فصلنامه بین المللی قانون یار
License Number: 78864 Article Cod:2021S5D17SH9926445 ISSN-P: 2538-3701

بررسی علل و انگیزه ارتکاب به جرایم اینترنتی و راه های پیشگیری از آن

(تاریخ دریافت ۱۳۹۹/۰۹/۱۵، تاریخ تصویب ۱۴۰۰/۰۱/۱۸)

احمد بیرامیان

چکیده

اینترنت علی رغم تمامی امکانات و اطلاع رسانی در عزم بین المللی که برای ما به ارمغان آورده است ولی متأسفانه بعضی از افراد سودجو و فرصت طلب با فرا گرفتن مهارت و دانش لازم راه های ورود به سیستم های کامپیوتری دولتی و خصوصی و ... را به دست آورده اند که موجب بروز مشکلات و خسارات فراوانی گردیده است و با توسعه و تحول اینترنت ، در مقابل انقلاب عظیمی در ایجاد جرایم در سطح بین المللی بوجود آمده است . لذا در بیشتر کشورهای دنیا جرایم اینترنتی بعنوان یک معضل حاد و بسیار مهم تلقی می گردد و دولتها در صدد پیدا نمودن راه حل های مختلفی در جهت جلوگیری از وقوع آن می باشند. پلیس جنایی فدرال آلمان نیز تعریفی از جرائم رایانه ای ارائه داده که عبارت است از: «جرم رایانه ای دربرگیرنده همه اوضاع، احوال و کیفیاتی است که در آن شکل‌های پردازش الکترونیک داده‌ها، وسیله ارتکاب یا هدف یک جرم قرار گرفته است و مبنایی برای نشان دادن این ظن است که جرمی ارتکاب یافته است». همچنین به‌موجب نظر وزارت دادگستری آمریکا «هرگونه عمل ناقض قانون کیفری که مستلزم آشنایی با دانش مربوط به تکنولوژی کامپیوتر جهت ارتکاب عمل، تعقیب یا رسیدگی به آن باشد، جرم رایانه ای است» نهایتاً در این مقاله قصد داریم به بررسی علل و انگیزه ارتکاب به جرایم اینترنتی و راه های پیشگیری از آن بپردازیم .

واژگان کلیدی: فضای مجازی، اینترنت، جرایم کامپیوتری، جرم سایبر، نکنولوژی کامپیوتر

بخش اول: بررسی و ویژگی های جرایم کامپیوتری

جرایمی که توسط کامپیوتر یا شبکه و یا علیه آنها انجام می شود از ویژگی های متمایزی نسبت به جرایم کلاسیک دارند.چرا که ماهیت این گونه جرایم به دلیل تکنولوژی پیچیده و بالا،خصوصیات منحصر به فردی داشته که می توان به شیوه ارتکاب آسان، خسارات و ضررهای هنگفت با حداقل منابع و هزینه ، عدم حضور فیزیکی در محل ارتکاب جرم ،عدم شناسایی جرایم در برخی موارد ،خصوصیت فراملی بودن و وسعت دامنه جرم را نام برد.

الف-خصوصیات مرتکبین جرایم کامپیوتری معمولا مرتکبین جرایم کامپیوتری در دو دسته از هم قابل تمایز هستند.مرتکبین اتفاقی و مجرمین واقعی.دسته اول معمولا شامل جوانانی می شوندکه به انگیزهٔ بازی و تفنن مرتکب جرایم رایانه ای می شوند.ارتکاب این جرایم از آنجایی که منعکس کننده معایب سیستم ها و نحوهٔ نفوذ پذیری به شبکه و سیستم های کامپیوتری است لذا اتخاذ تدابیر پیشگیرانهٔ امنیتی مفید است.جرایم خطرناک و جدی که موجب خسارات مالی هنگفت می گردد از سوی مرتکبینی که دارای تخصص فنی یا تحصیلات دانشگاهی هستند وقوع می یابند که این دسته از مجرمین را باید جدی گرفت.در یک سری از جرایم کامپیوتری انگیزه اصلی کسب منفعت مالی است و لیکن انگیزه های دیگری چون انتقام جویی شغلی،سرگرمی،اثبات برتری قدرت،خودنمایی، چالش و... وجود دارد.لذا یکی از وجوه تمایز مرتکبین جرایم کامپیوتری از یکدیگر نوع انگیزه آنان می باشد .بر این اساس سه گروه از مجرمین از یکدیگر شناخته شده اند.مزاحمان کامپیوتری،خلافکاران ،خرابکاران.انگیزه گروه اول صرفا دستیابی به سیستم های کامپیوتری و اطلاعات موجود در آن می باشد و اکثراً نوجوانانی هستند که برای تفریح و سرگرمی و ارضای حس برتری جوئی است که دست به این اقدامات می زنند.انگیزه دسته دوم یعنی خلافکاران کسب منفعت مالی است و عمدتاً در دو مقوله ی جاسوسی و کلاهبرداری فعالیت دارند که روز به روز بر تعداد اینها در جهان افزوده می شود.و انگیزه گروه سوم تنها صدمه زدن و ایراد خسارات به دیگران است که نه به قصد کسب منفعت و نه سرگرمی و تفریح می باشند.بلکه افرادی هستند که دارای اختلالات

روانی بوده ویا قصد انتقام جویی دارند.این گروه در اجتماع و در اذهان عمومی مردم جایگاه چندان نامطلوبی ندارند و از مقبولیت بیشتری برخوردارند و چه بسا به عنوان یک قهرمان و یا بزرگترین بزهکاری کامپیوتری سال در تمام دنیا مشهور شده و نامشان زبانزد عام می شود.[1]

ب: ملموس نبودن جرایم کامپیوتری و عدم تخمین میزان جرایم ارتکابی با افزایش و بکار گیری کامپیوتر در تمام عرصه های زندگی و همچنین سهولت استفاده از آن و گسترش شبکه جهانی اینترنت امروزه جرایم کامپیوتری می تواند به وسیله هر کسی در هر نقطه ای از دنیا به وقوع بپیوندد.ملموس نبودن جرایم کامپیوتری مبتنی بر چند عامل می باشد.اول آنکه تکنولوژی پیشرفته یعنی ظرفیت حافظه ی فشرده کامپیوتر و سرعت بالای عملیات موجب کشف دشوار جرایم کامپیوتری است.دوم آنکه به دلیل عدم وجود سابقه و شناخت در خصوص جرایم کامپیوتری بزه دیدگان و مامورین اجرای قانون پس از مدتی متوجه وقوع جرم می شوند و دسته آخر اینکه بسیاری از بزه دیدگان توان تشخیص،پیشگیری و مقابله با حوادث مربوط به اینگونه جرایم را ندارند.از طرف دیگر مرتکبین زبده،غالبا از خود مدرکی به جای نمی گذارند. چون اطلاعات نسخه برداری می شوند بدون آنکه از محل خود برداشته شود و سوابق عمل هم قابل پاک شدن است .بخش جرایم کامپیوتری سازمان اطلاعات آمریکاFBIتخمین زده که بین ۸۵ تا ۹۵ درصد جرایم کامپیوتری حتی کشف نمی شوند.[2]

ج-فراملی و بین المللی بودن جرایم کامپیوتری و الکترونیکی جرایم کامپیوتری به دلیل ماهیت و تکنولوژی خاص ،اختصاص به محیط فیزیکی معین و محدودی ندارد و به راحتی در مقیاس بین المللی قابل تحقق می باشد.مسافت،زمان و مکان مانعی برای آن به حساب نمی آید .حضور فیزیکی شخص در محل حادثه معنایی ندارد .با کمک کامپیوتر و از طریق اینترنت سرقت از یک بانک یا دستیابی به اطلاعات محرمانه نظامی در ظرف چند ثانیه امری بعید و دور از دسترس نمی باشد.از طریق دسترسی به سیستم کامپیوتری در کشور و یا در کل

[1] شریفی، مرسده، جرایم رایانه ای در حقوق جزای بین المللی، پایان نامه کارشناسی ارشد، دانشگاه آزاد اسلامی واحد تهران، ۱۳۸۹،ص۶۸

[2] فضلی، مهدی، مسوولیت کیفری در فضای سایبر، انتشارات خرسندی، چاپ اول، تهران ۱۳۸۹،ص۸۷

کشورهای دنیا،این امکان را به کاربر غیر مجاز اینترنت می دهد که به راحتی به بانک های اطلاعاتی مستقر در قاره ای دیگر دسترسی پیدا کند.با توجه به گسترش روز افزون جرایم کامپیوتری و بدون مرز شدن جرایم جدید تر جرایم سایبر،عدم حضور فیزیکی مجرم در محل،سرعت بالا و زمان اندک ارتکاب جرم ،لزوم هر چه سریعتر تعاون بین المللی را برای دستیابی به یک سیاست کیفری هماهنگ را ایجاب می کند[1].

د-حجم و وسعت ضرر و خسارت وارده از طریق جرایم کامپیوتری به وسیله تکتولوژی کامپیوتر ،مرتکبین با کمترین سرمایه و هزینه می توانند با ورود به شبکه اطلاعاتی و نفوذ در آن خسارات هنگفتی وارد نمایند.سهولت ارتکاب با حجم زیاد موضوعات مطروحه،سرعت عملکرد کامپیوتر،عدم نیاز به تخصص خاص یا بالا عدم نیاز به حضور فیزیکی مرتکب در محل و... همگی موجب گردیده تا حجم صدمات و خسارات وارده افزون گشته و گاه به چندین هزار برابر جرایم معمولی برسد.وسعت خسارات وارده ناشی از یک نفوذ غیر قانونی یا گسترش ویروس در اینترنت می تواند در کسر ثانیه صدها هزار استفاده کننده در سراسر جهان را متحمل خسارت نماید.به عنوان نمونه کوچک از جرایم کامپیوتری که منجر به خسارت فراوانی گردیده ،می توان به ویروس ملیسا در سال ۱۹۹۹ میلادی اشاره کرد که این ویروس با ایجاد اختلال در سیستمهای پست الکترونیکی [2]در سراسر جهان موجب بروز میلیونها دلار خسارت گردیده.خالق این ویروس ادعا نموده که ویروس را روی کامپیوتر شخصی خود تولید کرده بود و برای ورود به سایت American on line فقط از یک نام و رمز عبور به سرقت رفته استفاده کرده است .با این وجود عواقب جرایم کامپیوتری علاوه بر خسارات سنگین می تواند تهدیدی جدی برای امنیت بشر باشد.وابستگی امور حساس کشورها در زمینه های پزشکی ،مخابراتی،هواپیمایی،و ... به عملکرد کامپیوتر باعث می شود تا کوچکترین اختلال و خدشه در کار این سیستم ها عواقب وخیم و جبران ناپذیری را به دنبال داشته باشد.[3]

[1] همان،ص۴۷

[2] E-mail

[3] عمیدی، مهدی، مطالعه تطبیقی جرایم رایانه‌ای از دیدگاه فقه و حقوق کیفری ایران، پایان نامه کارشناسی ارشد حقوق جزا و جرم شناسی، دانشگاه آزاد اسلامی واحد تهران مرکز ، ص ۶۵

ه-نحوه تعقیب و رسیدگی به جرایم کامپیوتری و اینترنتی نوین بودن جرایم کامپوتری و اینترنتی و شیوه ی ارتکاب اینگونه جرایم،نحوه رسیدگی و تعقیب را از جهت مسائل آیین دادرسی با چالش هایی روبرو کرده است.به طوری که تدابیر کلاسیک حقوقی به هیچ عنوان پاسخگو نبوده و با مشکلات عدیده ای در این زمینه روبرو می باشد.نوع تحقیق ،بازرسی محل،و وقوع جرم ،توقیف اسباب و آلت جرم با جرایم کلاسیک متفاوت بوده و بدون تخصص و مهارت کافی مقامات قضایی کشف جرم میسر نیست.تخصص نداشتن مامور تحقیقاتی از محیط کامپیوتری و جرایمی که از سوی کاربران سایر کشورها بوقوع می پیوندد،محل وقوع جرم را از دایره تحقیقات و کشف به دور و بسیار دشوار و غیر قابل دسترس می کند.و یا تحقیقات از شبکه ای یا بانک اطلاعاتی گاهی باعث تجاوز به حاکمیت کشوری و یا تجاوز به شبکه و یا بانک اطلاعات مادر می شود که اطلاعات در آن ذخیره کرده اند.در واقع جایگزین شدن موضوعات غیر ملموس و مجازی به عوض ادله ی مثبت ملموس و عینی در عرصه ی تکنولوژی اطلاعات،مسائل حقوقی نوینی را مطرح ساخته و از خصوصیات بارز جرایم کامپیوتری و اینترنتی می باشد[1].

بخش دوم: نقش کامپیوتر و اینترنت در فراهم سازی بستر جرم

از قدیم برای دارایی های قابل رویت و مادی ملموس ارزش اقتصادی قائل بودند، با پیدایش تکنولوژی کامپیوتری این واقعیت که داده های عینی غیر ملموس نیز می تواند دارای ارزش اقتصادی باشند و اطلاعات موجود در رایانه نیز می تواند موضوع ارتکاب جرم قرار گیرند،آشکار گردید.بنابراین در محیط کامپیوتر و سیستم های کامپیوتری دارایی های غیر ملموس «اطلاعات،برنامه»ارزش بسیار عمده ای نسبت به دارایی های ملموس کامپیوتر«قطعات کامپیوتر»دارد.تکنولوژی کامپیوتر و قابلیت های آن را می توان در قابلیت ذخیره سازی وتراکم داده ها و اطلاعات و برنامه های کامپیوتری در رسانه هایی چون نوار، دیسکت، کاست، فلاپی و میکروفیلم دانست که ازدست دادن یا سرقت آنها می توانند حائز اهمیت باشد.تا چندی بیش مسائل مربوط به دستیابی به سیستمهای کامپیوتری و اطلاعات تنها در

[1] همان،ص۶۶

محدوده ی اتاق کامپیوتری محدود می شد،ولی اکنون که شبکه جهانی و تکنولوژی اطلاعات پا به عرصه ی وجود نهاده اند دستیابی به سیستم های کامپیوتری بسیار آسان گشته است.در حال حاضر دستیابی اغلب از یک موقعیت راه دور در شبکه و بدون نیازبه حضور فیزیکی مرتکب و در شبکه ارتباطی بین المللی صورت می گیرد [1].نفوذ کنندگان و هکرها به طور معمول خود را به جای کاربران غیر مجاز معرفی می کنند و وارد سیستم می شوند،حفاظت به کمک اسم رمز اغلب به عنوان یک ابزار حفاظتی در برابر دستیابی غیر مجاز شناخته می شود.در حالی که نفوذ یا بندگان امروزی قادرند به آسانی و با استفاده از روش های مرسوم ازاین سیستم حفاظتی عبور کنند و به اطلاعات مورد نظر خود در یک شبکه یا یک سیستم دست پیدا کنند.[2] مدارهای ارتباطی داده های کامپیوتر ممکن است از طریق گرفتن انشعاب،نصب فرستنده مخفی،تحلیل تابش های الکترو مغناطیسی ناشی از تجهیزات و زیر نظر گرفتن سیگنال هم شنوائی القا شده در مدارهای الکتریکی دچار آسیب پذیری باشند.سیگنالهای الکترونیکی روی مدارها ممکن است دچار مسیر یابی نادرست شوند و یا در اثر تداخل امواج الکترو مغناطیسی کارآیی سیستم های پردازشی کاهش یابند و در نتیجه سیستم های کامپیوتری دچار اختلال شوند[3]. از دیگر مزایای اینترنت،عمومیت و گستردگی آن می باشد.به عبارتی ورود به شبکه ی جهانی اینترنت با کمترین هزینه ممکن و به راحت ترین شیوه و به صرف ارتباط از طریق تلفن یا اتصال به شبکه می تواند انجام گیرد.لذا می توانید گنجینه ای کامل از اطلاعات و مایحتاج خود را در آن بیابد به طوریکه دسترسی به این همه اطلاعات در سراسر دنیا به طریقی غیر از شبکه جهانی مستلزم هزینه بسیار و صرف وقت فراوان است.از طریق دسترسی به یک دنیا اطلاعات و امکانات در یک نقطه ی ثابت و کوچک مثل اتاق،قابلیت های اینترنت را صد چندان نمایان می نماید.بعنوان نمونه در فضای شبکه ی جهانی

[1] رضاییان،محمد جواد،مقاله بررسی جرایم اینترنتی، مجله دانشکده حقوق و علوم سیاسی دانشگاه تهران ،شماره ۴۵،۱۳۸۸،ص ۵۴

[2] همان،ص ۵۵

[3] سلیمی و داودی، علی، محمد (۱۳۸۶)، جامعه‌شناسی کجروی، قم: نشر پژوهشگاه حوزه و دانشگاه، چاپ سوم،ص۶۳

اینترنت یک کاربر در دور ترین نقطه ی آلاسکا با فشار دادن چندین دکمه می تواند به یک سرویس دهنده دانشگاهی در آفریقا دسترسی پیدا نموده و در خواست و یا اطلاعات خود را جویا شود.سپس دقایقی بعد با فشار دادن دکمه ای دیگر با یک کاربر ژاپنی ارتباط بر قرار نموده و صحبت کند.اینترنت حتی در عرصه های سیاست،پست ،جنگ اطلاعاتی و جاسوسی،تجارت الکترونیکی،تبادل فرهنگ ها و اطلاعات وارد شده و کار را برای کاربران آسان کرده است.[1]

بخش سوم: علل گرایش افراد به جرایم اینترنتی

علل و عوامل بسیاری در شکل گیری جرایم سایبری موثرند همچون عوامل اقتصادی. فرهنگی. سیاسی. مشکلات روحی و روانی نظیر: افسردگی.عصبانیت.حسادت.انتقامجوئی.حس تفریح و سرگرمی.خودکم بینی و حقارت.حس رقابت و... در ادامه به برخی از این عوامل اشاره می شود.

بند اول: علل اقتصادی

جرایمی نظیر (تحصیل مال بطور غیرمجاز از طریق سامانه رایانه ای) یا همان کلاهبرداری نمونه ای از این دست جرایم میباشد که عمدتا با اهداف اقتصادی بوقوع می پیوندد بعنوان مثال برخی بزهکاران سایبری از طریق فیشینگ به اطلاعات حسابهای بانکی کاربران دسترسی یافته و با وارد نمودن گذرواژه ها و دیگر اطلاعات در سامانه های مربوطه مبادرت به برداشت وجوه از حساب بانکی افراد می کنند. گفتنی است در موارد بسیاری ارتکاب جرایم رایانه ای که به حسب ظاهر اقتصادی نیست با انگیزه های اقتصادی شکل می گیرد و بالعکس برخی جرایم سایبری به ظاهر اقتصادی با انگیزه های غیراقتصادی ارتکاب می یابد بعنوان مثال در پرونده ای فرد پس از نفوذ به سیستم رایانه ای قربانی خود و تحصیل اسناد و مدارک شخصی وی اقدام به اخاذی از وی نمود و بالعکس در پرونده ای دیگر متهم صرفا با هدف ابراز توانائی خود در هک مبادرت به نفوذ به حساب بانکی یکی از مشتریان بانک نموده و مبلغی را برداشت و آنرا

[1] همان،ص۶۴

عینا به بانک مسترد نموده تا فقدان امنیت شبکه بانکی و توانائی بالای خود در این زمینه را به رخ بکشد جالب آنکه در بیان علت رفتار مجرمانه خود اعلام نمود از آنجا که جویای شغل بودم خواستم توانایی خودم را به دیگران نشان بدهم بلکه زمینه اشتغال برایم فراهم شود.[1]

بند دوم: علل فرهنگی

فقر فرهنگی و عدم پایبندی به ارزشهای جامعه و باورهای دینی یکی از عوامل مهم ارتکاب برخی بزه ها در محیط سایبر میباشد.پیش از این نیز اشاره شد که با خلق دنیای مجازی موانع بسیاری از بین رفته و ارتکاب جرایم تسهیل گردیده است. فضای سایبر شرایطی را به وجود آورده که بزهکاران می توانند در مکان هایی غیر از جاهایی که آثار و نتایج اعمال آن ها ظاهر می شود مرتکب جرم شده و به راحتی و با کمترین هزینه و اضطراب، بیشترین خسارات و صدمات را به بار آورده و در عین حال ناشناخته باقی بمانند. ارتکاب جرائمی نظیر انتشار آثار مبتذل و مستهجن از طریق سامانه رایانه ای یا مخابراتی یا حامل های داده و یا تسهیل دسترسی افراد به محتوای مبتذل و مستهجن نمونه ای از جرایم سایبری است که عدم توجه به اصول اخلاقی و ارزشهای جامعه موجد آن است. ایجاد سایتهای غیراخلاقی و ترویج بی بند و باریهای جنسی و روابط ناسالم دختران و پسران در قالب سایتهای دوستیابی. سایتهای پخش فیلمهای غیراخلاقی بصورت آنلاین و ... از مصادیق این جرایم میباشند.[2]

بند سوم: مشکلات روحی و روانی

بخش عمده ای از جرایم رایانه ای ارتکاب یافته در کشور عزیزمان برخواسته از مشکلات روحی و روانی بزهکاران فضای مجازی میباشد. مردی صرفا به جهت اختلاف با همسرش و با قصد انتقام گیری از وی اقدام به انتشار عکسها و فیلمهای خصوصی همسر خود در سایتهای اینترنتی نمود. خانمی صرفا با هدف انتقامگیری از همسرش که مبادرت به ازدواج مجدد نموده

[1] شیرزاد، کامران (۱۳۸۸)، جرایم رایانه‌ای از دیدگاه حقوق جزای ایران و حقوق بین الملل، تهران: نشر بهینه فراگیر، چاپ اول،ص۳۴

[2] همان،ص۳۶

است اقدام به انتشار عکسهای بدون حجاب خود در سایتهای اینترنتی نمود در پرونده دیگری مردی از روی حسادت اقدام به نصب نرم افزار شنود بر سیستم رایانه ای خانمی نموده و سپس متن چتهای خصوصی وی را دریافت و برای سایرین ارسال می نمود. در پرونده های متعدد دیگر افراد با ایجاد صفحات جعلی در سایتهای اجتماعی اقدام به آبروریزی و هتاکی به قربانیان خود می نمایند... مصادیق این بخش از علل ارتکاب جرایم سایبری بسیار گسترده تر از سایر علل و عوامل میباشد که مطالعات جرمشناسی در این حیطه را می طلبد.[1]

بخش چهارم: تأثیر رایانه در گسترش مفاسد اخلاقی

امروزه جرائم کامپیوتری و اینترنتی بر اساس ارزشها و منافع مورد حمله نیز متنوع شده مثلاً جاسوسی کامپیوتری جزء جرائم علیه آسایش و امنیت عمومی، نفوذ و خدشه در سیستمهای مالی جزء جرائم علیه اموال و تصاویر پورنوگرافی جزء جرائم علیه تمامیت معنوی اشخاص و ... می باشد. بدواً لازم است راجع به مفهوم و تعریف پورنوگرافی که موضوع این پژوهش می باشد توضیح داده شود . ترجمه و معادلی که در مورد واژه پورنوگرافی در زبان فارسی مورد استفاده قرار می گیرد هرزه نگاری است . واژه هرزه در فرهنگ واژگان فارسی به معنی بیهوده ، بی فایده ، عیاش ، فاسد بکار می رود و نگاری از ریشه نگاریدن و نگاشتن به معنی نوشتن و نقاشی کردن است. بنابراین پورنوگرافی یا هرزه نگاری عبارت است از هر گونه نوشته یا فیلم، تصاویر و مطالب مربوط به امور جنسی که فاقد هر گونه ارزش ادبی ، هنری ، سیاسی و علمی است و اعمال مجرمانه در پورنوگرافی عبارت است از اینکه شخصی ابزار سمعی و بصری یا وسایلی که حاوی اینگونه تصاویر و عکسهای هرزه باشد را بفروشد یا پخش کند یا چنین وسایلی را در معرض نمایش گذارد یا کودکان و جوانان را به شرکت در این نمایش یا پورنوگرافی اغوا یا تشویق نماید.[2] این نوع اعمال مجرمانه که ماهیتاً در جرائم کلاسیک نیز وجود دارد با توسعه و پیشرفت تکنولوژی کامپیوتر و اینترنت وارد این رسانه جمعی شده است

[1] رجب‌پور کاشف، مهدی (۱۳۹۰)، «تقابل امنیت فناوری اطلاعات با جرایم سایبری»، ماهنامه تخصصی وب، شماره ۱۳۵.ص 54

[2] همان،ص ۲۲

و از لحاظ گستردگی و وسعت در زمینه پخش و توزیع در نوع خود بی نظیر می باشد بعنوان مثال صندوقهای پستی ، آدرسهای الکترونیکی و سایتهایی در اینترنت وجود دارد که به تبلیغ ، پخش و عرضه تصاویر پورنو می پردازد.[1]

بخش پنجم: طرق مختلف تولید و توزیع محتویات مستهجن و مبتذل

۱)نقاشی : به نظر می رسد آنچه امروزه ما بعنوان هرزه نگاری از آن یاد می کنیم (صرفنظر از هرزه نگاری متنی و نوشتاری)با اولین خط ها و نقاشی ها بر دیواره غارها شکل گرفته است، نقاشی ها و طراحی های گوناگون و مختلفی با موضوعهاتی که امروزه هرزه نگاری به آنها اطلاق می گردد در آثار نقاشان قدیمی کشورهای کهن مثل یونان ، رم ، مصر ، چین و حتی هند و ژاپن به چشم می خورد . از این رو به جرأت می توان گفت که نخستین روش هرزه نگاری نقاشی بوده است.

۲)متن : هرزه نگاری متنی یا نوشتاری را هم می توان از نظر قدمت جزو قدیمی ترین روشهای تولید و توزیع هرزه نگاری دانست . بهره گیری از واژه های تحریک آمیز یا تصویر سازی و ایجاد موقعیت های تخیلی تحریک آمیز با اتکا به قدرت تخیل و تصویر سازی ذهنی خواننده، ماهیت اصلی هرزه نگاری متنی را تشکیل می دهد که با وجود پیشرفت های روزافزون روشهای هرزه نگاری همچنان جایگاه خود را حفظ کرده که شاید مهمترین دلیل آن سادگی آن از جهت فناوری ساخت و توزیع است و همچنین امکان استفاده ساده تر و خطر کمتر جهت شناسایی شدن و ...

۳)صوتی : هر چند هرزه نگاری تصویری با بهره گیری از عکس و فیلمها قسمت عمده ای از هرزه نگاری امروزی را تشکیل می دهد ولی به هر ترتیب نمی توان منکر وجود تأثیر هرزه نگاری صوتی شد مخصوصاً این مسئله در محیط سایبر هم جایگاه خود را حفظ و گسترش داده است این نوع هرزه نگاری از طریق واژه ها و تصویر سازی ذهنی مبتی بر صوت انسان و

[1]. روح الهی ،حسین (۱۳۹۰) تحلیل روانشناختی بزهکاری مدرن (جرایم رایانه ای)، همایش منطقه ای چالشهای جرایم رایانه ای در عصر امروز،ص۲۳

جابجایی لحن ، صوت و صدا انجام می گیرد و علیرغم اینکه در تعریف و مفهوم هرزه نگاری یا پورنوگرافی که ماهیتی تصویر گرانه دارد سازگار نیست ولی لاجرم زیر همین عنوان طبقه بندی می شود.

۴)رایانه: ورود رایانه به دنیای امروزی همانگونه که بسیاری از علوم و صنایع و فناوری های گوناگون را با دگرگونی و پیشرفت های عظیمی روبرو ساخت در زمینه هرزه نگاری نیز تأثیر فراوانی داشت و منشأ تأثیرات شگرفی در زمینه تولید و توزیع هرزه نگاری گردید.اهمیت رایانه ها نه بعنوان ابزار نمایش متن و تصویر و فیلم و صوت بلکه بعنوان فناوری نوینی است که می تواند منشأ ساخت و تغییر و تولید و غیره آثار هرزه نگاری گردد.

۵) خلق هرزه نگاری کاملاً گرافیکی (مجازی): هر چند شاید بتوان خلق یا ساخت هرزه نگاری گرافیکی را زیر عنوان قبلی طبقه بندی کرد ولی بدلیل اینکه این مسئله موجب بروز چالش های نوینی در بحث قانونگذاری و جرم انگاری و اجتماعی گردید بصورت مستقل مورد بحث قرار گرفته است.

خلق تصاویر رایانه ای کاملاً گرافیکی که بسیار واقعی به نظر می رسیدند مشکلات اخلاقی جدیدی را ایجاد کرد . وجود عکسهای غیر واقعی هرزه نگاری از افراد مشهور نشاندهنده امکان استفاده از تصاویر غیر واقعی است برای گرفتن حق السکوت یا تحقیر کردن شخص. در نهایت تولید تصاویر کاملاً ساختگی که اعمال واقعی را ثبت نمی کنند برخی انتقادها به هرزه نگاری به چالش کشید که آیا واقعاً ایرادات و اعتراضاتی که به هرزه نگاری وارد می شود با خلق تصاویر کاملاً مجازی که در آن انسان واقعی حضور ندارد ،مورد سوء استفاده قرار نمی گیرند، برطرف می گردد یا همچنان باقیست.

۶)گوشی تلفن همراه : از زمانی که گوشیهای تلفن همراه صاحب صفحه رنگی شدن و قابلیت عکسبرداری و فیلمبرداری و نمایش عکس و فیلم راپیدا کرده مدت زیادی نمی گذرد اما هر پیشرفت فن آوری جدید همانگونه که می تواند در خدمت استفاده سودمند باشد برای

مجرمین و بزهکاران فرصتی برای سهولت ارتکاب اعمال خود می باشد از این رو این وسیله در توزیع آثار هرزه نگاری نقش عمده ای ایفا می کند.[1]

قانون جرایم رایانه ای تخصصی ترین متن قانونی مرتبط با جرایم سایبر محسوب می گردد این متن از سالها قبل در تحقیقات و پژوهش های این حوزه بعنوان تنها منبع موجود مورد استفاده قرار گرفته است و متأسفانه بدلیل طولانی شدن روند تصویب مکرراً مورد اصلاح و تغییر واقع شده است . یاد آوری این نکته ضروری به نظر می رسد که چنانکه در مقدمه مربوط به قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیت می نمایند این قانون موجب بروز برخی اشکالات و تعارضات با قانون مزبور بویژه در مواد ۱۰ قانون نحوه مجازات و ۱۴ و ۱۵ قانون قسمت حامل های داده و ... می گردد . بدین صورت که انتقال آثار سمعی و بصری مستهجن و مبتذل از طریق حامل های داده بموجب مواد مزبور جرم انگاری شده است در حالیکه قانون سمعی و بصری این مورد را قبلاً مورد جرم انگاری قرار داده است حال می بایست به اعتبار سمعی و بصری بودن آثار آنرا مشمول این قانون و یا به اعتبار استفاده از حامل داده برای انتقال آن ، آن را مشمول قانون جرایم رایانه ای دانست.[2] ماده ۱۵ قانون جرایم رایانه ای در راستای پشتیبانی از بزه دیدگان و در پیکره بزهی پیش بینی شده است که به آن معاونت به عنوان بزهی جدا گفته می شود. معاونت به عنوان بزهی جدا به بزهی گفته می شود که رفتارش، رفتار معاونت است ولی پیرو قاعده های بزه اصلی است. به طور منطقی همه بزه هایی که در جایگاه معاونت به عنوان جرم جداگانه رخ می دهند مطلق هستند و بزه بودنشان منوط به این نیست که بزه اصلی رخ دهد. برای مثال طبق بند یک ماده ۶۳۹ قانون مجازات اسلامی ، تشویق مردم به فساد یا فحشا یا فراهم نمودن موجبات آن قابل کیفر است. در اینجا تشویق یا فراهم نمودن موجبات مصداق رفتاری هستند ولی در مقام بزهی جداگانه پیش بینی شده اند بی آنکه بایسته باشد تا این دو رفتار به فساد یا فحشای مردم بیانجامد.[3] ماده ۱۵ قانون جرایم رایانه

[1] تقوی ،محسن،تاثیر تکنولوژی بر بروز جرایم در جامعه،چاپ اول،انتشارات گلستان ،تهران،۱۳۹۲،صص۴۷-۵۰

[2] عالی پور، حسن، حقوق کیفری فناوری اطلاعات (جرایم رایانه ای)، انتشارات خرسندی، چاپ اول، تهران ۱۳۹۰،ص۹۵

[3] همان،ص۹۶

ای : « هر کس از طریق سامانه های رایانه ای یا مخابراتی یا حامل های داده مرتکب اعمال زیر شود به ترتیب زیر مجازات خواهد شد:

الف) چنانچه به منظور دستیابی افراد به محتویات مستهجن ، آنها را تحریک، ترغیب، تهدیدیا تطمیع کند یا فریب دهد یا شیوه دستیابی به آنها را تسهیل نموده یا آموزش دهد ، به حبس از نود و یک روز تا یکسال یا جزای نقدی از پنج میلیون ریال (۵,۰۰۰,۰۰۰ریال) تا بیست میلیون ریال (۲۰,۰۰۰,۰۰۰ریال) یا هر دو مجازات محکوم خواهد شد.

ارتکاب این اعمال در خصوص محتویات مبتذل موجب جزای نقدی از دو میلیون ریال (۲,۰۰۰,۰۰۰ ریال) تا پنج میلیون ریال (۵,۰۰۰,۰۰۰ ریال) است.

ب) چنانچه افراد را به ارتکاب جرائم منافی عفت یا استعمال مواد مخدر یا روان گردان یا خودکشی یا انحرافات جنسی یا اعمال خشونت آمیز تحریک یا ترغیب یا تهدید یا دعوت کرده یا فریب دهد یا شیوه ارتکاب یا استعمال آنها را تسهیل کند یا آموزش دهد ، به حبس نود و یک روز تا یکسال یا جزای نقدی از پنج میلیون ریال (۵,۰۰۰,۰۰۰ ریال) تا بیست میلیون ریال (۲۰,۰۰۰,۰۰۰ریال) یا هر دو مجازات محکوم می شود .

تبصره – مفاد این ماده و ماده ۱۴ شامل آن دسته از محتویاتی نخواهد شد که برای مقاصد علمی یا مصلحت عقلایی دیگر تهیه یا تولید یا نگهداری یا ارائه یا توضیح یا انتشار یا معامله می شود.در ماده ۱۵ قانون جرایم رایانه ای ، دو بند پیش بینی شده که در اینجا به بند الف آن پرداخته می شود :

تمامی مصادیقی که در بند الف ماده ۱۵ قانون جرایم رایانه ای به آنها اشاره شده است از مصادیق معاونت در جرائم است، قانونگذار با جرم انگاری این موارد قصد از بین بردن و ایجاد مانع برای راههایی را داردکه ممکن است موجب ارتباط افراد با محتویات مستهجن و مبتذل گردد. در قانون مجازات اسلامی بند ۴ ماده ۶۴۰ (مبنی بر اینکه :« هر کس برای تشویق به معامله اشیای مذکور در فوق(نوشته یا طرح، گراور، نقاشی، تصاویر، مطبوعات، اعلانات، علایم، فیلم، نوار سینما) و یا ترویج آن اشیاء بنحوی از انحاء اعلان و یا فاعل یکی از اعمال

ممنوعه فوق و یا محل بدست آوردن آن را معرفی نماید.»)موارد شبیه به این مصادیق مورد جرم انگاری قرار گرفته است با این تفاوت که در این ماده ارتکاب مصادیق و جرم از طریق سامانه های رایانه ای و مخابراتی مدنظر قرار گرفته است.ضمن اینکه به نظر می رسد منظور از حامل های داده نوار ،سی دی ، دی وی دی ، فلاپی دیسک ،فلش مموری یا هر نوع حافظه سیار یا وسیله ی دیگری باشد که برای جابجایی اطلاعات مورد استفاده قرار می گیرد. در مورد عبارت « حامل های داده» نکته دیگر اینکه با توجه به امکان انتقال فایل های صوتی و تصویری از این طریق به نظر می رسد این مسئله در موارد متعددی با قانون مجازات اشخاصی که در امور سمعی و بصری فعالیت می کنند در تضاد و ظاهراً ناسخ آن می گردد. علاوه بر این چه در این ماده و چه در ماده ۱۴ بحث صلاحیت دستخوش تغییر و در واقع اشکالات فراوانی می گردد. [۱]

بخش ششم: پیشگیری اجتماعی از جرایم و انحراف های سایبری و تدابیر لازم در این راستا

از جمله مهم‌ترین آن‌ها شناسایی هویت و خصوصیات مجرمان و منحرفان سایبری بر اساس انگیزه‌های هر یک و همچنین، شناسایی هویت و خصوصیات بزه دیدگان سایبر ارزیابی خطرپذیری [۲]آن‌ها برای جهت‌دهی نوع و میزان آموزش‌های پیشگیرانه است. سپس با توجه به نتایج به‌دست آمده، می‌توان بر اساس الگوهای کلی پیشگیری از جرم، راهکارهای قابل اجرا و مؤثری را پیشنهاد داد. با این حال، این مباحث به مجال دیگری موکول می‌گردد.[۳]

بند اول: پیشگیری اجتماعی جامعه مدار سایبری

به‌طور کلی، با کدهای رفتاری می‌توان گروه‌های خاصی را که وظیفه‌ای به آن‌ها سپرده شده، در مقابل اعمال خود پاسخگو نگه داشت. از جمله آن‌ها، گروه‌های مشاغل هستند که در حوزه‌های مختلف به فعالیت می‌پردازند و چون که به متصدیان شبکه‌ای خود، داده‌های واجد

[1] . Gina.De.Angelis،Cyber Crimes،Chelsea House Publisher.۲۰۰۰

[2] Risk Assessment

[۳]–طارمی، محمد حسین، گذری بر جرایم رایانه‌ای ۱۳۸۷، ص ۸۸

ارزشی را واگذار کرده‌اند تا با رعایت سه اصل محرمانه بودن[1]، تمامیت [2]و دسترس‌پذیری[3] در فضای سایبر منتشر کنند، ضروری است متناسب با حرفه، نوع و میزان اطلاعات آن‌ها و دیگر شرایط،کد رفتاری مربوط را برای آن‌ها تدوین کنند. شایان ذکر است، در این مورد تاکنون برای بعضی مشاغل و موضوعات حساس، از سوی مراجعه مهم و معتبر بین‌المللی، کدهای رفتاری نمونه‌ای منتشر شده است. برای مثال، به‌تازگی برای فعالان عرصه تجارت الکترونیکی و بازاریابی شبکه‌ای[4]،کدهای رفتار یکسانی تدوین شده تا از وقوع جرم و تخلف‌های مرتبط با پیام‌های تجاری ناخواسته الکترونیکی اجلوگیری شود .[5]اما گروه دیگری که کدهای رفتاری برای آن‌ها از جمله ضروریات شغلی است، ارائه دهندگان خدمات شبکه‌های اطلاع‌رسانی رایانه‌ای هستند. آن‌ها در حقیقت پل ارتباطی میان دنیای فیزیکی با فضای سایبر محسوب می-شوند و نسبت به بقیه دست‌اندرکاران این حوزه، افزون بر این‌که توانایی اقدامات بسیار متنوع و گسترده‌ای را دارند، مسئولیت‌های خطیری نیز بر دوش آن‌ها گذاشته شده است. این افراد به-راحتی می‌توانند امکان نفوذ به پایگاه‌ها را فراهم کنند یا اطلاعات حساس و کلیدی راجع به آن‌ها را در اختیار افراد ناصالح قرار دهند[6]. به دلیل وجود چنین شرایطی، چندی است بر نحوه عملکرد ارائه دهندگان خدمات شبکه‌ای نظارت بیشتری صورت می‌گیرد که از جمله مهم‌ترین آن‌ها اقدامات انجام شده در جهت نظارت بر حفظ حریم آن‌لاین افراد از سوی این ارائه دهندگان خدمات است ۰ آن‌ها به‌راحتی می‌توانند علاوه بر امکان‌پذیری ساختن شنود و ردیابی ارتباطات الکترونیکی، دسترسی به پایگاه‌های داده‌ای که ورود افراد غیرمجاز به آن‌ها ممنوع

[1] Confidentiality
[2] Integrity
[3] Availability
[4] Network Marketing
[5] عمیدی، مهدی، مطالعه تطبیقی جرایم رایانه‌ای از دیدگاه فقه و حقوق کیفری ایران، پایان نامه کارشناسی ارشد حقوق جزا و جرم شناسی، دانشگاه آزاد اسلامی واحد تهران مرکز ، ۱۳۸۷
[6] همان،ص۸۷

است یا اطلاعات شخصی و شخصی حساسی را که خود آن‌ها برای پیشبرد فعالیت‌های شبکه-ای جمع‌آوری کرده‌اند میسر سازند.[1]

بند دوم: پیشگیری اجتماعی رشدمدار سایبری

به نظر نمی‌رسد کسی در این واقعیت تردید داشته باشد که نه تنها نسل جوان و نوجوان جامعه ما، بلکه بدون استثنا در تمامی جوامع، توانسته است تعامل بهتری را با فضای سایبر برقرار کند. البته چندان جای شگفتی نیست، زیرا نسل گذشته امور خود را در دنیای فیزیکی به پیش می‌برده و شاید لزومی ندیده با این فضای جدید انس بگیرد، در حالی که نسل جدید با این فضا رشد یافته و از همان ابتدا هر آن‌چه پیرامون خود مشاهده کرده، رنگ و بوی سایبری داشته است.[2] به هر حال، این وضعیت بیم و امیدهایی را برانگیخته است. از یک سو، می‌توان امیدوار بود نسل جدید در برپایی هرچه سریع‌تر یک جامعه اطلاعاتی[3] تمام عیار، مبتنی بر اصول و قواعد حاکم بر این فضا، همت لازم را داشته باشد. اما از سوی دیگر، باید آن‌ها را از خطرات و آسیب‌های فراوان این فضا مطلع کرد تا با گرفتاری در آن‌ها، نتیجه عکس حاصل نشود.

بند سوم: تدابیر الزام آور کار برای اینترنت

بعضی دبیران برای این‌که استفاده صحیح از اینترنت را در قالب یک عمل الزام‌آور به کودکان بیاموزند، برای هر مبحث درسی، فهرستی از پایگاه‌های مجاز و مناسب را تهیه کرده و از دانش‌آموزان می‌خواهند در مهلت تقریبی متناسب داده شده، به تمامی آن‌ها مراجعه و

[1] شریفی، مرسده، جرایم رایانه ای در حقوق جزای بین المللی، پایان نامه کارشناسی ارشد، دانشگاه آزاد اسلامی واحد تهران، ۱۳۸۹،ص۱۰۲

[2] همان،ص۱۰۳

[3] Information Society

مطالب درسی مربوط را مطالعه و استخراج کنند. به این ترتیب، دانش‌آموزان زمان پرداختن به محتواهای نامناسب و غیرقانونی را نخواهند داشت[1].

بند چهارم: تدابیر رسانه ای

چون بسیاری از والدین و مربیان، اطلاعات زیادی راجع به ضرورت سلامت اینترنت یا ماهیت و میزان خطرات آن ندارند، غالبا نمی‌دانند چه چیزی را باید یا نباید انجام دهند. از این-رو یا با این قضیه خودبینانه برخورد می‌کنند و هیچ اقدامی در جهت حفاظت از فرزندان خود در اینترنت به عمل نمی‌آورند یا این‌که با مبالغه‌آمیز خواندن خطرات، معتقدند هرزه‌نگاری و مرتکبان جنسی در اینترنت، گستردگی و شیوع فراگیر دارند[2]. با این حال، برنامه‌های رسانه عمومی به خودی خود نمی‌توانند آموزش جامعی از این موضوعات پیچیده ارائه دهند. آن‌ها برای انعکاس پیام‌های تا حدودی ساده کارایی دارند. برای مثال، در اواخر دهه 80، در ایالات متحده امریکا یک برنامه تبلیغاتی بزرگ در راستای آگاه‌سازی عموم اعلام می‌داشت: «ساعت ده‌شب است، آیا می‌دانید فرزند شما کجاست؟ به همین ترتیب، یک برنامه مشابه در خصوص سلامت اینترنت می‌تواند پیامی این چنین منعکس کند: «فعالیت‌های آن‌لاین امروز فرزند شما چه بوده است؟»؛ یا »شما هم می‌توانید یاد بگیرید چگونه از فرزند خود در اینترنت محافظت کنید»؛ یا برای ترغیب مردم به قرار دادن رایانه‌ها در قسمت‌های عمومی منزل این پیام پخش می‌گردد: «آیا به خودتان اجازه می‌دهید یک غریبه در اتاق خواب فرزند شما باشد.[3]

نتیجه گیری

شیوع جرایم رایانه‌ای درحوزه‌های مختلف اجتماعی موجب بروز آسیب ها وخسارات متعددی در جامعه می‌گردد.از مهم ترین آسیب های وارد برفرد وجامعه از بین بردن مبانی واصول اخلاقی‌و نظام اجتماعی بوده که خسارات زیادی به نظام‌های اقتصادی ،سیاسی

[1] شریفی، مرسده، جرایم رایانه ای در حقوق جزای بین المللی، پایان نامه کارشناسی ارشد، دانشگاه آزاد اسلامی واحد تهران، ۱۳۸۹،ص ۱۳۶

[2] همان،ص ۱۳۸

[3] همان،ص ۱۳۹

،فرهنگی جامعه وارد می‌آورد. هرچه بیشتر فن آوری رایانه‌ای توسعه یابد جرایم رایانه‌ای مرتبط با هنجارشکنی‌های غیراخلاقی نیز توسعه پیدا خواهد نمودوتاثیرمنفی برنظام اجتماعی‌و بنیادی خانواده‌ها خواهد گذاشت.پس از بررسی قانون جرایم رایانه‌ای موجود به نظر می‌رسد قوانینی که بتواند با این جرائم برخورد نماید حداقلی بوده و تنها نیاز امروزرا برطرف می‌کند. لذا باپیشرفت این فن آوری باید تدابیری اندیشید که مطالعات اخلاقی وحقوقی در این ارتباط نیز متناسب با آن گسترش یابد ودولت ها می‌بایستی قوانین خودرا با جرایم رایانه‌ای متناسب نمایند.آنچه از ملاحظات اخلاقی،اجتماعی و حقوقی جرایم رایانه‌ای به دست می‌آید این است که باید برشناخت مسایل اصلی حقوقی و اخلاقی شهروندان درفضای سایبرتاکیدکردوگفت-حفظ حقوق معنوی پدیدآورندگان نرم افزارهای رایانه‌ای یا حق مالکیت معنوی،ترویج اطلاعات سالم‌وپاک، اعتمادسازی درمحیط سایبر، ایجاد اصل انکارناپذیری و جلوگیری از انتشارغیرمجازداده‌های متنی ،صوتی،تصویری ،پورنوگرافی در فضای مجازی وحفظ امنیت داده‌هاوشبکه مواردی هستند که درمحیط سایبر باید پیاده‌سازی شوند تا اخلاق انسانی ودینی به منظور نظم اجتماعی وعنصری روانی مهم بر افراد،جامعه و حاکمیت تضمین شود.

پیشنهاد ها

۱- مردم خودشان اطلاعات خود را در فضای مجازی فاش می‌کنند. به عبارتی اشخاصی هستند که از اینترنت اطلاع کافی ندارند و بدون اطلاع ، اقدام به چت کردن با افراد ناآشنا می نمایند. این اشخاص ، اطلاعات شخصی خودشان را در معرض دسترس این افراد قرار می دهند. به این گونه که توسط افراد متخصص هک شده و اطلاعات شخصی شان در اختیار آنها قرار می گیرد. همچنین گاهی اوقات اشخاص برای خرید یک محصول از یک سایت ، رمز عبور کارت شتاب خود را در اختیار متصدیان سایت قرار داده و سبب می شوند که از کارت آنها پول برداشت شود که می بایست پس از اقدام به پرداخت های اینترنتی از جمله شهریه و قبوض ، رمز خود را بر روی سیستم قرار نداده و یا حذف نماییم که مورد سوء استفاده دیگران قرار نگیرد .

۲-نصب آنتی ویروسها و نرم افزارهایی که وظیفه حذف یا جلوگیری از ورودکرم های اینترنتی دارند. برای جلوگیری از دزدی اطلاعات، خیلی از ویروس ها و کرم های اینترنتی هنگامی که وارد کامپیوتر می شوند سیستم امنیتی را از کار می اندازند و اقدام به دادن اطلاعات شخص دریافت کننده به شخص فرستنده ویروس می نمایند که از طریق آنتی ویروس ها و ضدکرم های اینترنتی که به روز شده اند می توان از ورود آن ها و سرقت داده ها جلو گیری کرد.

۳- نهایتاً به منظور کنترل و نظارت بر روی سایت های اینترنتی که در امور بازرگانی فعال بوده و خدمات اینترنتی به کاربران ارائه می دهند ، جلساتی میان پلیس فتا و وزارت بازرگانی برگزار شد و شرکت های ارائه دهنده خدمات اینترنتی و فعال در امور بازرگانی تحت نظارت پلیس قرار گرفته و ساماندهی شوند.

منابع و مآخذ

قرآن کریم

منابع فارسی

الف-کتب

۱. امام خمینی، سید روح‌الله. (۱۴۲۱ق) تحریرالوسیله، تهران: مؤسسه تنظیم و نشر آثار امام‌خمینی، چاپ و نشر عروج، چاپ اول.

۲. بابازاده، قاسم. \"پیرامون کنوانسیون اروپائی جرائم کامپیوتری\" خبرنامه انفورماتیک ، شورای عالی انفورماتیک شماره ۸۱ فروردین ۸۱ ، ص ۳۸.

۳. بازیگر – یدالله - کلاهبرداری ، اختلاس و ارتشاء درآرای دیوان عالی کشور (تهران)، نشر حقوقدان ، ۱۳۷۶ شمسی .

۴. باستانی، برومند، \"جرائم کامپیوتری و اینترنتی\"، چاپ بهنامی، سال ۱۳۸۳ ص ۲۷

۵. برومند باستانی«جرائم کامپیوتری و اینترنتی» انتشارات بهنامی، تهران،۱۳۸۳

۶. بهجت، محمدتقی. (۱۴۲۸ق) استفتائات، قم: دفتر معظم‌له، چاپ اول.

۷. تاریخچه اینترنت، تکنولوژی و اطلاعات ، شهریور ۸۵

۸. تاریخچه پیدایش اینترنت ، وب سایت مدرسه رشد... ۲۰۰۶

۹. جاویدنیا ، جواد جرایم تجارت الکترونیکی انتشارات خرسندی چاپ دوم ۱۳۸۸

۱۰. جعفری لنگرودی، محمد جعفر ، ترمینولوژی حقوق–انتشارات گنج دانش – ۱۳۸۳

۱۱. جعفری، محمدتقی. (۱۴۱۹ق) رسائل فقهی، تهران: مؤسسه منشورات کرامت، چاپ اول.

۱۲. خداقلی – زهرا – جرایم کامپیوتری ، تهران – انتشارات آریان – چاپ اول ۱۳۸۳

۱۳. خداقلی –زهرا – جرایم کامپیوتری ، تهران – انتشارات آریان – چاپ اول ۱۳۸۳

۱۴. خداقلی، زهرا ،جرایم کامپیوتری ، تهران – انتشارات آریان – چاپ اول ۱۳۸۳

۱۵. خرم آبادی – عبدالصمد – کلاهبرداری رایانه ای از دیدگاه بین المللی دانشگاه تهران سال ۳۷ شمارهٔ ۲ ۱۳۸۶

۱۶. دکتر ابراهیم حسن بیگی "حقوق و امنیت در فضای سایبر" موسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار، تهران،۱۳۸۴

ب-منابع عربی

۱. ابن زهره، حمزهٔ بن علی. (۱۴۱۷ق) غنیهٔ النزوع فی علمی الاصول و الفروع، قم: مؤسسه امام صادق(ع)، چاپ اول.

۲. ابن‌ادریس، محمدبن‌منصور بن‌احمد. (۱۴۱۰ق) السرائر الحاوی لتحریر الفتاوی، قم: دفتر نشر اسلامی، چاپ دوم.

۳. ابن‌برّاج، عبدالعزیز بن نحریر. (۱۴۰۶ق) المهذب، قم: دفتر نشر اسلامی وابسته به جامعه مدرسین حوزهٔ علمیهٔ قم، چاپ اول.

۴. ابن‌منظور، محمدبن‌مکرم. (۱۴۱۴ق) لسان‌العرب، بیروت: دارالفکر للطباعهٔ و النّشر.

۵. بوشهری، جعفر. (۱۳۸۷) حقوق جزا: اصول و مسائل، تهران: شرکت سهامی انتشار، چاپ دوم.

۶. جلالی فراهانی، امیرحسین، کنوانسیون جرایم سایبر و پروتکل الحاقی آن (به همراه گزارش های توجیهی آا)، معاونت حقوقی و توسعه قضایی قوه قضائیه، تهران: نشرخرسندی، چاپ نخست، ۱۳۸۹

۷. جوهری، اسماعیل‌بن‌حماد. (۱۴۱۰ق) الصحاح – تاج اللغهٔ و صحاح العربیّه، بیروت: دارالعلم للملائین، چاپ اول.