نظارت الکترونیک بر جرایم رایانه‌ای و نقش آن در قانون‌گرایی[1]

بهزاد پورنقدی[2]

تاریخ دریافت: ۱۳۹۲/۰۲/۰۵

تاریخ پذیرش: ۱۳۹۲/۰۳/۱۷

چکیده

زمینه: *نظارت الکترونیکی با هدف کاهش هزینه‌های نظارت سنتی و مراجعات حضوری و افزایش بهره‌وری و استفاده از ارتباطات الکترونیکی به دنبال سازوکارهای مناسب و کارآمد است. «نظارت الکترونیک» یکی از مفاهیم جدید مدیریتی و اصول قانون‌گرایی است که به عنوان مفهومی کارآمد در خدمت و تکمیل دولت الکترونیکی بسیار مورد استقبال واقع شده است.*

روش تحقیق: *این مقاله، پژوهشی کتابخانه‌ای و مطالعاتی می‌باشد که با استفاده از منابع موجود به بررسی وضعیت و ضرورت نظارت الکترونیک بر جرایم رایانه‌ای و قانون‌گرایی پرداخته است.*

یافته‌ها: *یکی از مشکلات اساسی امر نظارت در ایران، تعدد سازمان‌های نظارتی، استفاده از سیستم‌ها و روش‌های قدیمی و سنتی نظارتی و کشف جرایم می‌باشد. اجرای نظارت الکترونیک می‌تواند ابزاری مناسب و نظام‌مند برای پیشگیری، کشف و شناسایی جرایم رایانه‌ای در راستای تحقق دولت الکترونیک باشد.*

نتیجه‌گیری: *در صورت استفاده از سیستم نظارت الکترونیک، نهادهای نظارتی، امنیتی و انتظامی می‌توانند به پیشگیری و کشف سریع و دقیق جرایم بپردازند که این امر موجب ارتقاء قانون‌گرایی و قانون‌مندی در جامعه خواهد شد.*

واژگان کلیدی: *نظارت الکترونیک، جرایم رایانه‌ای، قانون‌گرایی، کشف فساد و تخلف.*

---

[1] این مقاله بخشی از کتاب تألیفی «الزامات و راهکارهای نظارت الکترونیک بر جرایم رایانه‌ای از سوی سازمان بازرسی» است که با تصویب و حمایت اداره کل بازرسی استان سمنان (سازمان بازرسی کل کشور) تدوین و منتشر شده است.

[2] دکترای مهندسی فناوری اطلاعات، استادیار دانشگاه آزاد اسلامی واحد بوئین زهرا. ایمیل: *behzad_pournaghdi@yahoo.com*

مقدمه

اصطلاح «جامعه‌مدنی» با «قانون‌گرایی» و «قانون‌مداری» یکسان انگاشته می‌شود. هر چند کلیّت این تساوی مورد تردید واقع شده، اما بدون شک، قانون یکی از مؤلفه‌های جامعه مدنی می‌باشد. جامعه اسلامی (همانند سایر جوامع بشری) برای حفظ نظم و امنیت، نیازمند قانون است. زیرا آزادی مطلق و بی‌حدّ و مرز انسان موجب اضمحلال و انحطاط جامعه می‌گردد. قانون و قانون‌گرایی، دو عنوان فرازمند تاریخی هستند که از آغازین روزهای حیات انسانی مورد توجّه بشر بوده‌اند. بدین‌سان در طول حرکت انسان در تاریخ، هر اندازه به سوی تشکیل نظام‌های اجتماعی پیش می‌رود، اندیشمندان بشری ضرورت تنظیم قواعدی را برای حیات اجتماعی انسان مورد توجّه قرار داده و بر اهمیت آن بیشتر توصیه می‌کنند. با رشد تفکر و اندیشه‌ها، قانون‌مداری و قانون‌گرایی، انسجام و نظام نوینی یافته و افرادی به تنظیم قانون پرداختند (حق پناه، ۱۳۷۷: ۲۷).

در عصر حاضر، فضای مجازی به دنیایی گفته می‌شود که با استفاده از فناوری اطلاعات و تکنولوژی‌های نوین ارتباطات و علوم رایانه، اینترنت و امکانات مجازی؛ همانند دنیای واقعی در کیفیت زندگی افراد جامعه تاثیرگذار است. فضای مجازی در معنا به مجموعه‌ای از ارتباطات درونی انسان‌ها از طریق کامپیوتر و وسایل مخابراتی بدون درنظر گرفتن جغرافیای فیزیکی گفته می‌شود. در این فضا مرز بین دنیای درون و بیرون تقریباً ناپدید شوده و دیگر زمان معنایی ندارد. در واقع می‌توان گفت که فضای مجازی گستره‌ای از ذهن است که می‌تواند تمامی اشکال زندگی واقعی را بسط و معنا دهد. مهمترین تحول در عرصه علم و دانش، توسعه و گسترش علوم کامپیوتر و فناوری اطلاعات[1] است که در سال‌های اخیر شاهد پیشرفت‌های چشمگیری در این زمینه بوده‌ایم و امروز این علم در خدمت و کمک‌رسانی به سایر علوم بر آمده و در تمامی ابعاد زندگی مردم و تکالیف روزمره ایشان دخیل و حائز اهمیت است. فناوری اطلاعات و

---

[1] *Information Technology (IT)*

ارتباطات[1] در ابعاد گسترده‌ای وارد حیطه‌های مختلف کاری جوامع بشری شده و حوزه نظم و امنیت نیز از این قاعده مستثنی نیست. بطور کلی سیستم دستگاه‌های قضائی، نظارت و نهادهای انتظامی، پلیسی و امنیتی با بکارگیری دانش فناوری اطلاعات و ارتباطات باعث توان اجرایی خود در تحقق اهداف و آرمان‌ها، کشف فساد، مبارزه با جرایم و تخلفات و نظارت بر حسن جریان امور و اجرای درست قوانین و مقررات در جامعه، تشکیلات و نهادهای اجتماعی خواهند شد. امروزه تحولات عظیمی در فناوری به وقوع پیوسته و شاهد تحولات بزرگ در زمینه فناوری ارتباطات فرا ملی، طی چند دهه اخیر بوده‌ایم. امکانات رسانه‌ای از جمله: اینترنت، ماهواره و تجهیزات جانبی آنها در عرصه اطلاع‌رسانی بین‌المللی دستاوردهای زیادی را به همراه داشته است.

بیان مسئله

در علوم رایانه و حقوق، جرایم رایانه‌ای را می‌توان چنین تعریف نمود: هرگونه عمل خلاف قانون که با سوء نیّت، از طرف شخص یا اشخاص با بکارگیری از رایانه صورت پذیرد، جرایم رایانه‌ای نامیده می‌شود. جرایم رایانه‌ای علیه اشخاص عبارتند از: نشر اکاذیب و باج‌گیری، تولید و انتشار داستان‌ها و عکس‌های مستهجن، فروش و یا به تصویر کشاندن عکس‌های مبتذل جهت تحریک کاربران و یا پیدا نمودن اشخاص از طریق چت (گپ زدن) جهت به نمایش گذاشتن عکس‌های آنها در اینترنت و معرفی آنها به دیگر اشخاص جهت داشتن روابط نامشروع. در یک تقسیم‌بندی کلی می‌توان جرایم رایانه‌ای را به شرح ذیل مطرح نمود:

۱- جرایم سنتی شامل: جاسوسی، سابوتاژ، جعل، کلاهبرداری، تخریب، افترا، نشر اکاذیب، پولشویی و قاچاق مواد مخدر.

۲- جرایم ناظر به کپی رایت برنامه‌ها و مالکیت مادی و معنوی.

---

[1] *Information Communication Technology (ICT)*

۳- جرایم علیه حمایت از داده‌ها و دسترسی غیر مجاز.

۴- جرایم در تجارت الکترونیکی.

۵- جرایم در بانکداری الکترونیک.

۶- جرایم مخابراتی و ماهواره‌ای.

۷- جرایم علیه اطفال و زنان.

۸- سایبر تروریسم.

همچنین بطور کلی جرایم رایانه‌ای به دو دسته تقسیم می‌شوند:

۱- جرمی که در فضای مجازی یا سایبری رخ می‌دهد، جرم رایانه‌ای است و بر اساس این دیدگاه، اگر رایانه ابزار و وسیله ارتکاب جرم نباشد، آن جرم را نمی‌توان در زمره جرایم رایانه‌ای قلمداد کرد.

۲- هر فعل یا ترک فعلی که در، یا از طریق و یا به کمک سیستم‌های رایانه‌ای رُخ می‌دهند جرم رایانه‌ای قلمداد می‌شود که از این دیدگاه جرایم نیز به سه گروه تقسیم می‌شوند:

- رایانه موضوع جرم: در این دسته از جرایم، رایانه و تجهیزات رایانه‌ای موضوع جرایم سنتی (کلاسیک) مثل سرقت، تخریب تجهیزات و غیره هستند.
- رایانه واسطه جرم: رایانه وسیله و ابزار ارتکاب جرم است و از آن برای جعل مدرک، گواهینامه و غیره استفاده می‌شود.
- جرایم محض رایانه‌ای: دسته سوم جرایم محض، جرایمی مانند هک یا انتشار ویروس رایانه‌ای که صرفاً در فضای سایبری یا مجازی اتفاق می‌افتد.

در کنوانسیون بین‌المللی بوداپست (۲۰۰۱) موضوعی تحت عنوان جرم رایانه‌ای مطرح نشده، بلکه در فضای مجازی از جرم سایبر نام برده شده است که در زبان فارسی آن را به جرم مجازی[1] تعبیر کرده‌اند. در اسناد و کنوانسیون‌های بین‌المللی، پیرامون جرایم رایانه‌ای رویکردی

[1] *Virtual Crime*

دوگانه وجود دارد. به این معنا که هم ارتکاب جرایم رایانه‌ای محض مانند هک کردن و هم ارتکاب برخی جرایم مانند جرایم سنتی با استفاده از سیستم‌های رایانه‌ای مانند نقض حقوق مالکیت معنوی جرم انگاری شده است. در کشور ما تعاریفی که در قانون جرایم کامپیوتری آمده؛ جرم‌ها را به جرایمی از قبیل: کلاهبرداری رایانه‌ای، جعل رایانه‌ای، تغییر، حذف و محو، متوقف‌سازی، جاسوسی رایانه‌ای، ملاحظه در خطوط ارتباطی، تخریب رایانه‌ای، دستیابی غیرمجاز، شنود غیرقانونی و غیره تقسیم کرده و مجازات‌هایی برای برخورد با این جرایم در نظر گرفته شده است.

در چنین شرایطی که جرایم از حالت سنتی خارج شده و در محیط رایانه‌ای و فضای مجازی اتفاق می‌افتد، کنترل و نظارت دستگاه‌های نظارتی، امنیتی، انتظامی و قضائی نیز مستلزم مطابقت با شرایط فعلی بوده و نظارت سنتی نیز دیگر کارآمدی و بهره‌وری مناسب را نخواهد داشت. «نظارت الکترونیک» یکی از مفاهیم جدید مدیریتی است که به عنوان مفهومی کارآمد در خدمت و تکمیل دولت الکترونیکی بسیار مورد استقبال واقع شده است. برنامه‌ریزی منابع سازمان، سیستمی است که می‌تواند با نظم دادن یکپارچه به تمامی اطلاعات تولید شده و ثبت، دسته‌بندی و طبقه‌بندی، پردازش و ارایه گزارش‌های مدیریتی، تمامی این اطلاعات را در اختیار مدیران قرار دهد تا در نظام برنامه‌ریزی و نظارت مورد استفاده قرار گیرد (حسینی و فولادی طرقی، ۱۳۸۹: ۶۷۷). نظارت الکترونیک یکی از راهکارهای مؤثر و گام‌های اساسی در جهت قانون‌گرایی و سلامت جامعه و دستگاه‌های اداری یک کشور محسوب می‌گردد.

جرایم رایانه‌ای و سایبری

جرایم سایبری طیف وسیعی از بزه‌کاری‌ها را شامل می‌شود و از انواع مزاحمت تا جرایم فاجعه‌آمیز را دربر می‌گیرد که در یک محیط مجازی به وجود می‌آید. جرایم سایبری و مجازی قدمت کوتاهی دارند و تنها طی بیست سال اخیر این اصطلاح رواج یافته است و با ساده‌تر شدن

کاربرد و استفاده از رایانه‌ای برای همگان و کاهش قیمت دسترسی به ابزار فناوری اطلاعات، معظلی نوین به نام جرایم سایبری در فضای مجازی پدید آمده است و نهادهای امنیتی، انتظامی و نظارتی را با چالش جدیدی مواجه ساخته است. جرایم سایبری که به جرایم نسل سوم رایانه و اینترنت وابسته است، در محیط مجازی یا فضای سایبری قابل تحقق می‌باشد. از این جهت رفتار مجرمان رایانه‌ای کاملاً متفاوت از مجرمان سنتی است. در این نوع از بزه، مرتکبان ناشناس در فضایی ناشناخته دست به اعمال مجرمانه می‌زنند. برخلاف جرم کلاسیک، جرم رایانه‌ای دارای تکنولوژی برتر و وسایل پیشرفته‌تری می باشد. مرتکبین این جرایم با استفاده از فناوری نوین و ابزارهای جدید به اهداف شوم خود دست پیدا می‌کنند، بدون آنکه همانند جرم کلاسیک اثری از خود برجای بگذارند. ویژگی دیگر این جرایم نامشخص بودن هویت مجرمان و همچنین عدم تشخیص درست طیف بزه‌دیدگان است، زیرا افراد و سازمان‌های متعددی می‌توانند هدف این مجرمان قرار گیرند. بنابراین جرم رایانه‌ای نشان‌دهنده یک مجرمیت با بزه‌دیده‌ای نامشخص است. این موضوع نشان می‌دهد که مجرمین رایانه‌ای و مجازی فارغ از زمان و مکان بوده و این نوع از جرایم و تخلفات هم‌اکنون جنبه فرا ملی و فرا سرزمینی به خود گرفته است. فناوری‌های نوین در این عرصه و پیشرفت تجهیزات ارتباطی، مخابراتی و الکترونیکی، سهولت وقوع جرایم رایانه‌ای در فضای مجازی، متخلفان و مجرمان را قادر ساخته که فعالیت‌های خود را بدون داشتن ارتباطی خاص با یک محل معین و مشخص انجام دهند. پر واضح است که با وقوع این نوع از جرایم، خطری جدی برای جامعه بین‌المللی و جامعه داخلی یک کشور و سیستم اداری و تشکیلات سازمانی آن رقم می‌خورد.

در حالت سنتی، بزه‌دیده یا مجنی علیه که هدف جرم است؛ انسان می‌باشد و در جرایم علیه اشخاص، تمامیت جهانی و معنوی فرد هدف ارتکاب جرم است. در جرایم علیه اموال، جرم علیه مال متعلق به انسان است که شکل اولیه بزه‌دیده در جرایم سایبری رابطه انسان و ماشین بود. در کلاهبرداری کامپیوتری اولیه و کلاسیک، مجرم رایانه‌ای با ورود دستورات و کدهای امنیتی و بدون فریب کاربران، وجوه کاربران دیگر را به خود اختصاص می‌داد. در شیوه جدید و جرایم

نوین رایانه‌ای از بزه‌دیده به صورت ماشین - ماشین تغییر یافته است، که بیشترین مورد تحقق آن در جرایم تجارت الکترونیکی و جرایم بانکداری الکترونیکی است (عالی پور، ۱۳۹۰: ۸۹).

رابطه بین نظارت و قانون‌گرایی

«نظارت» مجموعه اقدامات و فعالیتی است که «بایدها» را با «هست‌ها»، «مطلوب‌ها» را با «وضعیت فعلی» و «پیش‌بینی‌ها» را با «عملکردها» مقایسه می‌کند و نتیجه این مقایسه، تصویر روشنی از تشابه یا تمایز بین این دو گروه از عوامل خواهد بود که در اختیار مدیران سازمان‌ها قرار می‌گیرد. همچنین «نظارت» عبارت است از مقایسه بین آنچه هست و آنچه باید باشد. بر اساس تعریف دیگری که از نظارت ارائه شده؛ «نظارت» عبارت است از سنجش و اصلاح عملکرد، برای به دست آوردن این اطمینان که اهداف سازمان و طرح‌های اجرایی آن با کامیابی به انجام رسیده است (کونتز و همکاران: ۳۸۸). در جوامع پیشرو تفکر نظارت و بازرسی همیشه به عنوان یک فرهنگ والا و قابل قبول پذیرفته شده است. نظام بازرسی و نظارتی مناسب، شامل مجموعه‌ای از شاخص‌های کارآمد نظارتی است که این شاخص‌ها مانند هر پدیده دیگری با ملاک‌های متنوع قابل طبقه‌بندی می‌باشند. بر این اساس می‌توان شاخص‌ها را به دو دسته شکلی و ماهوی تقسیم‌بندی نمود. شاخص‌های شکلی، از اجزای سیستم نظارت شکلی و شاخص‌های ماهوی، از اجزای نظام نظارت ماهوی بوده که این دو نظام مکمل یکدیگر هستند (کریمیان، ۱۳۸۰). همچنین فرایند نظارت و کنترل و بازرسی دارای چهار مرحله اصلی می‌باشد که عبارتند از:

۱- تعیین استانداردها و معیارهایی برای اندازه‌گیری
۲- اندازه‌گیری عملیات و عملکرد
۳- مقایسه عملکرد با استانداردها
۴- اقدامات اصلاحی

در تعیین استاندارد و معیار، تاکید اصلی بر این است که اهداف سازمان به صورت کمی و قابل سنجش بیان شوند، زیرا اهدافی که به صورت کیفی بیان می‌گردند، قابل اندازه‌گیری و سنجش نخواهند بود و این موضوع فرایند نظارت را با مشکل مواجه خواهد کرد. بنابراین اهداف کیفی و کلی را باید به صورت هدف‌های ریز و کوچک و به صورت اعداد و ارقام ذکر کرد تا هنگام نظارت بتوان آن‌ها را مورد ارزیابی و سنجش قرار داد. در یک تقسیم بندی کلی، می‌توان استانداردها را به دو گروه اصلی تقسیم کرد:

۱- استانداردهای کمی (استانداردهای هزینه، درآمد سرمایه و برنامه).

۲- استانداردهای کیفی (این نوع از استانداردها بر کیفیت تولیدات یا خدمات تأکید دارند و مطلوبیت آن‌ها را تعیین می‌کنند).

نظارت یکی از ابزارهای مهم و حیاتی قانون‌گرایی، پیشگیری از وقوع جرم و کشف جرایم و تخلفات است. یک سیستم بازرسی و نظارتی بدون در اختیار داشتن اطلاعات کافی، صحیح و به موقع نمی‌تواند نقش مؤثری در راستای اهداف و مأموریت‌های خود ایفا کند. بنابراین، طراحی یک شبکه گسترده اطلاعاتی مبتنی بر ابزار الکترونیک که قادر است برای مسئولان نظارت و بازرسی، اطلاعات لازم را فراهم سازد و این اطلاعات را به موقع در اختیار آنان قرار دهد، در فرایند انجام کنترل و نظارت ضروری است. از آنجایی که نظارت دائمی و مستمر بر عملکرد افراد، کارکنان و یا فعالیت‌ها و نحوه عملکرد سازمان‌ها و ادارات به دلایلی همچون صرف وقت و هزینه‌های زیاد امکان‌پذیر نیست، ضرورت تشکیل یک سیستم نوین نظارت و بازرسی الکترونیک با استفاده از تجهیزات و بسترهای فناوری اطلاعات کاملاً روشن و آشکار است. زیرا این امر موجب به دست آوردن نتایج بهتر و نظارت و کنترل گسترده‌تر و دقیق‌تر با صرف هزینه و وقت کمتر می‌شود. همچنین یکی از عوامل موثر در بهبود عملکرد نظارت سازمان و کاهش هزینه‌ها و صرفه‌جویی در منابع مالی و امکانات، بودجه، منابع انسانی و زمان، سیستم نظارت الکترونیک است. سیستم نظارت الکترونیک یک فرایند نظارتی نوین است که با استفاده از تجهیزات و امکانات فناوری اطلاعات و ارتباطات و به منظور دستیابی به نتایج بهتر کنترل و نظارت سازمانی

می‌پردازد و این امر موجب حصول فرایند بازرسی مؤثر، دقیق و کشف سریع فساد و تخلفات اداری می‌شود. یکی از مسائلی که نقش مهم و اساسی در سیستم‌های نظارتی دارد، وجود اطلاعات طبقه‌بندی شده، گسترده و مناسب است. زیرا اطلاعات پراکنده، غیرمرتبط و ناقص برای فرایند نظارت، کنترل و بازرسی یک تهدید و چالش جدی است. گاهی سیستم‌های نظارتی به دلیل حجم انبوهی از اطلاعات متفرقه و طبقه‌بندی نشده و یا عدم درجه‌بندی اطلاعات و اخبار بر حسب نیاز، نمی‌توانند به شناسایی و کشف موارد تخلف و فساد بپردازند که این مشکل با استفاده از سیستم‌های نوین نظارت الکترونیکی و پردازش سیستمی و رایانه‌ای اطلاعات قابل حل است. حجم و درجه‌بندی اطلاعات دریافتی، جریان و یا عملکرد عادی یک سازمان با مقایسه شاخص‌ها و استانداردهای موجود باید به گونه‌ای باشدکه هم قابل فهم باشد و از طرفی امکان تصمیم‌گیری و اقدامات اصلاحی را برای تشکیلات نظارتی ممکن سازد. بنابراین وجود چنین سیستمی تنها با بکارگیری یک مدل کارآمد نظارت الکترونیکی امکان‌پذیر است که برای تحقق چنین نظارتی، نیازمند بکارگیری و استفاده از سیستم‌های نظارت رایانه‌ای و الکترونیکی هستیم.

روش‌های نوین کنترل، نظارت و بازرسی

روش‌های فعلی نظارت و سیستم‌های ارزیابی و کنترل سنتی، از کارایی لازم برخوردار نبوده و پاسخگوی نیازهای امروز جوامع تکنولوژیک نمی‌باشد. حذف روش‌های قدیمی و ناکارآمد و بهره‌برداری از روش‌های نوین نظارت و بازرسی همچون نظارت الکترونیک، ضروری و اجتناب ناپذیر است. همچنین لازم است نسبت به اتخاذ روش‌های نوین نظارت و بازرسی با بهره‌گیری از فناوری‌های جدید و پیشرفته و استفاده از آخرین تجارب کشورهای پیشرو در این زمینه توجه ویژه‌ای داشته باشیم. اصرار بر اتخاذ روش‌ها و شیوه‌های سنتی و انجام نظارت‌های فیزیکی و لزوماً با حضور ناظران و بازرسان، محدودیت‌هایی را در انجام وظایف محوله قانونی نهادهای نظارتی ایجاد کرده و موجب کاهش توانایی یا ناتوانی سازمان‌های نظارتی در توسعه فعالیت‌های

نظارت، کنترل و بازرسی شده است. نظارت مستقیم شامل نظارت‌های حضوری و یا غیرحضوری، مکاتبه‌ای، رایانه‌ای و الکترونیکی است که توسط ناظران و بازرسان انجام می‌شود و همچنین نظارت‌های غیر مستقیم و نظارت همگانی و مردمی که توسط افرادی خارج از سازمان‌های نظارتی مانند سازمان‌های مردم نهاد[1] صورت می‌گیرد، روش‌هایی هستند که سازمان‌های نظارتی کمتر به آن‌ها پرداخته‌اند (عبداللهی، ۱۳۸۳). امروزه با گسترش علوم رایانه‌ای، فناوری اطلاعات و پیشرفت فناوری‌های ارتباطی که شبکه‌های رایانه‌ای، رسانه‌های دیجیتال، تجهیزات الکترونیک و اتوماسیون در سازمان‌ها و دستگاه‌های اداری در حال شکل‌گیری و اجرا می‌باشد؛ می‌توان با استفاده از ابزار الکترونیک و نظارت و کنترل همه جانبه و بدون محدودیت زمانی و مکانی در محیط اطلاعات و داده‌ها، از چگونگی فعالیت دستگاه‌های اداری و نحوه عملکرد سازمان‌ها آگاه گردید و چگونگی عملکرد آن‌ها نظارت داشت.

امروزه تحولات شگرفی در زمینه فناوری اطلاعات رخ داده و پیشرفت‌های این تکنولوژی فراگیر شده، به‌طوری که موجب دگرگونی در زمینه‌های مختلف مدیریت سازمان‌ها شده است. فناوری اطلاعات، عنصری کلیدی در حذف محدودیت زمانی و مکانی، دسترسی بهتر و سریع‌تر به اطلاعات و داده‌ها، به‌روز بودن و غیره است. به عبارت دیگر، فناوری اطلاعات روش انجام کارها را دگرگون کرده و باعث شده بستری که مبتنی بر کاغذ بنا شده بود به بسترهای الکترونیکی تبدیل شود که آن را در اصطلاح تبادل الکترونیکی اطلاعات می‌نامند. فناوری اطلاعات، استفاده از رایانه و ارتباطات راه دور برای جمع‌آوری، پردازش، ذخیره‌سازی و انتشار اطلاعات صوتی، تصویری، متنی و عددی است. مهمترین ویژگی فناوری اطلاعات، سرعت زیاد در پردازش داده‌ها، دقت فوق‌العاده زیاد، سرعت بالای دسترسی به اطلاعات، به‌روز بودن، امکان مبادله الکترونیکی اطلاعات[2]، ارتقای سطح خدمات و کاهش هزینه‌ها می‌باشد.

---

1 *NGO*
2 *Electronic Data Interchange*

گسترش حجم عملیات، پیچیده شدن معاملات و انجام آنها به صورت الکترونیکی، باعث شده که اسناد الکترونیکی جایگزین اسناد کاغذی و سنتّی شود. به تبع آن نیز روش‌های کنترل، نظارت و بازرسی دچار دگردیسی و تغییر و تحول شده است. از این‌رو ضروری است که نهادهای نظارتی به‌دلیل این تغییرات و تاثیر آن بر عملکرد سیستم‌های سازمانی، فرایند نظارت و بازرسی را بصورت الکترونیکی با محوریت فناوری اطلاعات استوار نمایند. زیرا فناوری اطلاعات و نظارت الکترونیک بهترین ابزار برای ارتقای کیفیت نظام کنترل، نظارت و بازرسی است. کنترل و بازرسی از طریق نظارت الکترونیکی، الزام مکانی را برای بازرسان رفع کرده و به ایشان اجازه می‌دهد تا وظایف کاری را بین اعضای گروه بازرسی مستقر در محل و یا غیرمستقر در محل مورد بازرسی، تقسیم کنند.

در قانون جرایم رایانه‌ای کشور ایران، داده یا *Data* تعریف نشده است. کنوانسیون جرایم سایبر، داده را به داده‌های رایانه‌ای و داده ترافیک تفکیک نموده است. در این کنوانسیون، منظور از «داده رایانه‌ای» هرگونه نمایش حقایق، اطلاعات یا مفاهیم به شکلی مناسب که برای پردازش در یک سیستم رایانه‌ای که شامل برنامه‌ای مناسب است و باعث می‌شود که این سیستم عملکرد خود را به مرحله اجرا گذارد، مورد استفاده قرار می‌گیرد (جلالی فراهانی، ۱۳۸۹: ۲۱). منظور از «داده ترافیک» هر گونه داده رایانه‌ای است که در خصوص ارتباط برقرار شده به وسیله سیستم رایانه‌ای باشد. این نوع داده از سوی سیستم رایانه‌ای به وجود می‌آید که بخشی از زنجیره ارتباط رایانه‌ای و شبکه را تشکیل می دهد. این زنجیره شامل سیستم مبدأ، مقصد، مسیر، مدت ارسال، تاریخ، اندازه و حجم، دوام یا نوع خدمات اصلی ارایه شده است (همان: ۲۲).

خصوصیات سازمانی جرایم رایانه‌ای

در تقسیم‌بندی مجرمین رایانه‌ای به مجاز و غیرمجاز مشاهده می‌کنیم که برخی از این مجرمین، به طور غیرمجاز به یک سیستم یا شبکه رایانه‌ای دسترسی پیدا کرده و از این طریق مرتکب جرم می‌شوند. کارمند یک سازمان، ارگان، نهاد، موسسات مالی، شرکت‌ها و غیره، اجازه

استفاده و کاربری رایانه‌های این موسسات را دارند، در حالی که یک مشتری یا مراجعه کننده مجاز به استفاده از سیستم‌های رایانه‌ای نیست. در بررسی خصایص سازمانی این دسته از مجرمان، باید به برخی جرایم سازمان‌یافته هم توجه کرد. برخی تروریست‌های رایانه‌ای به صورت سازمانی اقدام به اجرای عملیات تروریستی و خرابکارانه شامل سایبر تروریسم می‌کنند و یا به افشای اطلاعات محرمانه و یا سایر جرایم رایانه‌ای می‌پردازند. کسی که بدون سوء نیت مجرمانه به سیستم رایانه‌ای دسترسی پیدا کند، با کارمند یک موسسه مالی که از حساب مشتریان وجوهی را برداشت می‌نماید بسیار تفاوت دارد (شیرزاد، ۱۳۸۸: ۹۰).

خصوصیات رفتاری مجرمان رایانه‌ای

مرتکبین جرایم رایانه‌ای از خصوصیات و رفتارهای خاصی نسبت سایر مجرمان سنتی برخوردار هستند. مطابق نتایج حاصل شده از تحقیقات مرتبط با این موضوع، مجرمین رایانه‌ای اکثراً افرادی درون‌گرا و غیر اجتماعی هستند (همان: ۹۰). بیشتر مجرمان رایانه‌ای از افراد تحصیل کرده جامعه می‌باشند و این گروه در ارتکاب سایر انواع جرایم موفق نبوده و از این جهت، تعقیب و دستگیری این مجرمان دشوارتر است. از سوی دیگر نیز، علم کیفرشناسی اقتضا دارد که به خاطر موقعیت اجتماعی خاص این گونه مجرمان برخورد متفاوت و عموماً ملایم‌تری با آنها صورت گیرد و انگیزه این دسته از مجرمان هم عموماً با انگیزه مجرمان جرایم عادی متفاوت است. گاهی انگیزه این دسته از مجرمان عاملی غیر از سود مادی و انتفاع شخصی مجرم است. زیرا برخی از این مجرمین در صدد قدرت نمایی و نشان دادن مهارت خود در علوم رایانه هستند و برخی دیگر صرفاً برای سرگرمی این کار را انجام می‌دهند. حتی در انگیزه برخی از این مجرمان عوامل بشر دوستانه هم وجود دارد و برخی دیگر از مجرمین، اصولاً با محدودیت و چارچوب قانونی مشکل داشته و محدودیت دسترسی به بعضی اطلاعات را نمی‌پذیرند. همچنین اکثر این دسته از مجرمان جوان و یا حتی نوجوان هستند (همان: ۹۲).

نتیجه‌گیری و پیشنهادها

در عصر نوین دانش و فناوری اطلاعات، نیاز جوامع انسانی به رایانه و اینترنت هر روز افزایش یافته است. این موضوع به افراد فرصت طلب و سودجو این امکان را می‌دهد تا مقاصد و اهداف شوم خود را در فضای سایبری دنبال کنند. علاقه به ارتکاب جرم در فضای سایبر به دلیل نامحدود بودن و احتمال ردگیری و شناسایی پایین مجرمین توسط نهادهای امنیتی و پلیسی افزایش یافته است. به همین جهت لازم است حقوقدانان و متخصصین جرم شناسی تمام تلاش خود را به کار گرفته تا بتوانند با افزایش آگاهی در رابطه با مسایل حقوقی فضای سایبر و علوم رایانه‌ای، به قانون‌گذاران کشورها و جوامع بین‌المللی کمک نموده تا به امنیت دنیای مجازی کمک کنند. این اقدام با همکاری نیروهای پلیس هر کشور باعث افزایش احساس امنیت جامعه خواهد شد. برای رسیدن به این هدف، راهکارهایی پیشنهاد می‌گردد که با اجرای آنها، ضمن کاهش وقوع جرایم رایانه‌ای، احساس امنیت فردی و اجتماعی نیز در سطح جامعه افزایش پیدا می‌کند. از پدیده‌هایی که رایانه و پس از آن شبکه جهانی اینترنت همراه خود به ارمغان آورد، مخاطراتی بود که در سراسر قلمرو گسترده خود سایه انداخته است. چنین مخاطراتی چنانچه مورد بی‌توجهی جامعه و مسئولین قرار گیرد، بسیار بزرگ و گاه غیر قابل جبران خواهد بود. چرا که آسیب‌های روانی ناشی از کاربری نادرست و خلاف قانون، موجب اختلال در رفتار شهروندان شده، جامعه را در رسیدن به فواید بی‌شمار این فناوری نوین ناکام می‌گذارد. این اختلالات، شهروندان را فرسوده و ناتوان کرده و فعالیت‌های روزمره آنان را مختل می‌کند. آسیب‌های اجتماعی و فرهنگی ناشی از آن، اعضای جامعه را در رفتار فردی با خانواده و رفتار اجتماعی با دیگر شهروندان و حکومت متزلزل و متأثر از فرهنگ‌های منحط بیگانه می‌نماید. هنجارها و ارزش‌های متعالی جامعه رو به زوال رفته، احساس امنیت و آرامش از جامعه رخت برمی‌بندد. ضمن این که آسیب‌های سیاسی آن، موجب تضعیف اقتدار و حاکمیت دولت شده، آن را در ایجاد وحدت ملی، امنیت اجتماعی و احساس امنیت دچار چالش‌های جدی می‌کند. در قانون اساسی به بیان امنیت اجتماعی در ۳۰ محور پرداخته شده است و قوه قضائیه و نیروی انتظامی

پشتیبان حقوق فردی و اجتماعی تعیین شده و رسیدگی به تخلفات اجتماعی، نظارت بر اجرای قوانین، کشف جرم و مجازات مجرمین، اقدامات مناسب برای پیشگیری از وقوع جرم و اصلاح مجرمین از ابزار رشد کیفی امنیت اجتماعی توسط قوه قضائیه است. تسریع در احقاق حق مردم و سرعت در محاکمه و مجازات مجرمین بهترین بسترساز حفاظت از امنیت اجتماعی است. دستگاه‌های قضائی، امنیتی، انتظامی و پلیسی نیز وظیفه عمده‌ای در ایجاد و برقراری امنیت و مبارزه با اخلالگران امنیت دارد. استقرار نظم و امنیت، مقابله با هرگونه خلافکاری و اقدام علیه امنیت ملی و نظم و امنیت کشور و جلوگیری از هرگونه بی‌نظمی و فعالیت‌های غیرمجاز، کشف جرایم و تخلفات، مجازات متخلفین و مجرمین از وظایف و مأموریت‌های نیروی انتظامی و سیستم قضائی کشور است. حضور به موقع بازرسان و نظارت محسوس یا نامحسوس تشکیلات قضائی، انتظامی و امنیتی کشور می‌تواند از آشفتگی سازمانی و یا وقوع جرایم رایانه‌ای پیشگیری کرده و به کنترل و حفاظت از منابع و سرمایه‌های کشور کمک کند.

با توجه به گستردگی دستگاه‌های اجرایی و تخصصی شدن فعالیت‌های اجرایی، منحصر کردن نظارت و بازرسی به شیوه‌های سنتی و به عبارتی؛ دستی و فیزیکی، همانند آن است که در انبار کاه به دنبال سوزن بگردیم. بنابراین در چنین اوضاعی تنها راه حل، اعمال شیوه مدیریت و نظارت الکترونیکی است. شیوه‌ای که ما را در جهت قانون‌گرایی رهنمون می‌سازد، زیرا تحقق قانون‌گرایی در گرو توسعه نظارت است و توسعه نظارت نیز، وابسته به مدیریت نظارت می‌باشد که این مهم تنها با اجرای سیستم یکپارچه نظارت الکترونیک محقق خواهد شد. بدیهی است برای تحقق نظارت الکترونیکی، ایجاد بسترهای فناوری اطلاعات و ارتباطات ضروری است و مستلزم این است که سازمان‌ها نیز به سمت الکترونیکی شدن گام بردارند. توجه به نظام‌های یکپارچه کنترل و نظارت در سازمان‌ها نیز در همین راستا بوده و سیستم برنامه‌ریزی منابع سازمان[1] یکی از طرح‌های مدیریتی و عملیاتی است که می‌تواند به صورت یکپارچه به تمامی اطلاعاتی که در حین عملیات تولید می‌شود؛ نظم دهد و با ثبت، دسته‌بندی و طبقه‌بندی،

[1] *ERP*

پردازش و ارائه گزارش‌های مدیریتی، تمامی این اطلاعات را در اختیار مدیران قرار دهد تا در نظام برنام ریزی و نظارت و کنترل مورد استفاده قرار گیرد.

پیشنهادهای کاربردی:

در خصوص توسعه قانون‌گرایی و نظارت الکترونیک بر جرایم رایانه‌ای، پیشنهادهای کاربردی ارائه می‌گردد:

- مطالعه جرم‌شناختی نظام‌مند در خصوص جرایم، حملات و تهدیدهای بالقوه رایانه‌ای نسبت به حریم خصوصی که جرم انگاری شده و یا عنوان مجرمانه دارند.
- ضروری است که دولت، قوه قضائیه و نیروی انتظامی با توجه به ویژگی‌ها و فرهنگ جوامع خود، برای ارتقای فرهنگ و سطح آگاهی جامعه در خصوص جرایم رایانه‌ای با استفاده از انواع وسایل ارتباطات جمعی و رسانه‌ای، اطلاع‌رسانی و تلاش کنند.
- بررسی دقیق‌تر خصوصیات رفتاری مجرمان رایانه‌ای که دستگیر شده‌اند این امکان را فراهم می‌سازد تا بتوانیم روحیات و خصوصیات این افراد را بهتر مورد بررسی و ارزیابی قرار داده و از وقوع جرایم دیگر توسط آنها در آینده بکاهیم.
- به دلیل ماهیت پیچیده فضای سایبر و نیاز به تخصص بسیار، در رابطه با تصویب قوانین سایبری و رایانه‌ای لازم است با کارشناسان خبره و متخصصین علوم رایانه مشاوره و همکاری شود تا قوانین مناسب و کاربردی و مورد نیاز جامعه به تصویب و اجرا برسند.
- لازم است تشکیلات نظارتی، امنیتی و انتظامی از امکانات، فناوری و دانش روز برای امر کنترل و نظارت بهره‌مند شوند. همچنین ضروری است که دستگاه‌های نظارتی، قضائی، امنیتی و انتظامی در فرایند اجرای امور، پیشرفت و بهبود داشته باشد و به ایجاد و استفاده از سیستم نظارت الکترونیک اقدام نماید.
- در حال حاضر سازمان‌های نظارتی متعددی در کشور ما به امر نظارت و بازرسی مشغولند، اما در میان این سازمان‌ها هماهنگی لازم وجود ندارد. لذا بایستی به منظور ایجاد

هماهنگی بین این نهادهای نظارتی، نوعی تشکیلات هماهنگ کننده ایجاد شود و شرح وظایف هر یک از بخش‌های نظارتی کشور را دقیقاً مشخص نماید تا از موازی کاری و همچنین عدم نظارت در برخی از موارد جلوگیری بعمل آید. همچنین ضروری است به بازبینی در ساختار نظارتی کشور و ایجاد هماهنگی بین سازمان‌های نظارتی پرداخته شود.

- لازم است سیستم خودنظارتی را در بین افراد جامعه و کارکنان سازمان‌ها را ترویج و توسعه دهیم. در سازمان‌های اجتماعی، بهترین نوع نظارت آن است که فرد، نظارت را از خودش شروع کند و روش خودنظارتی مرسوم گردد. منظور از خودنظارتی این است که فرد تقریباً آزاد است و آزادی فرد تا جایی است که به آزادی حقوق و اموال دیگر افراد لطمه نزند.

فهرست منابع

- جلالی فراهانی، امیر حسین (۱۳۸۹). کنوانسیون جرایم سایبر و پروتکل الحاقی آن، چاپ اول.
- حسینی، میرزاحسن و فولادی طرقی، مهدی (۱۳۸۹). بررسی موانع و محدودیت‌های اجرای نظارت الکترونیکی، فصل‌نامه مطالعات مدیریت انتظامی، سال پنجم، شماره چهارم.
- حق پناه، رضا (۱۳۷۷). جایگاه قانون و قانون‌گرایی در قرآن، مجله فلسفه، کلام و عرفان، شماره ۱۴.
- شیرزاد، کامران (۱۳۸۸). جرایم رایانه‌ای از دیدگاه حقوق جزای ایران و حقوق بین‌الملل، تهران: نشر بهینه فراگیر.
- عالی پور، حسن (۱۳۹۰). حقوق کیفری فناوری اطلاعات، ج اول، تهران: نشر خرسندی.
- عبداللهی، جواد (۱۳۸۳). موانع و محدودیت‌های اعمال نظارت کارآمد، مجموعه مقالات سومین همایش نظارت کارآمد.
- کریمیان، محمد وزین (۱۳۸۰). نظارت شکلی - نظارت ماهوی، دومین همایش علمی و پژوهشی نظارت و بازرسی.
- کونتز و همکاران. اصول مدیریت، ترجمه: طوسی و همکاران، جلد دوم.