نقش اخلاق ومسائل حقوقی در
کنترل جرائم فن آوری اطلاعات وارتباطات

الهام شامخی، وحید حجه فروش

چکیده

امروزه رایانه ها،شبکه ها و اینترنت اساسی ترین و ابتدائی ترین ابزار فن آوری اطلاعات و ارتباطات به شمار می آیند ، در این مقاله ابتدا انواع جرائم رایانه أی ، قوانین و مقررات موجود برای مقابله با این جرائم ونیز نقش شبکه واینترنت در گسترش وافزایش جرائم بحث شده است و در آخر به بررسی نقش اخلاق و الگوهای اخلاقی در جلوگیری و کنترل جرائم پرداخته واز آن به عنوان یک فرهنگ و اصل اساسی یاد شده است.

۱- مقدمه

اصطلاح جرم رایانه ای گستردگی زیادی دارد.این اصطلاح جرائمی را که بوسیله یک رایانه ، درون یک فضای رایانه ای و علیه یک رایانه ارتکاب می یابند را شامل می شود[۶]. درجوامع امروزی که اطلاعات نقش کلیدی در تمام عرصه ها را بازی می کنند مسلما معادلات سنتی به هم خورده و جرمهای جدیدی بخصوص توسط روشنفکران وتحصیلکردگان جامعه پدیدار می شوند که نمی توان با پایبند بودن به قانونی که همواره یک گام عقب تر از جرم است انتظار رفع کلیه ناهنجاریهارا داشت .در این شرایط اخلاق و پایبندی انسانها به معیارهای اخلاقی می تواند در تعدیل وسازماندهی روابط سیاسی ،فرهنگی و اقتصادی و..... عنصری حیاتی بوده وقواعد حیات انسانها را سازماندهی و تعدیل بخشد.

۲- انواع جرائم رایانه ای

جرائم محیط فناوری اطلاعات را در چهار دسته اصلی می توان تقسیمبندی کرد:

الف) موارد نقض حریم خصوصی،

ب) جرائم اقتصادی(هک کردن رایانه ها، جاسوسی رایانه ای، بهره برداری های غیرمجازنرم افزاری، خرابکاری رایانه ای و کلاهبرداری رایانه ای)،

ج) انتشار مطالب غیرقانونی و خسارت زا،

د) سایر جرائم (تهدید علیه حیات بشری، جرائم سازمان یافته و جنگ الکترونیک) [۲]

الف) موارد نقض حریم خصوصی

از زمانی که رایانه ها سیطره خود را در دهه ۶۰ آغاز کردند، در بسیاری از کشورهای غربی این نکته روشن شد که جمع آوری، ذخیره سازی، انتقال و دستیابی به اطلاعات شخصی، حقوق خصوصی شهروندان را به خطر می اندازد. اگرچه طبق آمار و ارقام رسمی، جرائم مربوط به حمایت از داده ها از اهمیت ناچیزی برخوردار می باشند، ولی برخی موارد شناسائی شده در این خصوص (مثل سوء استفاده از اسناد وزارت امنیت ملی جمهوری دموکراتیک آلمان سابق و یا اخاذی های احتمالی از بیماران آلوده به ویروس ایدز) بیانگر این واقعیت است که موضوع حمایت از داده ها در جامعه اطلاعاتی، مساله ای نگران کننده به شمار می آید.

امروزه مشکلات مشابهی در رابطه با ذخیره سازی اطلاعات کاربران برای شبکه های تلفنی و رایانه ای به وجود آمده است. از طرفی ذخیره این اطلاعات به منظور ارایه صورت حساب و استفاده از آنها در تهیه آمار و ارقام و تحقیقات کیفی مفید است و از طرف دیگر مقادیر فزاینده اطلاعات منتقل شده در شبکه های بین المللی رایانه ای، خطر نقض حریم خصوصی را تشدید کرده است. این خطرات بالقوه درباره داده های شخصی در اینترنت، با بکارگیری آپلت های قابل اجرا یا کوکی ها به طور ویژه ای نمود پیدا کرده است[۲].

ب) جرائم اقتصادی

در دهه ۷۰ میلادی، موضوع سوء استفاده های رایانه ای نه تنها شامل نقض حریم خصوصی بلکه شامل جرائم اقتصادی مرتبط با رایانه نیز میشد. در طول دهه ۷۰، دستکاریهای رایانه ای برای کلاهبرداری نقطه شروع بحث درباره جرائم اقتصادی مرتبط با رایانه و همچنین مرکز ثقل این نوع جرائم محسوب میشدند. اما امروزه استفاده های غیر مجاز از رایانه ها در اشکال متفاوتی ظهور پیدا کرده است.

۱. هک کردن رایانه: اصطلاح هک کردن رایانه عموماً به نفوذ در سیستم های رایانه ای اطلاق میشود که نه با اهداف مجرمانه ای چون دستکاری، خرابکاری و جاسوسی رایانه ای بلکه بیشتر به خاطر لذت از غلبه بر تدابیر فنی و امنیتی صورت می پذیرد. در عمل این نوع جرم به کرات اتفاق می افتد.
۲. جاسوسی رایانه ای- که به ندرت در آمار رسمی بیان میشود- در مقایسه با جاسوسی اقتصادی مرسوم خطر ویژه ای را پایه ریزی میکند زیرا در سیستم های رایانه ای حجم بالائی از داده ها در فضائی بسیار اندک ذخیره میشوند و به کمک فناوری های جدید ارتباطی می توان از روی داده ها کپی برداری کرده و آنها را سریعاً انتقال داد.موضوع این جرم به ویژه برنامه‌های رایانه ای، داده های تحقیقاتی و دفاعی و نیز داده های مربوط به حساب های تجاری است.
۳. بهره برداری های غیرمجاز نرم افزاری: تکثیر غیرمجاز و استفاده های غیرقانونی از برنامه های نرم افزاری، اغلب سرقت نرم افزار یا بهره برداری غیرمجاز از نرم افزار نامیده میشود. این جرم بنابر سیر تاریخی فناوری رایانه ای، در ابتدا شامل تکثیر نرم افزارهای شخصی حاوی اطلاعات مهم و اسرار تجاری شرکت ها بود. بنابراین بهره برداری های غیرمجاز نرم افزاری در بسیاری از موارد با جاسوسی رایانه ای همپوشی داشت.
۴. خرابکاری رایانه ای: موضوعات این جرم تجهیزات ملموس رایانه ای و همچنین داده های ناملموسی هستند که برنامه های رایانه ای و دیگر اطلاعات ارزشمند را شامل میشوند. درمورد طریقه ارتکاب جرم مذکور، می توان بین ایجاد خسارتهای فیزیکی (روش های قدیمی) ایجاد خسارت های منطقی (روش های جدید) تفکیک قائل شد.
۵. کلاهبرداری رایانه ای: نقطه شروع بحث جرا یم اقتصادی رایانه ای بوده وامروزه اصطلاح

کلاهبرداری رایانه ای به طیف وسیعی از جرا یم مختلف که از طریق رایانه و به منظور بهره برداری های مالی صورت میگیرد، اطلاق میشود. از انواع کلاسیک این جرم می توان دستکاری فاکتورهای مربوط به حقوق و صورت حساب های شرکت‌های صنعتی یا دستکاری در ترازنامه های بانکی را نام برد. [۲]

ج) انتشار مطالب غیرقانونی و خسارت زا

در اواخر دهه هشتاد، نخستین موارد ارتکاب این جرم از طریق رایانه ها، در قالب مطالب مشوق خشونت یا اطلاعات حاوی مضامین نژادپرستانه اتفاق افتاد که بیشتر توسط افراطیون سیاسی صورت می گرفت. امروزه، کانون توجه به طور ویژه ای بر روی انتشار تصاویر مستهجن کودکان و زنان و مطالب مخالف اخلاق و عفت عمومی در شبکه های بین المللی رایانه ای متمرکز شده است. انتشار مطالب غیرقانونی از قبیل افترا، توهین، هتک حرمت اشخاص یا مطالب غیر اخلاقی از دیگر جرایمی است که امکانات فناوری شکل تازه ای از نحوه ارتکاب به آنها بخشیده و همچون سایر جرائم رایانه ای در خصوص تعقیب و پیگیری، چالش های جدیدی را فراروی قانون گزاران قرارداده است. [۳]

د) سایر جرائم

- تهدید علیه حیات بشری

دستکاری های رایانه ای نه تنها برای دستیابی به منافع مالی، بلکه ممکن است به منظور تهدید علیه حیات بشری نیز به کار گرفته شوند؛ مانند دستکاری در سیستم کنترل پرواز یا شبکه رایانه ای بیمارستان ها.

- جرائم سازمان یافته

واضح است که تجهیزات و امکانات رایانه ای پیشرفته و سیستم های ارتباطی ذخیره، اداره و انتقال اطلاعات توسط گروههای جرائم سازمان یافته نیز مورد استفاده قرار می گیرند. جرائم سازمان یافته به طور خاص شامل انواع کلاهبرداری‌های پیچیده رایانه ای، کلاهبرداری از طریق کارتهای اعتباری و نیز بهره برداری های غیر مجاز و سؤاستفاده از برنامه های نرم افزاری میشود.

- جنگ الکترونیک

امکان وقوع دستکاری های رایانه ای در بخش نظامی نیز مورد شناسائی قرارگرفته است. امروزه "جنگ اطلاعات راهبردی" نوع بالقوه ای از انواع جنگ هاست. جنگ اطلاعاتی یا جنگ الکترونیک عبارت است از بکارگیری شبکه های الکترونیکی برای تخریب و یا ازکار انداختن اطلاعات دیجیتالی و غیرعملیاتی کردن زیرساخت های اطلاعاتی که می تواند علیه جامعه یا نیروهای نظامی یک کشور انجام پذیرد. این جنگ با هدف ازهم گسیختن سیستم های اطلاعاتی و مخابراتی، سیستم های کنترل و فرماندهی، ارتباطات و جاسوسی صورت میگیرد. [۳]

۳- نقش شبکه درافزایش جرائم

نبود قانونی مدون و شفاف برای جرایم رایانه ای عملاً راه را برای تبهکاری در این عرصه فراهم کرده‌است. افرادی که دل به پنهان‌کاری در عرصه تکنولوژی اینترنت و کامپیوتر بسته‌اند در نبود چنین قوانینی در آرامش به کار خود می پردازند. [۶]

فقدان دادگاه‌های تخصصی و ضرورت تربیت قاضی‌های متخصص، خلاء قوانین و عدم تطبیق قوانین جاری با جرم‌های مجازی تا اندازه‌ای خیال همگان را آسوده کرده که حتی یک کمیته ضربتی برای برخورد با تعداد معدودی سایت نیز شکل نگرفته است. [۶]

با رشد فزاینده میزان دسترسی مردم به فناوری، این مفهوم تبدیل به ابزاری قدرتمند در دست تعداد رو به تزاید مجرمان شده است. در بیشتر جرایم رایانه‌ای، خشونت وجود ندارد بلکه بیشتر طمع، غرور یا دیگر ضعف‌های شخصیتی در ارتکاب این جرایم نقش اصلی را بازی می‌کند. این جرایم بر پایه عدم صداقت استوارند نه اجبار[۷] .

بیشتر جرایم رایانه ای بدون استفاده از زور ارتکاب می‌یابند بنابراین بیشتر نیازمند برنامه‌ریزی هستند. به نظر جامعه‌شناسان افرادی که این جرایم را مرتکب می‌شوند از مجرمان معمولی یا خیابانی قابل تشخیص هستند. این افراد به‌طور متوسط دارای مدرک لیسانس هستند. آنها برای کار خود دقیقا برنامه‌ریزی می‌کنند و میل شدیدبه یادگیری دوباره نرم افزارها یا سیستمهای رایانه ای دارند[۷] .

امروزه جرم‌های رایانه‌ای برخلاف شیرین‌کاری‌های جالب توجهی که غالبا توسط هکرهای دهه های گذشته صورت می‌گرفت، بیشتر نیازمند مهارت بسیار زیاد هستند.

از آنجا که میلیونها نفر در سراسر دنیا به فناوری برتر دسترسی دارند، جرایم رایانه‌ای ممکن است توسط هر کس و با هدف قانون‌شکنی ارتکاب یابد.

دنیای تجاری بورس و معاملات بزرگ مثال روشنی از یک صنعت مبتنی بر رایانه‌ها برای حفظ اطلاعات و انتقال مقادیر عظیم پول در فواصل بسیار زیاد می‌باشد. بسیاری از صنایع و خدمات مهم دیگر نیز «مبتنی بر فناوری» هستند. هر قدر رایانه‌های بیشتری به یکدیگر متصل شوند و هر قدر روند حذف پول نقد در جامعه - با اتکا بر کارت‌های اعتباری، کارت‌های بدهی و کارت‌های ATM به‌جای پول نقد - باشد، جرایم رایانه‌ای مطمئنا افزایش بیشتری خواهند یافت ،بعبارتی انواع روشهای کلاهبرداری مرسوم که قبل از پیدایش اینترنت وگسترش رایانه ها نیز وجود داشت وبه عنوان جرائمی علیه اموال ومالکیت دیگران به شمار می آمد هم اکنون بصورت آن لاین ودرفضای مجازی ارتکاب می یابد.این شیوه نوین کلاهبرداری تحت عناوینی مانند کلاهبرداری رایانه ای، کلاهبرداری اینترنتی یا کلاهبرداری آن لاین شناخته شده است[۷] .

جرم های رایانه ای را باید بحران عصر دیجیتال دانست،این شیوه مجرمانه که بیشتر برای کسب منافع اقتصادی و مالی انجام می گیرد خیلی سریع با ظهور شبکه های رایانه ای شکل گرفته و با آهنگ سریع و روز افزون فناوری نیز بر تنوع وپیچیدگی آن افزوده می شود بطوریکه امروزه سازمان‌های مجری قانون و شرکت‌های نرم‌افزاری و رایانه‌ای بر سر پیشتاز بودن در مبارزه با جرایم رایانه‌ای به وسیله ایجاد و تقویت سیستم‌های امنیتی رایانه‌ای جدید با هم به رقابت می‌پردازند.

مجرمان رایانه‌ای چه کسانی هستند؟ مجرمان رایانه ای معمولا جوانان تحصیلکرده با وقت آزاد زیاد و علاقه شدید برای رخنه در شبکه ها هستند. اکثر جرایم به وسیله کارکنان فعلی و سابق شرکت‌های رایانه ای ارتکاب می‌یابند بطوریکه ۷۵ تا ۸۰ درصد جرایم رایانه‌ای تحت پیگرد قرار گرفته، به وسیله کارکنان فعلی و قبلی این شرکت‌ها ارتکاب یافته است.

باک بلوم بکر (Buck Bloom Becker) نویسنده و متخصص جرایم رایانه‌ای می‌گوید: ما باید هنگام صحبت درباره کسانی که گستره وسیعی ازجرایم رایانه‌ای رامرتکب می‌شوندازکلیشه‌های عمومی فراتر برویم. به‌رغم تمام توجه رسانه‌ها و حجم زیاد اخباری که منعکس می‌کنند، هکرها درصد بسیار کوچکی از مجموع مجرمان رایانه‌ای را تشکیل می‌دهند[۷] .

انواع بسیار متنوعی از جرایم رایانه‌ای،از سرقت مشخصات افرادوایجاد مزاحمت به وسیله فرستادن مطالب و تصاویر مستهجن و کلاهبرداری گرفته تا جرایم معمولی وجود دارد. عمومی‌ترین شکل این جرایم، سرقت و کلاهبرداری به صورت آنلاین می‌باشد[۷] .

فریک‌ها، کرکرها و گاهی اوقات هکرها به‌طور غیر قانونی به پست صوتی، پست الکترونیک و شماره حساب‌های اتصال به شبکه دسترسی پیدا می‌کنند و از آنها استفاده می‌کنند که این کار مشمول تقلب مالیاتی یا تقلب در استفاده از خطوط تلفن می‌شود.

کدهای دسترسی راه دور بسیار مورد توجه هکرها، کرکرها، فریک‌های تلفن و همین‌طور مجرمان خیابانی می‌باشد [۷] .

بعضی مجرمان رایانه‌ای این کدها را به‌وسیله گشت‌زنی در اینترنت به‌دست می‌آورند. آنها از خط تلفن که مراقب هک شدن نیستند استفاده می‌کنند و به جست‌وجو در شبکه می‌پردازند. یک دلیل برای آنکه این کار تبدیل به شکلی عمومی از جرایم رایانه‌ای در میان هکرها شده، آن است که این مجرمان معمولا برای پرداختن به سرگرمی خود باید روزی ۱۰ تا ۱۲ ساعت از خطوط تلفن استفاده کنند و طبعا این کار هزینه بالایی خواهد داشت. مجرمان دیگر این کدها را از تابلوی اعلانات الکترونیکی

»سرقت«(Pirate BBS)به‌دست می‌آورند و از این محل برای مبادله رایگان نرم‌افزارها، شماره کارت‌های اعتباری و اطلاعات دیگر استفاده می‌کنند. [۷].

هکرها، کرکرها و فریک‌ها تقریبا همیشه علاقه‌مند به‌دست آوردن امکان استفاده رایگان از تلفن می‌باشند. برای مثال در روسیه، مقامات مسوول دریافتند که هکرهای بسیاری تمایل دارند با پلیس رایانه‌ای و دیگر افراد دولتی در قبال به‌دست آوردن دسترسی رایگان به اینترنت همکاری کنند. در روسیه تقاضای بسیار زیادی برای اینترنت وجود دارد اما هزینه یک ساعت

اتصال به اینترنت معادل ۳ دلار است که مبلغ بالایی محسوب می‌شود و افراد کمی امکان استفاده از آن را دارند. مقامات مسوول در روسیه همانند مقامات مسوول شرکت‌های اینترنتی بزرگ (مانند آمریکا آنلاین (AOL))، امید دارند که بتوانند با دادن امکان دسترسی رایگان اینترنتی به هکرها، درمقابل اطلاعات - معامله‌ای طعنه‌آمیز - به امنیت اینترنت و دیگر شبکه‌های رایانه‌ای در مقابل هر نوع نفوذ جدی امنیتی کمک کنند. [۷]

یکی از وحشتناک‌ترین جرایم رایانه‌ای، سرقت مشخصات است. این نوع کلاهبرداری امروز بسیار آسانتر شده است زیرا اطلاعات شخصی افراد بسیاری به صورت آنلاین و رایگان قابل دسترسی است و حتی اطلاعات شخصی بیشتر را می‌توان با مبلغی اندک بدست آورد. آیا می‌دانید اگر نام خانوادگی شما در کتاب راهنمای تلفن باشد، بدون توجه به اینکه شما رایانه دارید یا نه، احتمالا تلفن و آدرس شما در شبکه جهان‌گستر قابل دسترسی خواهد بود؟ [۷]

شاید تعجب کنیدکه چگونه تمام این اطلاعات شخصی به شبکه رایانه‌هاراه یافته است. یادآور می‌شویم که اولین شبکه‌های رایانه‌ای، دولتی بودند.با افزایش میزان دسترسی رایانه‌ها و آسانترشدن استفاده از آنها، شرکت‌های خصوصی همانند دولت شروع به استفاده ازرایانه‌هابرای نگهداری اطلاعات کردند. روزنامه‌نگاری به نام پیتر مک‌گراد (Peter Mcgrath) درباره رایانه‌ها می‌گوید: «رایانه‌ها تبدیل به انبارهای نگهداری محرمانه‌ترین جزئیات زندگی مردم شدند. هر کسی که یک حساب در بانک باز می‌کرد، ردپایی الکترونیکی از خود به صورت مخارج خانه، خریداری اشیای مورد علاقه و ..... به‌جا می‌گذاشت. [۷].

به وسیله آن یک دنبال کننده می توانست از رایانه های دولتی مثلا، عدم بازپرداخت مالیات صاحب آن شماره را دریابد. امروزه که شماره گواهینامه رانندگی افراد نیز در رایانه‌های شبکه‌ای بزرگ، ذخیره می‌شود، مشخصات فیزیکی اشخاص - رنگ چشم، قد و امثال آن- نیز قابل دسترسی می‌باشد. خواندن نوارهای مغناطیسی، کارت‌های اعتباری و کارت‌های ATM و ثبت میلیون‌ها خرید و فروشی که هر روزه انجام می‌شود، توسط شبکه های رایانه ای انجام می پذیرد. [۷]

خوشبختانه با وجود آنکه امکان دسترسی به این اطلاعات شخصی تقریبا برای همه وجود دارد، عده کمی درصدد استفاده از این اطلاعات با مقاصد غیر اخلاقی می‌باشند. در شماره ۱۹ جولای ۱۹۹۷ مجله نیوزویک، گزارشی درباره پرونده کاترین رمبو(Kathryn Rembo) آمده است. کاترین یکی از قربانیان سرقت مشخصات بود. یک نفر اطلاعات شخصی کاترین را در یک فرم استخدام یافته بود و آن را در بانک داده‌های اینترنت و موتورهای جست‌وجوقرار داده بود و سپس با استفاده از این اطلاعات اقدام به درخواست کارت اعتباری کرده بود. در این گزارش قید شده است که این شخص، یک اتومبیل ، پنج کارت اعتباری، یک آپارتمان و یک وام ۳۰۰۰ دلاری را با استفاده از اطلاعات شخصی کاترین رمبو و سوابق اعتباری خوب او به چنگ آورده بود. [۷]

۴- قوانین و مقررات موجود

گسترش فناوری اطلاعات در ایران تحولات چشمگیری را در بخشهای مختلف به دنبال داشته است .نظامهای اقتصادی، اداری وعلمی در این زمینه باتحولات جدیدی مواجه شده اند وروز به روز درحال آمادگی برای تجدید ساختار ورویارویی با تاثیرات فناوری اطلاعات هستند.

نظام حقوقی کشور نیز به نحو گریز ناپذیری از این تحولات نوین تاثیر پذیرفته است.آنچه که دراین خصوص بیشتر از هر مسئله ای نظام فضائی کشور را به چالش فراخوانده ، پیدایش اشکال تازه ای از جرایم است که اصطلاحا جرایم رایانه ای نام گرفته اند.جرائمی از این دست درابتدا بیشتر ناظر به بهره برداریهای غیرمجاز از نرم افزارهای رایانه ای مثل شکستن قفل نرم افزاروتکثیر غیرمجاز آنها بود ولی به تدریج با گسترش اینترنت اشکال دیگری از جرائم نیز بروز پیدا کرد .جرائم خاص محیط فناوری اطلاعات که پیش از این سابقه شناسائی در قوانین جزائی را نداشته اند نیازهای تقنینی جدیدی را فراروی نظام قضائی کشور گذاشته اند.

تاثیر فناوری اطلاعات بر محیط حقوقی کشور فقط به جرائم محدود نمی شود.گسترش اینترنت انجام مبادلات الکترونیکی وارتباطات داده ای را فراگیر ساخته است: بنابراین جنبه های حقوقی مبادلات الکترونیک (از قبیل انعقاد قراردادهای الکترونیک

درفضای مجازی یا امنیت مبادلات و...)مباحث مربوط به حقوق مالکیت های معنوی وبحث مسئولیت های مدنی دراینترنت از جمله مسائلی است که مستلزم توجهات حقوقی لازم در محیط فناوری اطلاعات است. [۴]

الف) قانون

قانون مهمترین منبع دراکثر نظامهای حقوقی به شمار میآید.وجود پشتوانه های قانونی لازم، تنظیم روابط وتحکیم معاملات افراد را تا حد زیادی تضمین می کند.

بطور کلی قانون در استقرار نظم اجتماعی و پیشگیری از نابسامانی ها نقش بسزائی دارد.از همین رو برای مطالعه وضعیت نظام حقوقی ایران ، پرداختن به قوانین و مقررات موجود و تطبیق آنها با محیط الکترونیک ضروری است. [۴]

ب)مراکز و مراجع حقوقی ویژه

نهادهای حقوقی ویژه ای هستند که بتوانند تمام نیازمندیهای ITمنظور ازمراکز و مراجع حقوقی ویژه

. حقوقی تازه ای را که در عصر فناوری اطلاعات برای نظام حقوقی یک کشور رخ می دهد مرتفع سازند

درحال حاضرمراکز ویژه ای برای رسیدگی به جرائم رایانه ای وجودندارد ومحاکم کنونی باصلاحیت عام ، صالح به رسیدگی اند. [۴]

ج)منابع انسانی

کارآمدی نظامهای حقوقی هر کشوری وابستگی مستقیم به منابع انسانی آن دارد . با توسعه کمی وکیفی منابع انسانی آن دارد.با توسعه کمی وکیفی منابع انسانی رسالت نظام حقوقی و قضائی که همانا نیل به عدالت است ،بهتر محقق می شود. از این رو تامین نیروی انسانی کافی و متخصص در محیط حقوق فناوری اطلاعات از ضروریاتی است که دولتها آن را به طور اساسی دنبال می کنند.

برخی از منابع انسانی که تحقق عدالت در عصر فناوری اطلاعات منوط به تامین آنهاست عبارتند از:

۱-قاضی: قضاوت و رسیدگی به دعاوی مربوط به محیط فناوری اطلاعات علاوه بردانش حقوقی کافی ، مستلزم برخورداری از دانش رایانه ای لازم است.

۲- وکیل: بحث تخصصی شدن وکالت مقوله ای است که هنوز به طور جدی در نظام حقوقی ایران مورد توجه قرارنگرفته است.

از طرفی هنوز مبا حث و روابط رایانه ای در جامعه به حدی گسترش نیافته است که برای اختلافات و دعاوی ، نیاز به وکلای متخصص در این زمینه احساس شود.در حال حاضر وکیل متخصص دعاوی مربوط به محیط فناوری اطلاعات که با این نام شناخته شده باشد در کشور ما وجود ندارد.

۳- کارشناسان رسمی دادگستری: کانون کارشناسان رسمی دادگستری در مورد رویارویی با مباحث حقوقی مربوط به محیط فناوری اطلاعات و ارتباطات ، اقداماتی انجام داده است .در نتیجه برای تعداد محدودی از متقاضیان ، پروانه رسمی صادر شده است.

۴- مقامات تحقیق (ضابطین دادگستری): تحولات سریع در زمینه های رایانه ای ایجاب می کند که فرآیند تحقیق ومحققان با تحولات زمان همگام شود.

در حال حاضر چنین نیروی متخصصی در بدنه مقامات تحقیق وجود ندارد ولی در این خصوص برخی از شعب اداره آگاهی در تهران و دیگر استانها به امر پیگیری های کیفری جرائم رایانه ای اختصاص پیدا کرده اند.

تامین نیروی انسانی کارآمد در محیط حقوقی فناوری مستلزم همکاری همه جانبه تمام نهادهای ذیربط از قبیل قوه قضائیه، کانون وکلای دادگستری ،کانون کارشناسان رسمی ، سازمان ثبت اسناد واملاک کشور ؤنیروی انتظامی و امثال آنهاست. [۴]

۵- نقش اخلاق والگوهای اخلاقی درجلوگیری وکنترل جرائم

رشد دائم و تنوع بی‌پایان جرایم رایانه‌ای، تدوین قوانینی با احاطه مناسب بر جرایم رایانه‌ای جدید را دشوار ساخته است. بعضی جرایم مانند اختلاس، کلاهبرداری و جعل سند توسط قوانین موجود پوشش داده می‌شوند.جرایم دیگرمانندخرابکاری رایانه‌ای، تروریسم رایانه‌ای و جاسوسی رایانه‌ای نسبتا جدید هستند. برای این جرایم جدیدتر، نص قوانین موجود گاهی اوقات اجازه تحت پیگرد قراردادن آنچه به‌طور وضوح جزو رفتار کیفری محسوب می‌شود را نمی‌دهد.

آزادی بیان و مطبوعات , با تمام اهمیت وضرورتی که دارند , هیچگاه نمی تواند مطلق و بدون محدویت باشند و لازم است میان آزادی ارتباطات از یک سو و حریم منافع فردی و جمعی از سوی دیگر توازن برقرار کرد[۹]. همین دلیل سبب شده است درکلیه کشورها و نظامهای حقوقی سواستفاده کنندگان از آزادی ارتباطات مورد پیگرد قانونی و مدنی قرار گیرند[۹]. به طور کلی همه پدیده های ساخته بشر و از جمله اینترنت به دلیل آثار گسترده ای که در زندگی انسانها دارد به مرور به یکی از اجزای ضروری زندگی بشر امروزی تبدیل شده است و موجب پدید آمدن حقوق ویژه ای نیز خواهند شد[۹]. اینترنت در ایران کمتر از یک دهه است که راه افتاده است . هم اکنون تمام رسانه های سنتی سریعا خود را به اینترنت رسانیده اند و حتی رادیو و تلویزیون وارد اینترنت شده و از این طریق برنامه های خود را پخش می کنند. در کشور ما گرچه نشریات الکترونیک بسیار کم می باشد اما تقریبا تمامی روزنامه ها در اینترنت سایت ویژه خود را دارند. این در حالی است که هنوز شرایط و مباحث حقوقی و فنی آنها بررسی نشده است[۹]. لذا ظهور جرائم جدید در عصر فناوری اطلاعات واکنشهای متفاوتی را به همراه داشته است و قانونگذاران کشور های مختلف برای رویارویی با این دسته از جرائم ، سیاستهای متفاوتی را در پیش گرفته اند. در این میان اخلاق می تواند نقش عمده ای درجلوگیری از ارتکاب چنین جرائمی داشته باشد.چراکه اخلاق را می توان همچون پدیده ای اجتماعی مورد بررسی قرار داد. بنیان ارزشهای اخلاقی عواطف انسانی هستند در این ارتباط برای تعیین داوری می توان به « ناظر بی طرف خیالی» تمسک جست که درچارچوب اخلاق به وجدان تعبیر می شود. [۱]

اصلاح انسانها و جوامع ونجات آنها از مفاسد اجتماعی تنها در پرتو ترویج اخلاق صحیح ودعوت انسانها به آراسته شدن به فضایل اخلاقی میسر می باشد.این مهم در ادیان مختلف الهی نیز اشاره شده است . امروزه همه پدیده های ساخته بشروازجمله اینترنت به دلیل آثارگسترده ای که درزندگی انسانهادارد به مرور به یکی از اجزای ضروری زندگی بشرامروزی تبدیل شده است وپدید آمدن حقوق ویژه ای را نیز می طلبد. [۱]

بطوریکه درصد کمی از احکام و قوانین ادیان مختلف وبخصوص اسلام جزایی هستند و تفکر عمومی ادیان مبتنی بر برخورد با علت هاست نه معلول ها.

عمده احکام شریعت اسلام ، فکری، تربیتی، اخلاقی و آموزشی است و عمده متون فقهی وآیات ناظربراین مواردا‌ست.درحالی که برخورد باجرایم توسط دستگاه قضایی تنها برخورد با معلول است بعبارتی اخلاق می تواند در کنترل جرایم و مبارزه با جرم بسیار مثبت باشد.

۶- نتیجه گیری

در پایان وبه عنوان نتیجه باید اذعان داشت گرچه کشورهای مختلف اقدام به اتخاذ راه حلهائی پراکنده در این خصوص کرده اند اما ناکارآمدی این راه حلها به اثبات رسیده است[۶]، زیرا اولا به دلیل وسعت قلمرو شبکه های اطلاع رسانی امکان جلوگیری از این جرائم بدون وجود یک راه کار بین المللی و همه جانبه وجود ندارد و ثانیا سرعت ارتکاب اشکال جدید جرائم رایانه ای بیشتر از قانون گزاری واقدامات پیش گیرانه در این زمینه است[۶] .لزوم توجه به اخلاق و الگوهای اخلاقی به عنوان یک عامل مهم در عدم ارتکاب این جرائم ونشر وتوسعه وترویج الگوهای استفاده از امکانات وسیع شبکه های ارتباطی به صورت صلح آمیز بیشتر نمود پیدا می کنند.

در این راستا عوامل فرهنگ ساز در سطح اجتماع از قبیل جراید، صدا وسیما وهنرمندان می توانند با معرفی این الگوها باعث نفوذ هرچه بیشتر اخلاق شبکه در بین استفاده کنندگان از امکانات ارتباطی و جلوگیری از وقوع چنین جرائمی شوند.از طرفی دیگر از آنجا که بسیاری از مرتکبین این جرائم به دنبال نشان دادن مهارت خود درامر رایانه وشبکه هستند ودر واقع ممکن است ناخواسته مرتکب این جرائم شوند ایجاد بستری سالم جهت بروز استعدادهای چنین افرادی و در جهت مثبت می‌تواند بسیار مشکل گشا باشد.

۷- منابع

[۱] کتاب نظامهای اخلاقی در اسلام وایران ، نوشته مجید محمدی

[۲] خبرنامه حقوق فناوری ،کمیته مطالعات حقوق تکنولوژی ، شماره ۶ ،اشکا ل رایج جرایم رایانه ای بخش اول.

[۳] خبرنامه حقوق فناوری ، کمیته مطالعات حقوق تکنولوژی ، شماره ۷ ، اشکا ل رایج جرایم رایانه ای بخش دوم .

[۴] خبرنامه حقوق فناوری ، کمیته مطالعات حقوق تکنولوژی، شماره ۱۱، محیط حقوقیIT در ایران.

[۵] مقاله : شبکه های اطلاعاتی ونقض حقوق بشر،نوشته عباس کدخدائی (http://iranwsis.org)

[۶] مقاله : اولویتهای کمیته مبارزه با جرائم اینترنتی چیست؟ ، نوشته شهرام شریف (سایت اخبار دنیای کامپیوتر و اینترنت)

[۷] با یک کامپیوتر و یک مودم هرکس می تواند مجرم شود، ترجمه سعید حافظی.

[8] http://illisa.org.ir/farsi/akhbar

[۹] مقدمه ای در شناخت مسائل حقوقی رسانه های الکرونیک-نشریات الکترونیک مجوز ندارند. (/www.jomhorieslami.com/1381/1381)