهای دینی پشتیبانی می‌شود، راه حل مطمئن و کم هزینه‌تری در مقایسه با سایر تمهیدات است.

۳.فضای سایبر و اخلاق سکولار

اخلاق سکولار بنیان نظری خودش را بر توجیه پذیری اخلاق بدون اعتقادات دینی استوار می‌سازد. در اخلاق سکولار، ارزش‌های مادی و انسانی، نظیر خوشی، امنیت، هنر و عشق تعاون انسانی، امری بنیادین برای زندگی خوش به عنوان غایت زندگی اخلاقی در نظر گرفته می‌شود. معیارهای توجیه در اخلاق سکولار «لذت»، «سود»، «قدرت»، «تمایل انسانی» و «انتخاب فردی» است؛ مفاهیمی که در صدد است انسان را در توجیه اخلاق از وابستگی به منبع فرا انسانی بی نیاز سازد.

اخلاق سکولار علاوه بر مشکلات توجیهی، معرفتی و هنجاری‌ای که دارد، در کنترل هنجارشکنی‌های اخلاقی در فضای مجازی موفق نخواهد بود، زیرا معیارهای یادشده برای اخلاق سکولار به سبب نسبیت دستوری و هنجاری که همراه دارد، خود مبدأی برای توجیه، تقویت و فراگیرسازی تعاملات غیر هنجارمند است.

۴.اخلاق دینی در تعاملات سایبری

باورها و ارزش‌های دینی یکی از محرک‌های درونی است که فرد را به رفتار درست و هنجارمند سوق می‌دهد. اخلاق دینی، هم نقش تحریکی برای رفتار اخلاقی دارد و هم نقش بازدارنده برای رفتار غیر اخلاقی، از این رو اخلاق دینی، هم در فضای واقعی زندگی ما نقش‌های تحریکی و کنترلی ایفا می‌کند و هم در فضای مجازی. محوری‌ترین عنصر در تهذیب اخلاق «مراقبت» است. مراقبت در علم اخلاق به معنای خودکنترلی مستمر و محافظت دائم از رفتارهای ظاهری و باطنی است. حضور عنصر مراقبت در اخلاق نشانه این است که اخلاق از طریق توانمندسازی افراد با خودبازدارندگی به اهداف خود نایل

می‌شود. اکنون به تناسب تحقیق باید بررسی کرد که چگونه می‌توان کاربران و اهالی دهکده سایبر را به قدرت خودکنترلی و مراقبت توانمند ساخت؟ برای پاسخ به این سؤال، سزاوار است که درباره خاستگاه کم توجهی افراد به دستورات و رهنمودهای اخلاقی، کاوش کرده و در پی آن، دستاوردهای دین در این زمینه بررسی شود

۵.قرآن

در آیات و روایات متعدد، بر اجازه گرفتن برای ورود به منزل دیگران، تأکید شده است. از آن جمله است آیه ۲۴ سوره نور که خداوند می‌فرماید:

﴿یاأیها الذین آمنوا لا تدخلوا بیوتاً غیر بیوتکم حتی تستأنسوا﴾

«شما که ایمان دارید به خانه هیچ کس غیر از خانه‌های خود داخل نشوید تا آنکه اجازه ورود بگیرید»

این اجازه ورود، به این خاطر است که خداوند، منزل افراد را حریم خصوصی آنان دانسته؛ چراکه افراد در آن باید احساس امنیت کنند نه آنکه هر کسی هر وقت دل‌اش خواست، وارد منزل آن‌ها شود. همچنین، خداوند حفظ این حریم خصوصی را برای همه واجب کرده است. این حکم استیذان، یک حکم اخلاقی است که از اصول حفظ حریم خصوصی دیگران است. حفظ حریم خصوصی دیگران، فقط به ورود بدون اجازه به منزل چهاردیواری افراد متوقف نیست. امروزه می‌توان به خیلی از مکان‌ها، منزل گفت: مثلاً کسی که در پارکی چادری زده، آن چادر منزل اوست؛ یعنی مکانی است که او برای خود اختیار کرده و خود را در آن ایمن می‌داند، در صورتی که زمین آن مکان به ملکیت او نرسیده ولی همه انسان‌ها آنجا را منزلی برای او می‌دانند، لذا هیچ کس بدون اجازه وارد آن نمی‌شود. در عصر حاضر، که عصر پیشرفت تکنولوژی است، کامپیوتر و موبایل شخصی به مثابه نازل انسان‌هاست که تمام اطلاعات و ارتباطات شخصی و خانوادگی خود را در آن می‌ریزند. کاربران این دو دستگاه را مانند منزل خود، فضایی امن تلقی کرده‌اند که اطلاعات و ارتباطات مهم خود را در آن ذخیره می‌کنند. همین حس امنیت است که وجه اشتراک منزل افراد با کامپیوتر و موبایل افراد بوده و حریم خصوصی را به وجود می‌آورد؛ بنابراین

ورود به این دو دستگاه از هر طریق، مصداق ورود بدون اجازه به حریم خصوصی دیگران بوده و امری غیر اخلاقی است.

نتیجه بحث

با توجه به آنچه گذشت، فضای سایبر(اینترنت) در کنار دستآوردها و کاربردهای انکارناپذیر و مثبتی که در زمینه‌های گوناگون دارد، پیامد نامطلوبی نیز به همراه دارد که باید مورد توجه والدین، مربیان و همه مسئولان امر تعلیم و تربیت و برنامه‌ریزان فرهنگی جامعه قرار گیرد.حریم خصوصی افراد آنقدر اهمیت دارد که احترام به آن در قرن حاضر از مرزهای سنتی دین و اخلاق فراتر رفته و در بیش‌تر کشورهای جهان ضمانت قانونی پیدا کرده است؛ اما شئون انسانی و اهمیت حفظ آن در فضای مجازی و امنیت اطلاعات مبادله‌شده با چالش‌هایی مواجه شده و سلامت اخلاقی و حتی جسمانی کودکان و نوجوانان در جامعه به مخاطره افتاده است. اکثر والدین نیز به دلیل عدم آشنایی با اینترنت و ظرفیت‌های آن و شبکه‌های اجتماعی فضای مجازی و فنآوری نوین ارتباطی، از رفتارهای آنلاین فرزندان‌شان در فضای مجازی اطلاعی ندارند.

همین مسأله راه را برای صیادان اینترنتی باز می‌کند تا راحت‌تر بتوانند وارد حریم خصوصی خانواده شوند. اینترنت ابزاری مناسب برای توسعه افکار و اندیشه‌های بشری محسوب می‌شود به شرط آنکه در راه صحیح استفاده شود. افراد باید برای ورود به دنیای مجازی، اطلاعات کافی در اختیار داشته باشند تا دچار مشکلات اخلاقی، اجتماعی و اقتصادی نشوند.

ارتباطات سالم در فضای مجازی و لزوم هوشیاری جوانان و خانواده‌ها نسبت به تهدیدات فضای سایبری در درجه نخست اولویت قرار دارد. پیشگیری از آسیب‌های اخلاقی و اجتماعی و توجه والدین به رفتار فرزندان بسیار مهم است و برای جلوگیری از فروپاشی خانواده‌ها، والدین باید تا حدودی به فنآوری‌های روز دنیا مسلط باشند و بدانند که تغییر در رفتار فرزندان به معنای ایجاد تغییر در طرز فکر آن‌هاست و هنگامی که بنیان فکری و شخصیت آن‌ها به صورت ناصحیح شکل گیرد، راه نفوذ شیادان به حریم خصوصی افراد و محیط امن خانواده باز می‌شود؛ لذا چنانچه خانواده‌ها نسبت به

شیوه‌های جدید ارتباط فرزندان، خودآگاهی و شناخت کافی و لازم را داشته باشند، از بروز بسیاری از آسیب‌ها جلوگیری به عمل می‌آید. اینترنت به خودی خود، ابزاری بی‌طرف و خنثی است؛ اما اینکه اکنون مردم چگونه از آن استفاده می‌کنند، تعیین‌کننده است.

اگر استفاده مناسب و مثبت باشد، در جهت توسعه جامعه حرکت خواهد کرد، وگرنه مشکلات عمده‌ای را برای خانواده و اعضای آن به وجود می‌آورد؛ به عبارت دیگر، شبکه جهانی اینترنت یک شبکه اطلاعاتی سریع با منابع بی‌شمار است که استفاده نادرست و بیش از حد از آن در بین برخی از افراد و غرق شدن در دنیای رایانه و جدایی از دنیای واقعی، فواید آن را به آسیب تبدیل می‌کند. به طوری که هم‌اکنون استفاده نادرست از این ابزار در میان کاربران، در جوامع پیشرفته چنان گسترش یافته است که از آن به عنوان یک بیماری مدرن نام می‌برند که محصول عصر ارتباطات و انقلاب رایانه‌ای است.

باید دانست که فیلتر کردن هرچند لازم است و به طور موقت می‌تواند جلوی سوء استفاده از اینترنت را بگیرد، ولی آنچه در شرایط کنونی لازم است و باید دولت روی آن سرمایه‌گذاری کند، ایمن‌سازی، تقویت باورهای دینی و بارور کردن روحیه تقوا و خودداری است. تنها در این صورت است که فرهنگ استفاده درست از اینترنت در جامعه نهادینه و از آسیب‌های اخلاقی آن جلوگیری می‌شود.

برای جلوگیری از آثار و پیامدهای منفی فضای اینترنت در تربیت دینی فرزندان، به والدین پیشنهاد می‌شود:

۱. بر نحوه استفاده فرزندان از اینترنت، نظارت فعال داشته باشند؛

۲. همراه با کودکان از اینترنت استفاده نمایند و درباره مطالب آن با آن‌ها صحبت کنند؛

۳. کودکان را تشویق کنند که از میان انواع موضوعات و مطالب موجود در اینترنت، دست به انتخاب صحیح بزنند؛

۴. محدود کردن استفاده از اینترنت را برای کودکان در نظر داشته باشند؛

۵. از قرار دادن رایانه در اتاق‌های شخصی فرزندان و پشت درهای بسته بپرهیزند؛

۶. مسئولان و نهادهای فرهنگی- اجتماعی نیز وظیفه دارند فرهنگ استفاده درست و سالم از اینترنت را به افراد جامعه به ویژه جوانان و نوجوانـان کـه بـیش‌تـر در معـرض آسیب‌های اخلاقی اینترنت هستند، آموزش دهند.

کتابنامه

دزیانی، محمد حسن. ۱۳۷۶ش، **جرائم کامپیوتری**، جلد اول، تهران: دبیرخانه شورای عالی انفورماتیک.

معتمدنژاد، کاظم. ۱۳۸۳ش، **وسایل ارتباط جمعی**، جلد نخست، تهران: انتشارات دانشگاه علامه طباطبایی.

نجفی ابرندآبادی، علی حسین. ۱۳۸۲ش، **تقریرات درس جرم‌شناسی(پیشگیری)**، دوره کارشناسی ارشد حقوق کیفری و جرم‌شناسی، تنظیم مهدی سیدزاده، نیم‌سال دوم تحصیلی ۸۲-۱۳۸۱.

نجفی ابرندآبادی، علی حسین. ۱۳۸۳ش، **پیشگیری عادلانه از جرم، علوم جنایی**، مجموعه مقالات در تحلیل از استاد آشوری، تهران: انتشارات سمت.

کتب انگلیسی

Berson, M. J., & Berson, I. R. (2004). Developing Thoughtful" Cybercitizens". Social Studies and the Young Learner, 16(4), 5-8.

Casey, Eoghan, 2001, Digital Evidence and Computer Crime, Academic Press.

MacKinnon, R. (2012). Consent of the networked: The worldwide struggle for Internet freedom. Politique étrangère, 50, 2.

MacKinnon, R. (2012). The Netizen. Development, 55(2), 201-204.

Sieber,u.1995, Computer Crime and Criminal Information Law - New Trends in the International Risk and Information Society.

T.Kent, Stephen and I. Millett Lynette, 2804, Who goes There? Authentication Through the Lens of Privacy, National Academy Press.

Thomburgh, Dick & s, Lin Herbert, 2004, Editors, Youth, Pornography and The Internet, National Academy Press.

United Nations, 2004, Office on Drugs and Crime; the Global Program a gainst Corruption; UN Anti-Corruption Toolkit; Third Edition; Vienna; September

مقالات و پایان‌نامه‌ها

ابراهیمی، شهرام. ۱۳۸۳ش، «**پیشگیری از جرم**».

حسن بیگی، ابراهیم. ۱۳۸۲ش، «**آسیب‌شناسی شبکه جهانی اطلاع‌رسانی اینترنت و ارائه راهبردهای مناسب جهت مقابله با تهدیدها از دیدگاه امنیت ملی با تأکید بر جنبه‌های حقوقی و فنی**»، پایان‌نامه دکتری، دانشگاه عالی دفاع ملی.

حسینی، بیژن. ۱۳۸۲ش، «**جرائم اینترنتی علیه اطفال و زمینه‌های جرم‌شناسی آن**»، پایان‌نامه مقطع کارشناسی ارشد، دانشگاه آزاد اسلامی، واحد علوم تحقیقات.

حلالی فراهانی، امیرحسین. ۱۳۸۴ش، «**پول‌شویی الکترونیکی**»، فصلنامه فقه و حقوق، شماره ۴.

حلالی فراهانی، امیرحسین. ۱۳۸۴ش، «**پیشگیری وضعی از جرایم سایبر در پرتو موازین حقـوق بشر**»، فصلنامه تخصصی فقه و حقوق، شماره ۶.

دزیانی، محمد حسن. ۱۳۸۳ش، «**مقدمه‌ای بر ماهیت و تقسیم‌بندی تئوریک جرائم کـامپیوتری (سایبری)**»، خبرنامه انفورماتیک، شماره ۸۷.

دزیانی، محمد حسن. ۱۳۸۴ش، «**شروع جرائم کامپیوتری- سایبری**»، خبرنامه انفورماتیک، شـماره ۹۳.

صفاری، علی. ۱۳۸۰ش، «**مبانی نظری پیشگیری وضعی**»، مجله تحقیقات حقوقی، شماره ۲۴- ۳۳.

نیازپور، امیرحسین. ۱۳۸۳ش، «**پیشگیری از بزهکاری در قانون اساسی و لایحـه پیشـگیری از وقوع جرم**»، مجله حقوقی دادگستری، شماره ۴۵.

منابع اینترنتی

صدیق بنای، هلن، ۱۳۸۹، سایبر اسپیس، پایگاه اینترنتی آفتاب.

Norway 2011 attacks. (2013, October 13). In **Wikipedia, The Free Encyclopedia**. Retrieved 18:51, November 6, 2013, from http://en.wikipedia.org/w/index.php?title=2011_Norway_attacks&oldid=577006658

خرم‌آبادی، بعدالصمد، ۱۳۸۸، طبقه‌بندی جرائم رایانه‌ای

http://adl-e-adel.blogfa.com/post-105.aspx

نایب، مهرداد، ۱۳۸۸، امنیت شبکه چیست؟

http://ittop.ir/thread3981.html