# پژوهش

سال هفتم شماره ۶۲ تیر ۱۳۹۳

## نظارت الکترونیک و کاهش جرایم با منشاء رایانه و فضای مجازی

مرکز مطالعات و پژوهش‌های سلامت اداری و مبارزه با فساد

آدرس: تهران خیابان طالقانی-تقاطع خیابان شهید سپهبد قرنی سازمان بازرسی کل کشور

طبقه ششم- مرکز مطالعات و پژوهش‌های سلامت اداری و مبارزه با فساد

تلفن: ۶۱۳۶۲۳۰۷

نشانی الکترونیک: bazrasi.research@136.ir

www.Bazresi.ir


بسم الله الرحمن الرحيم

# گزارش پژوهشی

سال هفتم، شماره ۶۲، تیر ۱۳۹۳

# نظارت الکترونیک و کاهش جرایم با منشاء رایانه و فضای مجازی

پژوهش و تألیف
بهزاد پورنقدی

ناظر علمی:
دکتر معزالدین باباخانی تیموری

مرکز مطالعات و پژوهشهای سلامت اداری و مبارزه با فساد

این گزارش برگرفته از پروژه پژوهشی «الزامات و راهکارهای نظارت الکترونیک بر جرایم رایانه‌ای از سوی سازمان بازرسی» است که با حمایت اداره کل بازرسی استان سمنان اجرا شده است.
مطالب مندرج در این گزارش پژوهشی نشانگر دیدگاه نویسندگان آن بوده و لزوماً نمایانگر دیدگاه سازمان بازرسی کل کشور نمی‌باشد.
کلیه حقوق مربوط به گزارش حاضر متعلق به سازمان بازرسی کل کشور بوده و هرگونه انتشار مطالب آن بدون کسب اجازه از این سازمان، غیر مجاز می‌باشد.

# فهرست مطالب

## اشاره

امروزه با گسترش حوزه فعالیت سازمان ها، ادارات و نهادهای دولتی، وقوع جرایم و تخلفات با پیچیدگی خاصی صورت می گیرد که شناسایی و کشف این نوع جرایم و تخلفات مستلزم داشتن توانایی و تخصص لازم است. نظارت الکترونیک و استفاده از رایانه و آشنایی با فناوری اطلاعات دانش کافی و توانایی لازم در این زمینه را به کارشناسان، متخصصان و بازرسان سازمان بازرسی کل کشور به منظور تحقق اهداف سازمانی و مقابله اصولی و تخصصی با جرایم و تخلفات اداری اعطا می کند.

با توجه به روند روبه گسترش استفاده از فناوری های نوین و رایانه در ادارات و دستگاه های دولتی و تخصیص اعتبارات عمده در این زمینه، مسئولیتی خطیر و مهم به عهده سازمان‌های نظارتی می باشد و این امر با نظارت سنتی امکان پذیر نیست. بنابراین به منظور نظارت مناسب و تخصصی بر عملکرد دستگاه ها در بکارگیری فناوری اطلاعات و ابزارهای رایانه‌ای می باید از ویژگی ها و امکانات آن اطلاع کامل و فنی را دارا بود و با شناخت جرایم و تخلفات اداری، سازمانی و رایانه ای، از وقوع آنها جلوگیری و یا درصورت وقوع آنها را شناسایی و به مقابله با آن پرداخته شود.

تالیف و انتشار این کتاب، که خلاصه‌ای از آن را در قالب گزارش پژوهشی حاضر در اختیار همکاران قرار گرفته است، می تواند به ارتقای سطح کیفی و تخصصی بازرسان سازمان بازرسی کل کشور و همچنین سایر دستگاه‌های نظارتی در کشف تخلفات و مقابله با جرایم اداری و رایانه-ای کمک نماید.

**مرکز مطالعات و پژوهش‌های سلامت اداری و مبارزه با فساد**

# نظارت الکترونیک و کاهش جرایم با منشاء رایانه و فضای مجازی

بهزاد پورنقدی[1]

## سرآغاز

با ورود در قرن بیست و یکم که موسوم بـه عصـر ارتباطـات و اطلاعـات است، ضرورت ایجاد تحول در نظام‌های اداری و انجام اصلاحات سـاختاری با وضوح بیشتری نمایان می‌شود. در جهان متحولی کـه منـابع آن در برابـر نیازها و انتظارات، روز به روز کاستی می‌گیرد، دولت‌ها برای کارآمـد شـدن، تحـت فشـارهای زیـادی هسـتند و از سـازو کارهـای گونـاگونی بـرای رفـع مشکلات و کاستی‌ها استفاده مـی‌کننـد. در نظـام‌هـای اداری ناکارآمـد، انـواع بی‌نظمی به‌صورت و اشکال گوناگونی ظهور می‌کنند. از جمله پیچیـدگی بـیش از حد، نارسایی و نقص در قوانین و مقررات و اجرای آنها، بی‌توجهی نسـبت به قوانین و مقررات، ضعف نیروی انسانی، سازش کارگزاران دولتی با افـراد و گروه‌های بـا نفـوذ، شـالوده‌هـای سسـت و نامتناسـب سـازمانی، انحصـار مشاغل، ضعف سیستم مدیریت و... که در نهایت این بی‌نظمی‌ها و بـه عبـارت دیگر این الگوهای رفتاری بر روی هم تـأثیر گذاشـته و حتـی اثـر یکـدیگر را تشدید می‌نمایند. به طور کلی می‌توان گفت کـه عامـل اصـلی لـزوم تحـول و اصلاح در سیستم مدیریت دولتی و سازمان‌ها و ارگان‌های وابسته به دولـت، معضلات ناشی از اندیشه‌های کلاسـیک مـدیریتی و نظـام نظـارت ناکارآمنـد سنتی و قدیمی است (باقری، ۱۳۸۷).

---

۱ - استادیار دانشگاه آزاد اسلامی، واحد بوئین زهرا و پژوهشگر دفتر تحقیقات کاربردی فرماندهی انتظامی استان سمنان، پست الکترونیک: behzad_pournaghdi@yahoo.com

تعدد سازمان‌های نظارتی و عدم هماهنگی و ارتباط سیستمی و قانون‌مند میان سازمان‌های نظارتی، موجب انجام فعالیت‌های موازی، تکراری و پرهزینه می‌شود. این ناهماهنگی‌ها و عدم ارتباط سبب شده تا حاصل اقدامات و نتیجه فعالیت دستگاه‌های نظارتی، برای یکدیگر قابل بهره‌برداری و قابل استفاده نباشد. هرچند ارتباطات مقطعی و غیر متمرکزی میان آنها وجود دارد، اما این ارتباطات کافی نبوده و اهداف مورد نظر در زمینه نظارت و بازرسی را تامین نمی‌کند و باید در یک سیستم ارتباطی صحیح، نتایج اقدامات نظارتی هر یک از سازمان‌های نظارتی بر اساس یک راهبرد مشخص مورد بهره‌برداری قرار گیرد (عبداللهی، ۱۳۸۳). در راستای هماهنگی سازمان‌های نظارتی، تنظیم سیاست گذاری مشخص و تدوین برنامه‌های راهبردی و چگونگی همکاری دستگاه‌ها، امری اجتناب‌ناپذیر است. تبادل اطلاعات، استفاده از ظرفیت‌های موجود سازمان‌های نظارتی و توسعه فعالیت‌های نظارتی بر مبنای برنامه و هدف و به طور کلی اعمال مدیریت نظارت در کشور، تضمین‌کننده سلامت اداری و امنیت اقتصادی و اجتماعی، قضائی، سیاسی و فرهنگی است و این مهم در شرایط کنونی جهان، موسوم به دنیای اطلاعات و ارتباطات تنها با اجرای سیستم نوین نظارت الکترونیکی امکان‌پذیر خواهد بود.

اصولاً تشکیلات بازرسی و دستگاه‌های نظارتی بایستی خارج از دستگاه-های اجرایی (نظارت شونده) باشند. زیرا نهادهای نظارتی در این صورت کشف فساد و تخلف، به طور مستقل و بدون تعصّب سازمانی و جهت‌گیری تعاملی با متخلف و عامل فساد و بدون اینکه تحت تأثیر عوامل داخلی قرارگرفته باشد؛ موضوع را بررسی می‌کنند. به دلیل این‌که اغلب مدیران و یا کارکنان بخش اجرایی به مرور زمان با کاستی‌های و نارسایی‌های سیستم اداری و سازمانی اُنس پیدا می‌کنند، وجود و تکرار آن را عامل وقوع تخلف و فساد محسوب نمی‌کنند. اما اگر افراد و بازرسانی بیرون از دستگاه اجرایی،

عملکرد سازمان را بررسی کنند، بهتر و سریعتر به وجود کاستی‌ها، نواقص سازمانی، نارسایی‌ها و حتی تخلفات اداری و فساد پی می‌برند. گاهی اتفاق می‌افتد که در یک سازمان، به طور همزمان، بازرسان و یا ناظرین مختلفی از ارگان‌های نظارتی برای نظارت و بازرسی عملکرد آن دستگاه حضور پیدا می‌کنند. اغلب این امر موجب عدم استقبال و در بعضی مواقع نیز با عدم ارائه اطلاعات کامل و کافی توسط سازمان‌های نظارت شونده مواجه می‌گردد (دادگر، ۱۳۸۰). به همین دلیل وجود یک سیستم نظارتی یکپارچه و الکترونیک می‌تواند از وقوع چنین مشکلاتی جلوگیری نموده و به بهبود عملکرد نهادهای نظارتی کمک نماید. بدین ترتیب از امکانات، منابع و نیروهای بازرسی و نظارتی استفاده بهینه به عمل می‌آید و اطلاعات جمع‌آوری شده، به طور هماهنگ مورد تجزیه، تحلیل و استنتاج قرار می‌گیرد.

**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 است و موجب ناتوانی و یا کاهش توانایی 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 که توسط افرادی خارج از سازمان‌های نظارتی و به وسیله کارکنان و مسئولان دستگاه‌های دیگر 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 کامپیوتری، رسانه‌های دیجیتال، تجهیزات الکترونیک و اتوماسیون در 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 بر 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... 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 راه‌دور 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[۱]، ارتقای سطح خدمات و کاهش هزینه‌ها می‌باشد.

---

[۱] Electronic Data Interchange

گسترش حجم عملیات، پیچیده شدن معاملات و انجام آنها به‌صورت الکترونیکی، باعث شده که اسناد الکترونیکی جایگزین اسناد کاغذی و سنتّی شود. به تبع آن نیز، روش‌های کنترل، نظارت و بازرسی نیز دچار تغییر و تحول زیادی شده است. از این‌رو ضروری است که نهادهای نظارتی به‌دلیل این تغییرات و تاثیر آن بر عملکرد سیستم‌های سازمانی، فرآیند نظارت و بازرسی را به‌صورت 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.

### فضای مجازی و سایبری[۱]

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 مجموعه‌هایی 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 می‌شود و دیگر زمان معنایی ندارد. در واقع می‌توان گفت فضای مجازی گسترده‌ای از ذهن است که می‌تواند تمامی اشکال زندگی واقعی را بسط و معنا دهد. مهمترین تحول در عرصه علم و دانش، توسعه و گسترش و کاربرد علوم کامپیوتر و فناوری اطلاعات[۲] است که در سال‌های اخیر شاهد پیشرفت‌های چشمگیری در این

---

[۱] Cyberspace

[۲] Information Technology (IT)

زمینه بوده‌ایم و امروز این علم در خدمت و کمک رسانی به سایر علوم برآمده و در تمامی ابعاد زندگی مردم و تکالیف روزمره ایشان دخیل و حائز اهمیت است. فناوری اطلاعات و ارتباطات[۱] در ابعاد گسترده‌ای وارد حیطه-های مختلف کاری جوامع بشری شده است و حوزه نظم و امنیت نیز از این قاعده مستثنی نیست. به طور کلی سیستم دستگاه‌های قضائی، نظارت و بازرسی، انتظامی و امنیتی با به کارگیری دانش فناوری اطلاعات و ارتباطات، باعث افزایش توان اجرایی خود در تحقق اهداف و آرمان‌ها، کشف فساد، مبارزه با جرایم و تخلفات و همچنین نظارت بر حسن جریان امور و اجرای درست قوانین و مقررات در جامعه و تشکیلات اداری کشور خواهند شد. امروزه تحولات عظیمی در تکنولوژی 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 اطلاع-رسانی بین‌المللی دستاوردهای زیادی را به همراه داشته است.

فناوری اطلاعات دستاورد تلاش های علمی بشر و تجلی آرمان‌های ذهنی انسان است و اکنون در هزاره سوم و در عصر دانایی و انفجار اطلاعات قرار داریم. امروز به عقیده بسیاری از صاحب‌نظران، جهان در آستانه یک انقلاب اجتماعی نوین قرار دارد و زمینه این انقلاب را حرکت از جامعه کشاورزی به جانب جامعه صنعتی و در نهایت به سوی جامعه فراصنعتی مهیا ساخته است. این تحول نوین که انقلاب اطلاعاتی نام گرفته است به همان اندازه انقلاب صنعتی اهمیت دارد. چنان‌که به سبب آن، پردازش داده‌ها و تبادل اطلاعات به تولید کالای صنعتی و تجاری اولویت می‌یابد و فناوری اطلاعات به یک پدیده ابرصنعتی بدل خواهد شد. در عصر حاضر کشورهای ابرقدرت از نظر اقتصادی، نظامی، سیاسی و علمی را میزان اطلاعات آن کشور و توانایی‌های ارتباطی و فناوری اطلاعات مشخص می‌نماید. جوامع دارای

---

[۱] Information Communication Technology (ICT)

تکنولوژی اطلاعات و فناوری‌های گسترده ارتباطات، از جایگاه ویژه و مهمی در طبقه‌بندی پیشرفت و رشد و شکوفایی برخوردار هستند. در مسیر شکل‌گیری جوامع مدرن اطلاعاتی، اصلاح زیرساخت‌های ارتباطی و اطلاع‌رسانی، ایجاد امکانات لازم برای تولید و به کارگیری فناوری‌های نوین اطلاعاتی در سطوح مختلف، آموزش نیروی انسانی متخصص و تعیین استراتژی مشخص در زمینه فناوری اطلاعات و رسانه اهمیت بسزایی دارد. فناوری اطلاعات سایر علوم و فنون را با یکدیگر پیوند داده است و به انتشار علم و دانش و تسریع در فتح مرزهای علوم و فناوری کمک نموده است. تبادل اطلاعات بزرگترین و مهمترین تعهد فناوری اطلاعات نسبت به بشریت است که باعث انفجار اطلاعات در عصر حاضر و هزاره سوم گردیده است. در این زمان پیشرفت علم از حالات رکود و پیمایش آهسته و آرام خود به سمت جلو خارج گردید و به یک سیستم متحرک، پویا و فعال تبدل شده است. سیستمی که حجم داده‌های آن در عرض چند سال چندین برابر شد و میزان آن در طول یک دهه از تمامی یافته‌های قرون گذشته بیشتر گردید. حصول این دستاوردها و یافتن اطلاعات بسیار، تنها با وجود فناوری‌های نوین و فناوری اطلاعات امکان‌پذیر شده است.

با روند توسعه روزافزون فناوری اطلاعات در سطح جهان و ایران، موفقیت و شکوفایی طرح‌های علمی، فنی و عمرانی با استفاده از این فناوری تحقق می‌یابد. همچنین در اجرای سیاست‌های کلان دولتی و سازمان‌های اجرایی، طرح ها و بنگاه‌های اقتصادی، توسعه آموزش و پژوهش، استفاده از ظرفیت‌های موجود و حداکثر توان فنی و مهندسی و اجرای پروژه‌های کاربردی ضرورت و نیاز به استفاده از فناوری اطلاعات مشخص شده است. یک روزنامه نگار و محقق به نام «اندرو ناچیسون» در مقاله‌ای درباره جامعه و فناوری اطلاعات به نکات مهمی اشاره نموده که می‌تواند ذهن هر مخاطبی را در هزاره سوم به خود مشغول کند. او در این مقاله به تحولات عظیم دنیا

در هزاره سوم و با تکیه به فناوری قرن یعنی فناوری اطلاعات و ارتباطات اشاره می‌کند و می‌نویسد: که در نتیجه آن هر کسی در دنیا می‌تواند فارغ از زمان و مکان و بدون هیچ مرزی به سراسر دنیا سرکشی کند و خود به یک رسانه تبدیل شود. این زیباست که ما می‌توانیم اطلاعات و عقاید خود را بسیار سریع‌تر از گذشته در سراسر دنیا به اشتراک بگذاریم و در حقیقت فناوری اطلاعات و ارتباطات حجم غیرقابل تصوری از موضوعات را برای اشتراک فراهم می‌آورد. در فضای مجازی کاربران می‌توانند به هرگونه خدمات اطلاعاتی و الکترونیکی دستیابی داشته باشند. این دسترسی به خدمات بدون درنظر گرفتن فاصله جغرافیایی و مرزهای بین‌المللی در هر نقطه از دنیا واقع امکان‌پذیر است. محیط سایبر زمینه فعالیت‌های اقتصادی مهم و ابزار ضروری برای انجام کلیه معاملات تجاری و در سطح بین‌المللی بدون دخالت مستقیم بشر فراهم آورده است. محدوده فعالیت کاربران فضای مجازی به مرزهای فیزیکی محل سکونت، محل کار و حتی مرزهای یک کشور محدود نیست و در یک با صرف هزینه بسیار کم، هر کاربر می‌تواند در هر زمان و در هر مکانی با افراد دیگر در هر نقطه‌ای از جهان تبادل اطلاعات کند، بدون اینکه از محل واقعی و هویت فرد دیگر اطلاعی داشته باشد. از نظر اقتصادی، فضای سایبر را می‌توان یک بازار واحد جهانی محسوب کرد که از ثمره‌های موفق جامعه مبتنی بر تکنولوژی مدرن اطلاعاتی به دست آمده است که با روند توسعه آن، روابط اجتماعی و سنّتی و فرهنگی حاکم بر روابط افراد را در سطح جامعه دچار تحول می نماید (باستانی، ۱۳۸۳).

**جرایم سایبری**

جرایم سایبری طیف وسیعی از بزه‌کاری‌ها را شامل می شود 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، معضلی 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 فناوری برتر و وسایل پیشرفته-تری می باشد. مرتکبین این جرایم با استفاده از فناوری نوین و ابزارهای جدید به اهداف شوم خود دست پیدا می‌کنند، بدون آن‌که اثری همانند جرم کلاسیک 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 بگیرند. 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 فراملی و فراسرزمینی به خود گرفته است. فناوری‌های نوین در این عرصه و پیشرفت تجهیزات ارتباطی، مخابراتی و الکترونیکی، سهولت وقوع جرایم جرم 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 می-خورد.

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. 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 به‌صورت ماشین – ماشین تغییر یافته است، که بیشترین مورد تحقق آن در جرایم تجارت الکترونیکی و جرایم بانکداری الکترونیکی است (عالی پور، ۱۳۹۰: ۸۹). باتوجه به این مسئله، امروزه هم وسیله ارتکاب این جرایم متفاوت و مدرن است و هم مرتکبین آنها اشخاص خاص و دارای مهارت و تخصص هستند. ابزارهای به‌کار گرفته شده در این گونه از جرایم، انواع مختلفی دارد و هر روز نیز پیشرفته‌تر و توسعه‌یافته‌تر می‌شوند. در بند (و) از ماده (۲) قانون تجارت الکترونیک؛ سیستم رایانه‌ای چنین تعریف شده است: «سیستم رایانه‌ای هر نوع دستگاه یا مجموعه‌ای از دستگاه‌های متصل سخت افزاری و نرم افزاری است که از طریق اجرای برنامه‌های پردازش خود کار داده پیام عمل می‌کند». همین تعریف در ماده (۱) قانون جرایم رایانه ای مصوب خرداد ۱۳۸۸ مجلس شورای اسلامی نیز آمده است. در ماده (۱) از کنوانسیون جرایم سایبر، سیستم رایانه‌ای چنین تعریف گردیده: «سیستم رایانه‌ای دستگاهی است که از نرم افزار و سخت افزاری که برای پردازش خودکار داده های دیجیتالی طراحی شده، تشکیل یافته و ممکن است شامل ورودی، خروجی و امکانات ذخیره ساز اطلاعات شود، سیستم رایانه‌ای می‌تواند به‌صورت مستقل یا متصل به شبکه‌ای از سایر دستگاه‌های مشابه عمل کند». منظور قانون‌گذار از خودکار این است که انسان در فرایند پردازش دخالت مستقیم ندارد. منظور از پردازش داده‌ها؛ داده‌های سیستم رایانه‌ای با اجرای یک برنامه رایانه‌ای

عمل کند. یک برنامه رایانه‌ای مجموعه‌ای از دستورالعمل‌هاست که رایانه می‌تواند آنها را برای نتیجه مورد نظر اجرا کند. رایانه می‌تواند برنامه‌های مختلفی را اجرا کند که معمولاً سیستم رایانه‌ای از دستگاه‌های مختلفی تشکیل شده است که به پردازشگر یا واحد پردازش مرکزی و سایر تجهیزات جانبی تفکیک می‌شود (جلالی فراهانی، ۱۳۸۹). فضای سایبر شامل شبکه‌های رایانه‌ای و مخابراتی متصل به هم است که اطلاعات را در کمترین زمان و بدون محدودیت مکانی مبادله می‌کند. در این فضا، جرایم و تخلفات با سرعتی بیشتر نسبت به فضای حقیقی ارتکاب می‌یابند که در نتیجه به دلیل شیوه‌های مختلف و کثرت ارتکاب این جرایم، عنوان جدیدی به نام «جرایم سایبری» پیدا کرده‌اند.

**بررسی جرایم رایانه‌ای**

در علوم رایانه و حقوق، جرایم رایانه‌ای را می‌توان چنین تعریف نمود: هرگونه عمل خلاف قانون که با سوءنیت، از طرف شخص یا اشخاص با بکارگیری از کامپیوتر 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 کردن 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 ارتباط نامشروع. داستان‌های اینترنتی مستهجن تهدید جدی برای سلامت اخلاقی جوانان می‌باشد که آنها نسبت به خطرات این نوع داستان‌ها آگاه نیستند. در یک تقسیم‌بندی کلی می‌توان جرایم رایانه‌ای را به شرح ذیل مطرح نمود:

۱- جرایم سنتی که شامل: جاسوسی، تخریب، جعل، کلاهبرداری، تخریب، افترا، پولشویی و قاچاق مواد مخدر

۲- جرایم ناظر به کپی رایت برنامه‌ها
۳- جرایم علیه حمایت از داده‌ها
٤- جرایم در تجارت الکترونیکی
٥- جرایم در بانکداری الکترونیک
٦- جرایم مخابراتی و ماهواره‌ای
۷- جرایم علیه اطفال و زنان
۸- سایبر تروریسم.

به طور کلی جرایم رایانه‌ای به دو دسته تقسیم می‌شوند که در ادامه این بخش به تشریح این جرایم و همچنین قانون جرایم رایانه‌ای پرداخته می شود:

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 باشد 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 رخ می‌دهند جرم رایانه ای قلمداد می‌شود که از این دیدگاه جرایم نیز به ۳ 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 ویروسی کردن که صرفاً در فضای سایبر «مجازی» اتفاق می-افتد.

در کنوانسیون بین‌المللی بوداپست (۲۰۰۱) چیزی تحت عنوان جرم رایانه‌ای مطرح نشده، بلکه در فضای مجازی از جرم سایبر نام برده شده است که در فارسی به جرم مجازی[۱] تعبیر می‌شود. در اسناد و کنوانسیون‌های بین‌المللی پیرامون جرایم رایانه‌ای رویکردی 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 تلقی شده است. در کشور ما تعاریفی که در قانون جرایم کامپیوتری آمده؛ جرم‌ها را به جرایمی از قبیل کلاهبرداری کامپیوتری، جعل کامپیوتری، تغییر، محو، متوقف‌سازی، جاسوسی کامپیوتری، ملاحظه در خطوط ارتباطی، تخریب کامپیوتری، دستیابی غیر مجاز، شنود غیرقانونی و غیره تقسیم کرده و مجازات‌هایی برای برخورد با این جرایم در نظر گرفته شده است.

**بازرسان سایبری و الکترونیکی:**

بازرسان آینده مجبور خواهند بود که فرایند بازرسی و نظارت بر حسن اجرای قانون را به‌وسیله روش‌ها و تکنیک‌های بازرسی الکترونیک اجرا نمایند. امروزه بازرسان می‌توانند پرونده‌های مهمی را در زمینه کشف انواع فساد اداری و یا تخلفات سازمانی و جرایم رایانه‌ای، بدون ترک دفتر کاری خود به سرانجام برسانند. همچنین در آینده‌ای نزدیک، بازرسان و کارشناسانی که در مقابل انقلاب رایانه‌ای مقاومت کنند، هرگز اقدامی را با حصول موفقیت دربر نخواهند داشت.

---

[۱] Virtual Crime

**بررسی صحت و اصالت اسناد الکترونیکی:**

بازرسان و یا کارشناسانی که اسناد و مدارک تولید شده در جریان کشف را دریافت می کند، باید آنها را ساماندهی و ثبت و ذخیره نمایند. ساماندهی یا طبقه‌بندی اسناد و مدارک با توجه به میزان مفید و مرتبط بودن آنها با مورد یا موارد مطروحه می‌باشد. همچنین، بازرسان می‌توانند در بررسی و بازبینی حجم عظیمی از ادله الکترونیک از کمک سیستم‌های رایانه‌ای نیز بهره‌مند شوند و موارد مورد نیاز را با توجه به کلمات کلیدی ضروری مورد جستجو و بازبینی قرار دهند. ادله الکترونیک نسبت به اسناد و مدارک کاغذی سنتی؛ بیشتر در معرض نابودی، تغییر، دستکاری و یا دسترسی غیر مجاز قرار دارند. تاریخ و زمان مربوط به ادله الکترونیکی که توسط سیستم‌های عامل رایانه‌ای ایجاد و نگهداری می شود، به آسانی قابل تغییر هستند. این موضوع یکی دیگر از چالش‌های سیستم نظارت و بازرسی الکترونیک خواهد بود. زیرا با تغییر زمان ایجاد و ثبت داده‌های الکترونیکی، استنادپذیری ادله‌های الکترونیکی نیز از بین می‌رود و یا با مشکل روبرو خواهد شد.

در سایه یک دستورالعمل اجرایی از سوی سازمان بازرسی کل کشور به‌عنوان بالاترین نهاد نظارت و کنترل و بازرسی، می‌توان دستگاه‌های اجرایی، وزارتخانه‌ها، سازمان‌ها، ادارات و نهادهای دولتی و یا وابسته به دولت را ملزم به استفاده از یک سیستم مدیریت اسناد به منظور ثبت، نگهداری و ذخیره اسناد الکترونیکی نمود که این اقدام ضمن ایجاد یک سازوکار مدیریت جامع اسناد، فرایند نظارت و بازرسی الکترونیک و جستجوی فایل‌های مربوط به یک موضوع خاص را در جریان نظارت و بازرسی تسهیل می‌نماید. اگر تلاش شود که اسناد الکترونیک به هنگام تولید دسته‌بندی شوند، از محدوده اسناد غیرضروری در جریان بازرسی کاسته می‌شود و کشف تخلفات و یا فساد اداری با سهولت و دقت بیشتری انجام می‌شود. با اجرای این روش، سازمان بازرسی می‌تواند از سیستم مدیریت یکپارچه اسناد

الکترونیک برای شناسایی تخلفات و جرایم رایانه‌ای در سازمان‌های دیگر و تحقق نظارت و بازرسی الکترونیک استفاده نماید. همچنین با اجرایی شدن سیستم نظارت و بازرسی الکترونیک توسط سازمان بازرسی کل کشور، دسترسی به اسناد بالقوه، مهم و مرتبط با سوء جریان و تخلفات اداری، می‌توان به نظارت بر تولید و ارائه خدمات، حسن انجام وظایف سازمانی و اجرای صحیح قوانین و مقررات، حذف بوروکراسی، صرفه‌جویی در زمان و هزینه‌های نظارت و بازرسی، اصلاح سریع ساختارهای معیوب اداری و تشکیلات سازمانی، بررسی همه جانبه و نسخه برداری از اسناد الکترونیکی؛ فارغ از زمان و مکان و در هر شرایط جغرافیایی، اقدام نمود. سازمان‌ها و تشکیلات اداری کشور باید به امر آموزش کارکنان در زمینه ثبت و نگهداری ادله الکترونیک توجه نمایند و درباره انواع تهدیدهای الکترونیکی، فعالیت‌های غیرقانونی، تخلفات و جرایم رایانه‌ای که می‌بایست از آنها خودداری کنند، راهنمایی لازم را داشته باشند (ارسال پیام‌هایی از قبیل اظهارنظرها و لطیفه‌های جنسی یا نژادی، اظهارنظرهای انتقادی درباره یک جریان سازمانی و...). کارکنان ادارات و سازمان‌ها باید بدانند که چگونه امنیت سیستم رایانه‌ای خود را در مقابل تهدیدها و مخاطرات موجود در فضای سایبری و مجازی، شبکه‌های رایانه‌ای و اینترنت تأمین نمایند. همچنین باید به آنها توصیه شود که اسناد و مدارک مهم و حساس را با گذاشتن علامت «محرمانه» و در صورت لازم با اعمال روش‌های رمزنگاری و کدگذاری از این اسناد محافظت نمایند.

همچنین در خصوص کشف اسناد و ادله الکترونیکی و مبارزه با جرایم رایانه‌ای، سازمان بازرسی کل کشور می‌تواند با تربیت نیروهای متخصص و مجرب، به کارگیری تجهیزات رایانه‌ای مدرن و سیستم‌های پیشرفته نظارت الکترونیکی، برنامه فراگیری برای کشف فساد اداری، جرایم و تخلفات رایانه-

ای و دسترسی به اسناد الکترونیکی تهیه و اجرا نماید. در ادامه این بخش، اجرای برنامه‌ها و اقداماتی در این خصوص پیشنهاد می‌گردد:

طراحی و اجرای برنامه مدیریت جامع اسناد الکترونیک در تمامی وزاتخانه ها، سازمان‌ها، ادارات، تشکیلات و نهادهای دولتی و یا وابسته به دولت؛ شناسایی، نگهداری و دسترسی به داده‌ها و اسناد الکترونیکی مورد نیاز نهادهای نظارتی و بازرسی را تسهیل می‌سازد. همچنین استفاده از مشاوران و متخصصان فناوری اطلاعات، آموزش و انتصاب یک کارشناس و مسئول یا گروهی از کارکنان آموزش دیده برای پاسخ به درخواست‌های سازمان بازرسی و یا سایر نهادهای نظارتی در خصوص نگهداری و ارائه اسناد و ادله الکترونیک می‌تواند راه‌حلی مناسب برای سازمان‌ها و نهادهای اجرایی کشور باشد.

### مجرمان الکترونیکی و جرایم رایانه‌ای[۱]

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 می‌دهد. این زنجیره شامل سیستم مبدأ، مقصد،

---

[۱] Data and Information.

مسیر، مدت ارسال، تاریخ، اندازه و حجم، دوام یا نوع خدمات اصلی ارایه شده است (همان، ص ۲۲).

**مرتکبین جرایم رایانه‌ای:**

این دسته از جرایم گاهی از لحاظ مرتکبین جرم با جرایم سنتی تفاوت دارند. ارتکاب این نوع جرایم مستلزم میزان خاصی از اطلاعات و دانش است که این امر تعداد افراد قادر به ارتکاب این جرایم را محدود می‌کند. در نظام کیفری کلاسیک و قدیم تنها به جرم و مجازات توجه می‌شد و عامل وقوع جرم یعنی مجرم تا حدّ زیادی مورد شناسایی قرار نمی‌گرفت از این رو در این نظام فاعل جرم، انسان یا حیوان بود فرقی نمی‌کرد و کودکان نیز همچون افراد بالغ مسئول و قابل مجازات بودند (ولیدی، ۱۳۸۲، ص ۲۷۵). در بینش قانون‌گذار کشور، مفهوم بزه‌کار با مفهوم بزه؛ پیوندی نزدیک دارد، زیرا برای تحقق جرم علاوه بر عنصر مادی محتاج به عنصر دیگری یعنی عنصر روانی است. برای تحقق یک جرم، وجود عنصر روانی لازم و ضروری است. عنصر روانی یعنی این‌که فعل مجرمانه باید نتیجه اراده و خواست مجرم باشد و مجرم به نقض قوانین هم آگاه باشد. بنابراین مجرم برای ارتکاب جرم و بزه-کار بودن باید پیش از همه از توانایی درک و اراده برخوردار بوده و شخص حقیقی یا حقوقی باشد. اگر نسبت انسان را با عنصر مادی جرم مورد سنجش قرار دهیم، بزه‌کار کسی است که جرم را به صورت عنصر مادی مرتکب شده و یا به اجرای آن مبادرت نموده است. همچنین ممکن است مجرم و بزه کار به عنوان مباشر، شریک و یا معاون مرتکب جرم شود (همان، ص ۲۷٦).

**مجرمین رایانه‌ای:**

مرتکبین جرایم رایانه‌ای به دو دسته تقسیم می‌شوند:

۱- مجرمانی که برای انتفاع شخصی، مالی و یا اقتصادی اقدام به ارتکاب جرم نموده و به دنبال منافع هستند.

۲- مجرمانی که صرفاً برای ارضای حس کنجکاوی خود مرتکب جرم رایانه‌ای می‌گردند (شیرزاد، ۱۳۸۸، ص ۷۸).

گروه دوم عموماً کاربران و افراد متخصصی هستند که قصد خرابه کاری و یا ایجاد بحران در سیستم‌های رایانه‌ای و یا داده‌ها را ندارند.

در یک تقسیم‌بندی دیگر، مجرمان رایانه‌ای نیز به دو گروه مجاز و غیر مجاز تقسیم می‌شوند. مجرمینی که مجاز به دسترسی داده‌ها و اطلاعات یک رایانه یا شبکه هستند و از آن سوء استفاده می‌کنند و مجرمینی که به طور غیرمجاز به این ابزارها و اطلاعات دست می یابند و از این طریق مرتکب جرم می شوند (همان، ص ۷۹). در ارتکاب جرایم رایانه‌ای عموماً منظور این است که مجرمان چندان هم باهوش نبوده و برای تخریب سیستم‌های رایانه‌ای یا نفوذ و افشای اطلاعات، اگر چه سطح خاصی از آگاهی‌ها و اطلاعات لازم است، اما این اقدام به معنای نبوغ و هوش سرشار مجرمان این دسته از جرایم نیست (خداقلی، ۱۳۸۳).

**خصوصیات سازمانی جرایم رایانه‌ای:**

در تقسیم بندی مجرمین رایانه‌ای به مجاز و غیرمجاز مشاهده کردیم 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 سازمان یافته هم توجه کرد. برخی تروریست‌های رایانه‌ای به صورت سازمانی اقدام به اجرای عملیات تروریستی و خرابه کارانه 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، ص۹۰).

**تصویب قانون برای مبارزه با جرایم رایانه‌ای**

با توجه به گسترش امکانات رایانه‌ای و مخابراتی در سطوح مختلف جامعه و دسترسی سازمان‌ها و ارگان‌های دولتی به فناوری‌های نوین ارتباطی و رایانه‌ای، امکان سوء استفاده از این امکانات توسط کاربران عمومی فضای سایبر، کارکنان و یا شاغلین و یا افراد وابسته به سازمان‌ها، ادارات، ارگان‌ها و شرکت‌های حقوقی وجود دارد. جرایم و تخلفات رایانه‌ای در سطوح مختلف سازمانی می‌تواند با استفاده از آدرس‌ها و دامنه‌های ثبت شده اینترنتی در فضای سایبری و یا پست الکترونیکی شخصیت حقوقی، سوء استفاده از خطوط مخابراتی و یا دسترسی و افشای داده‌های رایانه‌ای محرمانه صورت پذیرد. همچنین در حالی که بسیاری از کشورهای جهان شرایط استفاده از امضای دیجیتال را فراهم نموده‌اند، در کشور ایران موضوعی درباره ارگان اداره کننده یعنی مرکز گواهی ریشه (یکی از عناصر مهم زیر ساخت کلید عمومی) درحال بحث و بررسی است. چنین مرکزی در رأس مجموعه‌های سلسله مراتبی قرار گرفته و مراجع فرعی را تصدیق می‌کند. شناخت ماهیت و نقش این مرکز در ایجاد اعتماد نسبت به تراکنش های الکترونیکی، قضاوت آگاهانه درباره نهاد اداره کننده آن را ممکن می‌سازد (بختیارونـد، ۱۳۸٦: ۱۹۳). از جمله راهکارهای امنیتی درباره پیغام‌های الکترونیکی، استفاده از مکانیسم‌های معروف به امضاهای الکترونیکی[۱] است. امضای الکترونیکی به کاربران کمک می‌کند هنگام دریافت پیغام در اینترنت پدید آورنده آن را شناخته و به اصالت آن اطمینان یابد. در دنیای امروز با

[۱] Digital Signature

روند روبه گسترش استفاده از فناوری‌های نوین و رایانه با مسائل و مشکلات جدیدی مواجه هستیم. سازمان‌ها و دستگاه‌های دولتی به‌منظور ارائه خدمات بهتر به مراجعین و افزایش سرعت ارائه خدمات و کاهش هزینه-ها اقدام به استفاده از فناوری اطلاعات و ابزارهای رایانه‌ای در سطح وسیعی نموده‌اند. همچنین شمار رشد کاربران فناوری اطلاعات در ایران به سرعت در حال افزایش است. استفاده از فناوری‌های نوین ارتباطی و رایانه‌ای دارای مزایای بی‌شماری است و لیکن علوم رایانه و فناوری اطلاعات مسائل و مشکلات خاص خود را به همراه آورده است که جامعه و سازمان‌ها را تحت تاثیر قرار می‌دهد. جرایم و تخلفات رایانه‌ای توسط متخصصین فناوری اطلاعات و کاربران رایانه که دارای اطلاعات وسیعی در این زمینه هستند، صورت می‌پذیرد که وقوع آن در خلاف جهت اهداف مصالح ملّی و اجتماعی جامعه است.

بنابراین وقوع جرایم و تخلفات رایانه‌ای با پیچیدگی خاصی صورت می-گیرد که شناسایی و کشف این نوع جرایم و تخلفات مستلزم داشتن توانایی استفاده از رایانه و آشنایی تخصصی با فناوری اطلاعات می‌باشد تا با استفاده از دانش کافی و توانایی لازم در این زمینه به مقابله اصولی و تخصصی با این نوع جرایم و تخلفات پرداخت و از ادامه آن جلوگیری نمود. قانون جرایم رایانه‌ای به لحاظ ساختار با رعایت اصول کنوانسیون جرایم سایبر که در سال ۲۰۰۱ در بوداپست مجارستان به تصویب شورای اروپا رسید، تدوین شده است. بنابر آمارهای رسمی بیش از ۳۵ میلیون کارت الکترونیکی نزد کاربران سامانه‌های خدمات الکترونیکی بانک‌ها، ۱۰ میلیون کارت نزد کاربران سامانه هوشمند سوخت و ۵۰ میلیون مشترک تلفن همراه و ثابت و ۳۲ میلیون کاربر اینترنت در کشور وجود دارد.[۱] در سال ۱۳۸۸ در

[۱] خلاصه گزارش اظهارنظر کارشناسی درباره لایحه جرایم رایانه‌ای، مرکز پژوهش‌های مجلس شورای اسلامی، ۱۳۸۷/۵/۱۹.

ایران بیشترین جرایم رایانه‌ای و اینترنتی و طرح شکایت در حوزه فناوری اطلاعات مربوط به ثبت دامنه در فضای سایبر و اختلاف بر سر دامنه بین اشخاص حقیقی و حقوقی بوده است و پس از این موضوع اختلاف بین کاربران اینترنت با شرکت‌های سرویس‌دهنده و سپس اختلاف بین شرکت-های اینترنتی و سرویس دهندگان با یکدیگر است که بیش از ۸۵ درصد از این دعاوی به سازش و صدور حکم منجر و پرونده مختومه اعلام شده و در برخی موارد که نیاز به کار کارشناسی بوده جهت بررسی بیشتر بسته نشده است.[۱] در سال ۱۳۸۵ تعداد ۷۹ پرونده در خصوص جرایم رایانه‌ای به سیستم پلیس آگاهی کشور وارد شده است که ۳۳ درصد پرونده‌ها در رابطه با موضوع دسترسی غیرمجاز به سیستم‌ها و داده‌های رایانه‌ای، بخشی از آن دسترسی‌های غیرمجاز در حوزه فعالیت‌های بانکی، ۳۰ درصد پرونده‌ها با موضوع هتک حیثیت افراد و نشر اکاذیب، ۱۶ درصد پرونده‌ها با موضوع کلاهبرداری‌های اینترنتی یا تولید و انتشار برنامه‌ها و کدهای مخرب و فریب سیستم‌های رایانه‌ای، ٦ درصد بحث تخریب و اختلال در داده‌های سیستم و ٥ درصد تکثیر غیرمجاز نرم‌افزارها و محتوای دیجیتال بوده است.[۲] امروزه تولیدکنندگان محتوا به یک سری بنگاه‌های خاص محدود نیستند و هر فرد می‌تواند انواع رسانه‌ها از جمله رادیو اینترنتی، پادکست و برنامه‌های تصویری ایجاد کند. مهمترین جرایم اینترنتی در جهان انتشار اخبار کذب، ارسال مطالب، تصاویر و فیلم‌های مستهجن، آموزش و تبلیغ تروریسم، هتک حرمت افراد، استفاده از فضای متعلق به دیگران، ارسال پیام‌های مخرب، اخلال دسترسی دیگران در فضای سایبری، دین زدایی، هک و ویروسی کردن سایت‌ها و... می باشند. استفاده از فضای سایبر نیز یک فناوری جدید

---

[۱] تارنمای گرداب؛ مرکز بررسی جرایم سازمان‌یافته وابسته به فرماندهی پدافند سایبری سپاه پاسداران انقلاب اسلامی ایران.

[۲] سرهنگ مهرداد امیدی، معاون مبارزه با جرایم خاص رایانه‌ای پلیس آگاهی کشور.

برای ارتکاب جرم است. لذا به دلایل زیر وضع حقوق جزای مستقل برای جرایم رایانه‌ای ضرورت دارد:

۱- دنیای مجازی به طور سمبلیک، دنیایی جدید است که باید از طریق قانون‌گذاری مستقل مانند دنیای واقعی آن را به نظم درآوریم.

۲- مجرمان سایبر از لحاظ جرم‌شناسی از مجرمان عادی متفاوت هستند و قوانین جزایی و مجازات‌های متفاوتی را نیاز دارند.

۳- ضرر و زیان‌های ناشی از جرایم سایبر بسیار بیشتر از جرایم عادی است.

٤- مشکلات ناشی از کشف جرم و تعقیب متهمان و به مجازات رساندن آنها و خاصیت بین‌المللی این جرایم به آنها ماهیتی متفاوت از جرایم سنتّی می‌بخشد.

نکته اساسی در جرایم اینترنتی حذف مکان در قلمرو مکان فیزیکی و محدود حاکمیت سیاسی است. ممکن است جرم در خارج از محدوده جغرافیایی و قلمرو حاکمیت کشور انجام شود و جرم انگاری لازمه نادیده گرفتن اصل صلاحیت سرزمینی و توسعه مرزهای جغرافیایی است. در ادامه به واکنش تقنینی کشورها در مورد جرایم رایانه‌ای پرداخته می‌شود که واکنش نانوشته کشورها در برابر تجاوز و تعدی به ارزش‌ها در ٥ مرحله، سیستم قضائی خود را جهت در برگرفتن قوانین مربوط به جرایم رایانه‌ای اصلاح کردند و این پنج مرحله عبارتند از:

مرحله یکم: حمایت از اطلاعات خصوصی.

مرحله دوم: ایجاد و اصلاح قوانین ناظر به جرایم رایانه‌ای.

مرحله سوم: وضع قوانین جدید جهت حمایت از دارایی‌های غیرمادی.

مرحله چهارم: تفکیک قوانین موجود با قوانین و موضوعات جدید.

مرحله پنجم: اصلاح قوانین در مورد جرایم مربوط به محتوا.

همچنین یکی از دغدغه‌های اصلی امروز دنیای سایبر، محتوای ناخواسته الکترونیکی یا همان اسپم[۱] است که ماهیتی تبلیغاتی دارد و با مقاصد تجاری و غیرتجاری برای کاربران سیستم های پیام‌رسان الکترونیکی ارسال می-شود. به‌طور کلی، اقداماتی که باید در چارچوب قانون‌گذاری انجام شود را می‌توان در دو محور گنجانید: ۱- مبارزه با محتوای غیرقانونی، ۲- جرم-انگاری علیه محتوای ناخواسته و زیان‌بار.

**تصویب قانون جرایم رایانه‌ای در ایران**

قانون جرایم رایانه‌ای شامل ۳ بخش اصلی، ٥٦ ماده و ۲۵ تبصره است و در روز سه شنبه مورخ پنجم خرداد ماه یکهزار و سیصد و هشتاد و هشت (۱۳۸۸/۳/۵) در صحن علنی به تصویب مجلس شورای اسلامی و مورخ بیستم خرداد ماه یکهزار و سیصد و هشتاد و هشت (۱۳۸۸/۳/۲۰) به تأیید شورای محترم نگهبان رسیده است. این قانون دارای سه بخش اصلی به شرح زیر است:

بخش یکم – شامل ۸ فصل (ماده ۱ تا ۲۷) جرایم و مجازات‌ها
بخش دوم – شامل ۳ فصل (ماده ۲۸ تا ۵۱) آیین دادرسی
بخش سوم (ماده ۵۲ تا ٥٦) سایر مقررات

**نقش قوه قضائیه در مقابله با جرایم رایانه‌ای**

از پدیده‌هایی که رایانه و پس از آن اینترنت همراه خود به ارمغان آورد، مخاطراتی بود که بر سراسر قلمرو گسترده این حوزه سایه انداخته است. اگر این مخاطرات مورد بی‌توجهی جامعه و مسئولین قرار گیرد، بسیار بزرگ و گاهی غیر قابل جبران خواهد بود. زیرا آسیب‌های روانی ناشی از کاربری نادرست و خلاف قانون، موجب اختلال در رفتار شهروندان شده، جامعه را

[۱] Spam

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 و امنیت اجتماعی و برقراری امنیت پایدار دچار چالش‌های جدی می‌کند. در قانون اساسی، به بیان امنیت اجتماعی در ۳۰ محور پرداخته شده است و قوه قضائیه 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. قوه قضائیه 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 کشور و جلوگیری از هرگونه بی‌نظمی و فعالیت‌های غیرمجاز، کشف جرایم و تخلفات، مجازات متخلفین و مجرمین از وظایف سیستم قضائی کشور است. حضور به موقع بازرسان قوه قضائیه و نظارت محسوس یا نامحسوس تشکیلات قضائی و سازمان بازرسی کل کشور می‌تواند از آشفتگی سازمانی و یا وقوع جرایم رایانه‌ای پیشگیری کرده و به کنترل و حفاظت از منابع و سرمایه‌های کشور کمک کند.

**اقدامات قانونی و مقابله با جرایم رایانه‌ای**

فناوری‌های مدرن الکترونیکی جایگاه ویژه‌ای در زندگی روزمره بشر پیدا کرده است. این فناوری‌ها از یک می‌تواند به عنوان ابزارهایی در دست مجرمان و تبهکاران قرار گیرد و ارتکاب جرم را تسهیل کند و از سوی دیگر سازمان بازرسی، نهادهای قضائی و سیستم عدالت کیفری و حقوقی نیز از این ابزارها برای کشف جرم و شناسایی مجرمان و جمع‌آوری دلایل و مدارک علیه آنان استفاده می‌کنند و دلایل علمی که از این طریق به دست می‌آید در ردیف محکمه پسندترین دلایل و مدارک به شمار می‌روند. هم اکنون در بسیاری از کشورهای جهان، کنترل هویت اشخاص در مرزهای ورودی و خروجی، تعقیب و مراقبت از مجرمان جهت کشف فعالیت‌های تبهکارانه، تسهیل ترافیک شهری و جاده‌ای، سیستم‌های هوشمند اعلام سرقت به پاسگاه‌های پلیس، نظارت بر فعالیت سازمان‌ها ادارات و بسیاری دیگر از فعالیت‌های دولتی و خصوصی با بهره‌برداری از ابزارهای الکترونیکی صورت می‌گیرد. استفاده از فناوری نه تنها در پیشگیری از وقوع جرم و تخلف کاربرد وسیعی پیدا کرده است بلکه در شناسایی و کشف و مجازات مجرمان نیز از جایگاه ویژه‌ای برخوردار است. علاوه بر استفاده از این ابزارها در کنترل زندانیان و نظارت بر اعمال آنان، این فناوری‌ها گاهی توانسته‌اند به عنوان جایگزین مجازات زندان عمل کنند. هرچند که استفاده از این فناوری‌ها در کشور ایران رواج چندانی پیدا نکرده است، لیکن با توجه به توسعه و گسترش روزافزون فناوری اطلاعات و علوم رایانه‌ای در کشور، سیستم های نظارت و بازرسی ناگزیر به استفاده از ابزارهای نظارت الکترونیکی در سیستم کنترل و نظارت و بازرسی خود خواهند بود. روش‌های قانون‌گذاری و اقدامات قانونی برای مبارزه با جرایم رایانه‌ای به دو حوزه ملی و فراملی (بین‌المللی) تقسیم می شود. روش‌های قانون‌گذاری ملی، فراسرزمینی و مختلط ناشی از پذیرش دکترین اثرگذاری در حاکمیت بر

فضای سایبر است، اما روش‌های خود انتظامی و بین‌المللی ناشی از پذیرش دکترین میراث مشترک بشریت در حاکمیت بر فضای سایبر می باشد (ضیایی، ۱۳۸۸).

**قانون‌گذاری ملی:**

«قانون‌گذاری ملی»، احاله قدرت به قانون‌گذاران داخلی کشورها است که هر کشور و حکومتی به طور مستقل حق وضع قوانین در این رابطه را خواهد داشت. به عنوان مثال کشور آمریکا تعدادی قانون کیفری تصویب نموده که در آن نقض توافقات بین‌المللی مرتبط با ارتباطات رادیویی و یا تلگرافی را جرم انگاری کرده است. در کشور آمریکا اختلال همراه با سوء نیت خاص در وظایف فراملی و ماهواره‌ای در سطح بین‌المللی همچون کلاهبرداری تلگرافی، جرم تلقی شده است و این روش تبعات نامطلوبی به دنبال دارد. با تکیه بر قانون‌گذاری ملی نمی‌توان از جرم انگاری کلیه جرایم علیه بشریت در فضای سایبر و حوزه بین‌المللی اطمینان خاطر داشت[۱].

**قانون‌گذاری فراملی:[۲]**

در «قانون‌گذاری فراملی»، کشورها موظف به وضع قوانین ملی با آثاری بین‌المللی هستند، چنان‌که در صلاحیت جهانی به وضع چنین مقرراتی می‌پردازند. این روش نیز معضل چند کیفری را به‌دنبال دارد، خصوصاً در این مورد که دولت‌ها و افراد جامعه نمی‌دانند کدام قانون را باید پاس داشته و در نهایت مجبور خواهند بود مضیق‌ترین قانون را رعایت نمایند (حافظی و خرم‌آبادی، ۱۳۸۳: ٤١).

---

[۱] Graham J. H. Smith, op. cit., p. ٥٣٣

[۲] Exterritorial

**اقدامات و روش خود انتظامی:[۱]**

برخی حقوقدانان بین‌المللی معتقدند حقوق حاکم بر فضای سایبر از جمله حقوق بشر، می باید در پروسه تبادلات کاربران آن ایجاد گردد. همان طور که حقوق تجارت بین‌الملل طبق عرف موجود میان بازرگانان ایجاد شده است. در این دیدگاه، اینترنت به عنوان تابع حقوق بین‌الملل، واضع و مجری حقوق بشر خواهد بود. یکی از مزیت‌های این روش، مؤثر بودن قواعد آن است. زیرا این قواعد توسط جامعه‌ای تدوین شده که قرار است آن را اجرا نماید. یکی دیگر از قابلیت‌ها و مزیت‌های این روش، تخصصی بودن آن است. زیرا این قواعد توسط جامعه‌ای مدون شده که نسبت به مقامات بیرونی از تخصص بیشتری برخوردار است. از دیگر مزیت‌های این روش، اجرای آسان و راحت شدن این قواعد توسط کاربران است.[۲]

**نظام قانون‌گذاری بین‌المللی:**

در مناسب‌ترین روش با انعقاد کنوانسیون‌های بین‌المللی، موضوع حقوق بشر در فضای سایبر را به عنوان یکی از شاخه‌های حقوق بین‌الملل شاهد خواهیم بود. این روش که بسیاری معایب روش‌های قبلی را نیز به همراه ندارد و تنها با مانع تعارض منافع دولت‌ها روبرو است. به این معنا که دولت-هایی که از نظر تکنولوژیک پیشرفته‌تر بوده و تأمین کننده خدمات اینترنتی هستند، روش قانون‌گذاری ملی یا فراملی را ترجیح می‌دهند. این در حالی است که کشورهای ضعیف‌تر که از نظر فناوری اطلاعات و ارتباطات در حوزه فضای سایبری از دیگر جوامع عقب‌تر هستند، علاقه‌مند به بین‌المللی شدن این حقوق خواهند بود. اولین تلاش برای مقابله با جرایم سایبری و سایبر تروریسم در عرصه بین‌المللی به اواخر قرن بیستم باز می‌گردد.

---

[۲] Self-regulating

[٤] Henry H. Perritt, JR. Cyberspace Law Journal, vol. ۱۲, ۱۹۹۹, p. ٤۲۳.

**شناسایی و کشف جرایم رایانه‌ای**

امروزه فعالیت‌های سایبری و تعاملات مجازی جزء اصلی و جدا ناشدنی از زندگی افراد محسوب می‌شود. بدیهی است با پیشرفت روز افزون دانش فناوری اطلاعات از این‌گونه فعالیت‌ها سوء استفاده‌هایی نیز می‌شود که می‌تواند پیامدهایی را به دنبال داشته باشد. به همین دلیل است که اهمیت تدوین و اجرای قوانین رایانه‌ای، مقررات سایبری و سیستم نظارت و بازرسی الکترونیکی مطرح می‌شود. اگر به نتایج تحقیقات به‌دست آمده در طی سال‌های اخیر توجه کنیم، شاهد آن خواهیم بود که بیش از ۸۵ درصد شرکت‌ها و سازمان‌های بزرگ دنیا با شکاف‌های امنیتی در ساختار سازمانی خود مواجه بوده‌اند. همچنین سازمان امنیت ملی (داخلی)[۱] کشور آمریکا رسماً اعلام کرده است، سالانه در اثر بروز جرایم رایانه‌ای، بیش از ۱۰ میلیارد دلار از سرمایه کشور از بین می‌رود. کشف جرایم رایانه‌ای، شامل استفاده از یک سری روش‌های هدفمند از تکنیک‌ها و دستورالعمل‌ها برای به‌دست آوردن و جمع‌آوری آثار جرم از تجهیزات و سیستم‌های اطلاعاتی، محاسباتی و انواع دستگاه‌های ذخیره‌سازی اطلاعات و رسانه‌های دیجیتال است، به گونه‌ای که بتوان آنها را در یک قالب منسجم و قابل ارائه و مفهوم در نهادهای قضائی و حقوقی و نظارت و بازرسی ارائه کرد. همچنین به فرآیند نگهداری، شناسایی، استخراج، تفسیر و مستندسازی آثار و شواهد کامپیوتری که دارای ویژگی‌های قانونی یک اثر جرم از قبیل: انجام شدن فرآیندهای قانونی، صحت و تمامیت اثر جرم، گزارش‌دهی درست اطلاعات به‌دست آمده و در نهایت صدور رأی از یک دادگاه قانونی و یا ارائه یک گزارش بازرسی توسط نهادهای نظارتی و بازرسی، کشف جرایم رایانه‌ای گفته می‌شود. در واقع کشف جرایم رایانه‌ای یک علم است که عمل دریافت، پردازش و شناسایی داده‌ها و ادله الکترونیک از کامپیوترها به روشی انجام می‌شود که تمامی

---

[۱] FBI

آثار، مدارک و اسناد به‌دست آمده در محاکم حقوقی و مراجع قضائی قابل ارائه باشند. همچنین کشف جرایم رایانه‌ای مترادف است با بررسی صحنه وقوع جرم و یا کالبد شکافی هدفی الکترونیکی که جرم بر روی آن انجام شده است. مهمترین نیازهایی که در کشف جرایم رایانه‌ای می‌توان مطرح نمود؛ نیاز به بررسی اکثر مستندات الکترونیکی مهم، جستجو و دریافت داده‌ها از رایانه‌ها می‌باشد. در این خصوص قطعاً مسئله صحت و اصالت داده‌ها و ادله الکترونیکی مطرح می‌باشد. در صورتی‌که در نگهداری ادله الکترونیک و یا فایل‌های دیجیتال سهل‌انگاری شود، این مدارک و مستندات به راحتی قابل تخریب و از بین رفتن هستند. در فرآیند کشف جرایم رایانه‌ای برای بازگردانی اثرات جرم معمولاً با استفاده از تکنیک و روش‌های خاص فایل-های حذف شده، فایل‌های رمزنگاری شده و همچنین فایل‌های تخریب شده را برای بررسی‌های بیشتر بازگردانی می‌کنند.

دانش کشف جرایم رایانه‌ای هنوز در مراحل توسعه و مقدمات خود قرار دارد. بنابراین نمی‌توان چنین دانشی را با کشف آثار جرم در جرایم سنتی و روش‌های دیگر مقایسه کرد، زیرا آثار و انواع جرم دیجیتال همواره در حال تغییر هستند. سازمان‌ها و نهادهای نظارتی و بازرسی همواره با فقدان آموزش در خصوص ارتقای سطح مهارت و تخصص کارشناسان و بازرسان روبه‌رو هستند. یکی دیگر از مشکلات کشف جرایم رایانه‌ای توسط سازمان بازرسی، عدم وجود وحدت رویه و یک روش یکسان و دسترسی به ابزارهای کشف جرایم رایانه‌ای است. همچنین نظارت و بازرسی الکترونیک در حال حاضر به‌صورت سلیقه‌ای مورد استفاده قرار می‌گیرد که با چنین روشی، اعمال نظارت همه جانبه و مناسب الکترونیکی امکان‌پذیر نخواهد بود.

مراحل کشف جرایم رایانه‌ای توسط بازرسان قضائی:

در خصوص کشف جرایم و تخلفات رایانه‌ای و حفظ ادله الکترونیک، مراحل و روش‌هایی ذیل برای آگاهی بازرسان سازمان بازرسی ارائه می-

گردد. بدیهی است رعایت نکات فنی و تخصصی در این خصوص می‌تواند در اقدامات نظارتی و بازرسی در زمینه کشف فساد و جرایم موثر باشد.

۱- ضروری است مجموعه سازمان بازرسی کل کشور از اخبار مردمی و همکاری خبرگان و متخصصان علوم رایانه‌ای و فناوری اطلاعات و ارتباطات بهره‌مند گردد.

۲- بازرسان از مسئولین فناوری اطلاعات و انفورماتیک ادارات و تشکیلات مورد بازرسی جهت همکاری و مشاوره دعوت کنند.

۳- کارشناس جرایم رایانه‌ای و بازرسان الکترونیک می‌بایست از کلیه شواهد، اسناد، ادله الکترونیک و مدارک موجود به‌صورت کامل یک نسخه پشتیبان و یا به تعداد کافی کپی تهیه کنند.

٤- کارشناس جرایم رایانه‌ای کلیه شواهد، مدارک و مستندات را به لابراتوار تخصصی کشف جرم در سازمان بازرسی منتقل کنند.

٥- بازرسان در صورت نیاز؛ مدیران، مسئولین، کارشناسان و یا کارکنان ذیربط را برای پاسخگویی فرا بخوانند.

٦- ضروری است کارشناسان جرایم رایانه‌ای و بازرسان الکترونیک، کلیه فایل‌ها را برای یافتن شواهد و مدارک مربوط به ارتکاب جرم آزمایش کنند و صحت و اصالت اسناد، شواهد و مدارک به‌دست امده اطمینان حاصل نمایند.

۷- بازرسان پس از بررسی مدارک و انجام بازرسی‌های لازم، گزارش مربوط به کارشناس جرایم رایانه‌ای را به‌صورت کامل مطالعه کرده و دفاعیات و شواهد را به صورت قابل قبول برای ارائه در گزارش پیوست می-نمایند.

استفاده از افرادی بی‌تجربه و غیرمتخصص در فرآیند بازرسی و کشف آثار جرایم رایانه‌ای باعث نامعتبر شدن اثر جرم و شواهد و مدارک موجود خواهد شد، فلذا لازم است همواره در این عرصه از افراد متخصص استفاده گردد.

**مفهوم دسترسی غیر مجاز**

در بین کارشناسان حقوقی و متخصصین علوم رایانه‌ای، نسبت به مفهوم دسترسی غیر مجاز، وحدت رأی و اتفاق نظر وجود ندارد. متخصصین فنی از عبارت «هکینگ»[۱] استفاده می‌کنند که تعریف این اصطلاح عبارت است از «هر نوع حمله به سیستم‌های و حفاظت شده رایانه‌ای». برخی کارشناسان عملیات هک را در معنی محدودتر شامل «نفوذیابی» یا «نفوذگری»، تعریف می‌کنند. همچنین برخی دیگر از متخصصین، هک را مترادف با دسترسی غیر مجاز می‌دانند. متخصصین علم حقوق رایانه نیز از اصطلاحات دیگری مانند نفوذ غیر مجاز، ورود غیر مجاز، دستیابی غیر مجاز استفاده می‌کنند. به این ترتیب، دسترسی غیر مجاز عبارت است از: «دسترسی بدون مجوز به سیستم‌ها یا داده‌های رایانه‌ای (به‌صورت کلی یا جزئی) یا بدون نقض تدابیر ایمنی یا حفاظتی آنها.

**روش‌های افزایش کارایی نظارت و بازرسی**

نظارت و بازرسی نقش عمده‌ای در تغییر ساختار و اصلاح یک حکومت ایفا می‌کند. بنابراین ضروری است که روش‌های افزایش کارایی، پوشش، کیفیت و تأثیر نظارت و بازرسی را افزایش داد. در کشورهای غربی به دلیل شکل‌گیری نهادهای مختلف در یک دوره طولانی تاریخی و بر اساس نیازها و بتدریج به دور از کشمکش‌ها و تنش‌های تند اجتماعی و همچنین ثبات نهادهای سیاسی، اجتماعی و اقتصادی در نظام قضائی، پیشرفت‌های زیادی در نظارت و بازرسی و رسیدگی به تخلفات حاصل شده است. بنابر این، تدوین قوانینی که قابلیت برطرف کردن نیازها در بعد ملی را داشته باشد موجب استحکام و تثبیت موقعیت بین‌المللی کشور خواهد شد. در رژیم گذشته، نظارت و بازرسی توسط دو نهاد بازرسی شاهنشاهی و دفتر ویژه

---

[۱] Hacking

اطلاعات انجام می‌شده که در جمهوری‌اسلامی این اختیارات به بازرسی کل کشور محول شده است. به رغم امید بسیاری که از این بازرسی‌ها چه در گذشته و چه در حال انتظار می‌رفت، به دلایل مختلف در عمل کارایی لازم را نداشته و به سطح مطلوب اثرگذاری دست نیافته است. بنابر این باید تعریف دقیقی از قوانینی که انگیزه فعالیت‌های فردی را تشویق می‌کند و همین‌طور برای کاربرد به‌وسیله مسئولان و ادارات مختلف قابلیت انعطاف کافی داشته باشد و در عین حال به فساد منجر نشود، در دست باشد. توجه به هزینه‌های اجتماعی که در اثر حذف فوری کارکردهای ضعیف به‌وجود می‌آید مهم است. به‌طور کلی در برنامه‌ریزی‌ها با توجه به شرایط فرهنگی و اجتماعی، باید از چالش‌هایی که نظارت و بازرسی دقیق و با کیفیت بالا در مبارزه با فساد و ناخالصی‌ها در سطح حکومت به‌وجود می‌آورد کاملاً آگاهی داشت. برای انجام اصطلاحات بایستی به موارد زیر توجه نمود:

۱- کنش‌های بین کارکردهای حاصله از نظارت و بازرسی و دستگاه‌های دولتی در رابطه با موقعیت‌ها و مسائلی که با آن سر و کار داریم.

۲- نقش تمرکز زدایی و تمایل شدیدی که به‌طرف تصمیم‌گیری‌های انحصاری وجود دارد.

۳- کمبود سازوکارهای مناسب ارزیابی کاربری نظارت و بازرسی.

٤- کمبود امکانات برای تربیت و اصلاح وضعیت حرفه‌ای کارکنان دولت برای هماهنگی با نظام بازرسی.

٥- نقش موثر و بسزای نظارت الکترونیک و شناخت روش‌های کارآمد بازرسی نوین.

لازم به ذکر است که فعالیت‌های مربوط به برنامه‌ریزی، بازرسی و نظارت و حفظ پویایی و کارآمدی آن در سطح ادارات دولتی، نیازمند تمرکز بر پنج محور ذیل است:

۱- مشارکت و توجه شهروندان

۲- ارزیابی کلی مدیریت
۳- تمرکز زدایی
٤- رفتار اخلاقی کارمندان
٥- نظارت و بازرسی الکترونیک

در این‌صورت و با افزایش کارآیی نظارت و بازرسی می‌توان انتظار داشت تا کیفیت خدمات دولتی در سطح کشور به نحو مطلوبی بالا رود. همچنین ضروری است نظارت و بازرسی بر روی سه بخش مهم تأکید نماید.

بخش اول: تعیین میزان نسبی فساد و سطح آن در سازمان‌های مختلف.

بخش دوم: توصیف و تشریح راهبردهای ضد فساد به کار گرفته شده.

بخش سوم: تعیین میزان موفقیت‌های حاصل از مبارزه با فساد.

در هر صورت به صرف انجام بازرسی و ارائه گزارش دقیق نمی‌توان در این امر موفقیت زیادی به دست آورد، مگر این‌که مدیران و مسئولان کلان کشور به مسئولیت خود متعهد باشند و بی‌طرفانه و بدون گروه‌گرایی، معیارهای ضد فساد را داوطلبانه و با جدیّت دنبال نمایند تا سلامت اداری در تمامی سطوح حاکم گردد.

**دولت الکترونیک**

یکی از مباحث مطرح در حوزه فناوری، ارتباطات و مدیریت «دولت الکترونیک» می‌باشد. این جنبه از ارتباطات رایانه‌ای و الکترونیک طی سال های اخیر در جهان مورد توجه قرار گرفته و بسیاری از سازمان‌های دولتی برای ارائه خدمات خود به مردم به استفاده از این پدیده روی آورده‌اند. دولت الکترونیک در واقع اصطلاحی است که به ارائه خدمات دولتی از طریق اینترنت و با به‌کارگیری ابزارهای رایانه‌ای اطلاق می‌شود. اصطلاح دولت الکترونیک به معنای کاربرد شبکه‌های کامپیوتری و هر نوع ابزار الکترونیکی دیگر، توسط وزارتخانه‌ها، سازمان‌ها و ادارات دولتی به سمت ارائه خدمات و

اطلاعات به مردم، شرکت‌ها و سایر سازمان‌های دولتی است. بدیهی است با توجه به گسترش روز افزون و بی‌حد و حصر اینترنت همانند هر فناوری و هر پدیده دیگر همانند تجارت الکترونیک، بانک الکترونیک و غیره نقش اینترنت و فناوری اطلاعات در دولت الکترونیک اهمیت پیدا می کند. از جمله مهمترین مزایای دولت الکترونیک آن است که همه افراد اعم از حقیقی و حقوقی سازمان و بخش‌های خصوصی و دولتی قادر می‌شوند از طریق اینترنت و رایانه و به دور از محدودیت‌های مکانی و زمانی به اطلاعات و خدمات دولتی دسترسی پیدا کنند.

از جمله مصادیق بارز مزیّت چنین دولتی را می‌توان از بین رفتن رانت و کاهش فساد و تخلفات اداری دانست. در چنین سیستمی دیگر نیاز به حضور فیزیکی دو طرف (شهروندان و حکومت) در یک محل واحد وجود ندارد، بلکه هر یک از طرفین با استفاده از امکاناتی که شبکه اینترنت در اختیارشان می-گذارد به اصلاح امور می‌پردازند. شهروندان می‌توانند از طریق سایت اینترنتی و سازمان‌های دولتی به آن دست از خدمات و اطلاعات دولتی که مورد نیازشان است دسترسی پیدا کنند، صاحبان کسب و پیشه می‌توانند در جریان آخرین بخش نامه‌ها، مزایده‌ها و مناقصه‌های دولتی و... قرار گیرند و حلقه کامل کننده همه اینها دو سویه بودن این بستر است. به‌صورتی که از یک طرف مراجعه کنندگان به چنین سایت‌هایی، بتوانند به این اطلاعات دسترسی داشته باشند و از طرف دیگر صاحبان سایت‌ها بتوانند نه تنها از مراجعه کنندگان بازخورد داشته باشند بلکه مراحل بعدی چنین عملیاتی را تکمیل و مثلاً در یک مزایده الکترونیک شرکت کنند و قیمت‌ها و شرایط حضور را از طریق اینترنت به ثبت برسانند و نتیجه آن را هم در موعد مقرر از همین طریق مشاهده و دریافت کنند. دولت الکترونیک مزایای دیگری نیز دارد که در حالت کلی می‌توان به ارائه بهتر خدمات دولتی به شهروندان از طریق دسترسی به اطلاعات و اداره موثر امور دولت اشاره کرد. در نتیجه

این فرآیند، رانت خواری، مفاسد اداری و هزینه‌های دولت کمتر و دقت شفافیت امور آن بیشتر خواهد شد. توسعه علمی و عملی در همه زمینه‌های دانش بشری یک امر مسلم و بدیهی است که با سرعتی شگرف در حال رخ دادن می باشد و دولت‌ها نیز به عنوان مهمترین رکن ملی هر کشوری ناگزیر از این تغییر و تحولات درونی می‌باشند. دولت الکترونیکی از جمله مفاهیم و استراتژی‌هایی بوده است که موجبات تسهیل مدیریت دولتی را در اغلب جوامع فراهم کرده و به همین دلیل توجه به آن و عملیاتی کردن اندیشه زیربنایی آن مورد توجه قرار گرفت که در همین مسیر جهانی نیز دولتمردان ما با هوشیاری و اندیشه حسن مدیریت در جهت استفاده و کاربست چنین مفهومی گام برداشتند. نظارت الکترونیکی مهمترین رکن و اهرم دولت الکترونیکی را به خود اختصاص داده است. به طور اساسی این نوع نظارت در جهت آرمان کلی نظارت الکترونیکی بوده و مهمترین ابزار در راه دست-یابی به اهداف آن را شامل می‌شود. نظارت الکترونیکی با هدف کاهش نظارت و مراجعات حضوری و افزایش استفاده از ارتباطات الکترونیکی به دنبال سازوکارهای مناسب و کارآمد است. ورود به قرن بیست و یک و عصر اطلاعات، با چالش‌ها و نگرانی‌های بسیار جدی همراه بوده است به‌طوری که هیچ یک از برنامه‌های توسعه‌ای طراحی شده و فناوری‌های نوین قرن بیستم نتوانسته‌اند تأثیر قاطعی بر حل این مسائل و تبعات ناشی از بروز آنها به‌جا گذارند (کِلی، ۲۰۰۳)[۱] و دولتمردان، انقلاب فناوری اطلاعات می‌تواند نقشی اساسی در مواجهه با این چالش‌ها داشته باشد (بکوس، ۲۰۰۱).[۲] فرانک وبستر[۳] به همراه کوین رابینز[۴] در کتابی با عنوان «عصر فرهنگ فناورانه: از جامعه اطلاعاتی تا زندگی مجازی» با کندوکاو در معانی اجتماعی و فرهنگی

[۱] Kelley, ۲۰۰۳

[۲] Backus, ۲۰۰۱

[۳] Frank Webster

[۴] Kevin Robbins

فناوری‌های نوین بر اجتناب ناپذیر بودن زندگی بشر در شرایطی تاکید می‌کند که اطلاعات و بسترهای تکنولوژیکی اطلاعاتی و ارتباطی به عنوان شاخص اصلی توسعه و پیشرفت هر جامعه‌ای محسوب می‌شود (وبستر و رابینز، ۱۳۸۵). یکی از مهمترین فرصت‌هایی که این فناوری پیش‌روی دولتمردان و مدیران قرار می‌دهد، امکان مهندسی مجدد و افزایش قابلیت دسترسی، تقویت کارآمدی و پاسخگوتر ساختن دولت است که استفاده از آن در فرآیند حکومت داری موجب پدیداری و پایدار شدن واقعیتی به نام دولت الکترونیکی است که لازمه دولت‌ها در جوامع اطلاعاتی امروز است (هو، ۲۰۰۲)[۱]. با توجه به تحولات در سطح جهان یکی از بخش‌هایی که تحت تأثیر تحولات جهانی قرار گرفته است بخش عمومی و سازمان‌های دولتی می‌باشند. دولت الکترونیکی به ارائه اطلاعات و خدمات دولت از طریق اینترنت یا سایر ابزارهای دیجیتال به‌صورت آنی اطلاق از «مدیریت کیفیت فراگیر» می‌شود. دولت الکترونیکی می‌تواند تعدادی از اهداف اصلی جمله مشتری محوری، توانمندسازی جوامع، کارکنان و مشتریان، اثربخشی و کارآیی را برای بخش عمومی محقق نماید (استانتن و جولیان، ۲۰۰۲)[۲]. دولت الکترونیکی عبارت است از استفاده از فناوری اطلاعات و ارتباطات برای متحول کردن دولت و فرآیند حکومت داری از طریق ایجاد قابلیت دسترسی، کارآمدی و پاسخگوتر نمودن آن است. بر اساس تعریف دیگر، دولت الکترونیکی عبارت است از استفاده از فناوری اطلاعات برای بهبود خدمات و اطلاعات دولتی که برای شهروندان، کارمندان، تجار و آژانس‌های دولتی در نظر گرفته شده است (بلانگر، کارتر و شاوپ، ۲۰۰۵).[۳]

---

[۱] Ho, ۲۰۰۲

[۲] Stanton & Jolian, ۲۰۰۲

[۳] Belanger, Carter, & Schaupp, ۲۰۰۵

**کنترل، نظارت و بازرسی الکترونیک**

«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، دسته بندی و طبقه بندی، پردازش و ارایه گزارش‌های مدیریتی، تمامی این اطلاعات را در اختیار مدیران قرار دهد تا در نظام برنامه ریزی و نظارت مورد استفاده قرار گیرد (حسینی و فولادی طرقی، ۱۳۸۹: ٦٧٧). از سوی دیگر، یکی از شاخص‌های برجسته دین مبین اسلام؛ روزآمد بودن و تطابق آن با اوضاع و شرایط متحول زمان است. اجتهاد، کوششی است برای همگامی با پیشرفت‌های بشری برخاسته از نیازمندی‌ها. سرعت تحولات و توسعه دانش بشری، فرصت تفکر و تدبیر را در زدودن تردید و وسواس، می رباید. عقب‌ماندگی از خیل عظیم جهان مجازی و فوق پیشرفته، خسرانی است که جبران آن در تصوّر نمی‌گنجد. مجال آزمون و خطا و تجربه از کف‌ها ربوده شد. لذا برای جبران یک جانبه‌نگری بودجه‌ریزان کشور، تدابیری اندیشیده شده که هر یک، در خور توجه ویژه است. از آنجا که گزارش‌های سازمان، از حمایت‌های حقوقی و قضائی شایسته برخوردار نبود، کوشش شد که هر چه بیشتر به علمی و تخصصی‌تر شدن نزدیک شود. برای آن‌که با خاستگاه‌ها و مظاهر فساد به‌صورت‌ریشه‌ای و هدفمند برخورد شود، درصد بازرسی‌های مستمر و از پیش برنامه‌ریزی شده، افزایش یافت، جهت کاهش تنش‌ها و ابهامات، به‌جای گزارش‌های محیطی، بیشتر به گزارش‌های موضوعی روی آورده شد. همچنین برای جبران کمبود نیروی انسانی، همت بر آموزش نیروها و هرچه کیفی‌تر کردن آنها، معطوف گردید تا هر یک، جای چندین نفر فعالیت نمایند. از جمله، تجهیز مدیران و کارشناسان به فناوری اطلاعات، از آموزش دوره-

های فناوری اطلاعات[۱] و ICDL[۲] و آموزش الکترونیکی[۳] و تخصصی‌تر کردن دوره‌های آموزشی و مهارتی در مراحل نوآموزی، بازآموزی و آماده سازی، به این امید که با بهره‌گیری از ماشین افزار و رایانه، سیستم نظارت و بازرسی را هرچه بیشتر با پیشرفت‌های روز در بخش‌های نرم افزاری و سخت افزاری هماهنگ نمود. با مجازی شدن مدیریت، سازمان و دولت، رفته رفته به مجازی شدن جهان نزدیک می‌شویم چنان‌چه اعمال مدیریت امروزی، تنها منوط به حضور مدیر در محل مدیریت و سازمان مطبوع خود نیست و بخش اعظم آن با کنترل از راه دور (همانند روش‌های پیشگیری و درمان در امور پزشکی) انجام می‌شود؛ اعمال نظارت و بازرسی نیز، می‌تواند با بهره-گیری از دانش فنی روز، شدنی باشد. گرچه در تولید علم سهم چندانی نداریم، حداقل در چگونگی کاربرد و مصرف آن باید سهیم شد؛ این‌که بیاموزیم که چگونه آنچه را دیگر کشورها ساخته‌اند، بهره برداری نماییم.

با توجه به گستردگی دستگاه‌های اجرایی و تخصصی شدن فعالیت‌ها، منحصر کردن نظارت و بازرسی به شیوه‌های سنتی و به عبارتی، دستی و فیزیکی، همانند آن است که در انبار کاه به دنبال سوزن گشت. لذا در چنین اوضاعی، تنها راه حل، اعمال شیوه مدیریت نظارت و نظارت مجازی (الکترونیکی) است. شیوه‌ای که ما را به توسعه قضائی رهنمون می‌سازد. چرا که تحقق توسعه قضائی در گرو توسعه نظارت است و توسعه نظارت نیز، وابسته به مدیریت نظارت است؛ نه نظارت و بازرسی منفعلانه، موردی و مقطعی. شهروندان عادی می‌توانند از طریق سایت اینترنتی و سازمان‌های دولتی به آن دست از خدمات و اطلاعات دولتی که مورد نیازشان است دسترسی پیدا کنند، صاحبان کسب و پیشه می‌توانند در جریان آخرین بخش نامه‌ها، مزایده‌ها و مناقصه‌های دولتی و... قرار گیرند و حلقه کامل کننده همه

---

[۱] Information Technology (IT)

[۲] مهارت هفتگانه رایانه

[۳] E-Learning

این‌ها دو سویه بودن این بستر است. به‌صورتی که از یک طرف مراجعه‌کنندگان به چنین سایت‌هایی، بتوانند به این اطلاعات دسترسی داشته باشند و از طرف دیگر صاحبان سایت‌ها بتوانند نه تنها از مراجعه‌کنندگان بازخورد داشته باشند بلکه مراحل بعدی چنین عملیاتی را تکمیل و مثلاً در یک مزایده الکترونیک شرکت کنند و قیمت ها و شرایط حضور را از طریق اینترنت به ثبت برسانند و نتیجه آن را هم در موعد مقرر از همین طریق مشاهده و دریافت کنند. دولت الکترونیک مزایای دیگری نیز دارد که در حالت کلی می‌توان به ارائه بهتر خدمات دولتی به شهروندان از طریق دسترسی به اطلاعات و اداره موثر امور دولت اشاره کرد. در نتیجه این فرآیند، رانت خواری، مفاسد اداری و هزینه‌های دولت کمتر و دقت شفافیت امور آن بیشتر خواهد شد.

**ضرورت حرکت به سوی نظارت الکترونیک:**

نظارت یکی از مهمترین وظایف مدیریت است که از حساسیت ویژه‌ای برخوردار است. به‌طوری که اگر در جامعه‌ای بازرسی و نظارت صورت نگیرد، به زودی مرگ آن جامعه فرا خواهد رسید (خدمتی، ص ٤٧). البته ضرورت وجود نظارت به معنی نداشتن اعتماد به کارکنان سازمان نبوده و سفارش به داشتن یک نظام قوی نظارتی نیز به معنای توصیه به نداشتن اعتماد به کارکنان نیست، بلکه باید در یک عبارت کوتاه گفت: «اعتماد در سازمان خوب است ولی نظارت هم لازم است». آنچه بایستی مورد توجه قرار گیرد این است که، با توجه به اینکه نظارت و بازرسی امر مهم و خطیری محسوب می‌شود، چگونه می‌توان این امر خطیر را به نحو مطلوب انجام داد تا نه تنها از فساد و تباهی در سیستم پیشگیری نماید بلکه موجبات رشد و بالندگی را نیز فراهم آورد و به عنوان مانعی برای توسعه سازمان‌ها محسوب نگردد. راهکارهای کنونی ارزیابی در کشور ما بیشتر سنتی بوده و

بیشتر بر جنبه تنبیه متخلف تاکید دارند تا بر پیشگیری از وقوع تخلف، بنابر این نیاز به سیستم‌های نظارتی پیش‌نگر و روش‌های جلوگیری از وقوع جرم احساس می‌شود. امروزه سیستم‌های جدیدی برای نظارت و بازرسی ایجاد شده‌اند که استفاده از آنها می‌تواند در تسهیل امر نظارت و همچنین در افزایش دقت آن بسیار موثر واقع شود. یکی از این ابزارها، فرآیند مراکز ارزیابی است که بیشتر به عنوان یک فرآیند ارزیابی پیش‌نگر مطرح است. بنابر این فرآیند مراکز ارزیابی می‌تواند در جهت بهبود نظارت و ارزیابی در کشور کمک شایانی نماید.

از جمله مهمترین مزایای دولت الکترونیکی آن است که همه افراد اعم از حقیقی و حقوقی سازمان و بخش‌های خصوصی و دولتی قادر می‌شوند از طریق اینترنت و رایانه و به دور از محدودیت‌های مکانی و زمانی به اطلاعات و خدمات دولتی دسترسی پیدا کنند. در نتیجه این فرآیند، رانت‌خواری، مفاسد اداری و هزینه‌های دولت کمتر و دقت شفافیت امور آن بیشتر خواهد شد (نوروزیان، ۱۳۸۹). یکی از مؤلفه‌های مهم و مرتبط با دولت الکترونیکی که از ارکان آن محسوب می‌شود، نظارت الکترونیکی است. نظارت و بازرسی به طور عمومی معنای وسیع و جامعی در ادبیات مدیریتی پیدا می‌کند. دولت علاقمند به نظارت و بازرسی بر دستگاه‌های اجرایی خود است و سازمان‌ها نیز به طور طبیعی به سنجش و نظارت بر کارکنان خود علاقمند هستند. پیشرفت‌های تکنولوژیکی اخیر منجر به رشد و توسعه سریع این روش نظارتی در بیشتر سازمان‌ها و نهادهای اجتماعی و صنعتی بوده است (گرنت و هیگینز، ۱۹۸۹).[۱] در سال‌های اخیر پژوهش‌ها و مطالعات وسیعی در ارتباط با نظارت الکترونیکی صورت پذیرفته است و بیشتر سازمان‌ها از نظارت الکترونیکی به عنوان راهی برای تشویق و ترغیب عملکرد مطلوب در بین کارکنان خود استفاده می‌کنند. نظارت الکترونیکی می‌تواند علاوه بر استفاده

[۱] Grant & Higgins, ۱۹۸۹

ابزاری در جهت نظارت و سنجش کارکنان، گام مؤثری در جهت بازخورد دادن به آنها باشد و کارکنان را به طور مؤثری در جهت شناسایی بهبود مسائل و مشکلات کاری خود کمک کند (استانتن و جولیان، ۲۰۰۲).

**سازمان بازرسی و نظارت الکترونیک:**

سازمان بازرسی کل کشور به عنوان اهرم اصلی نظارت و ارزیابی بر دستگاه‌های مشمول شناخته می‌شود و همواره رسالت‌های مرتبطی را در همین مسیر پی‌گیری می‌کند. از سال ۱۳۸۵ سازمان بازرسی کل کشور همگام با دیگر بخش‌های کشور سعی در الکترونیکی کردن عملکرد خود نموده که در این راستا اقداماتی نیز صورت گرفته است که بیشتر آنها در مرحله اولیه خود متوقف شده‌اند و پاره‌ای نیز با لحاظ مشکلات و موانعی در حال اجرا هستند. نکته مشخص این است که بازرسی و نظارت الکترونیکی در ایران دچار چالش‌های جدی و مؤثری است که بی‌شک پاره‌ای از آنها به دلیل عدم ساختار مناسب و مدوّن نبودن، از دید و مسئولین دور مانده است. نظارت الکترونیکی[۱] به عنوان یکی از مهمترین ارکان و اهرم‌های دولت الکترونیکی می‌باشد که در جهت آرمان کلی دولت الکترونیکی بوده و یکی از مهمترین ابزارها در راه دست‌یابی به اهداف آن می‌باشد. نظارت الکترونیکی با هدف کاهش نظارت و مراجعات حضوری و افزایش استفاده از ارتباطات الکترونیکی به دنبال سازوکارهای مناسب و کارآمد است.

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 اطلاعاتی در سازمان‌ها در همین راستا است و سیستم برنامه‌ریزی منابع سازمان (ERP) یکی از طرح‌های اطلاعاتی و عملیاتی است که می‌تواند به‌صورت یکپارچه به

---

[۱] E-Monitoring

تمامی اطلاعاتی که در حین عملیات تولید می‌شود؛ نظم دهد و با ثبت، دسته-بندی و طبقه‌بندی، پردازش و ارائه گزارش‌های مدیریتی، تمامی این اطلاعات را در اختیار مدیران قرار دهد تا در نظام برنامه‌ریزی و نظارت و کنترل مورد استفاده قرار گیرد. سازمان‌های مدرن و مدیران آنها برای نقش و جایگاه اطلاعات اهمیت ویژه‌ای قائل هستند. اطلاعات به عنوان مواد خام سازمان، اطلاعات به عنوان دارایی، اطلاعات منبع ارزش افزوده، اطلاعات منبع راهبردی و اطلاعات یک منبع مهم تاکتیکی از جمله مواردی است که نظریه‌پردازان فناوری اطلاعات و ارتباطات جهت تبیین جایگاه و اهمیت اطلاعات در سازمان به آنها اشاره دارند. برنامه‌ریزی منابع سازمان، فرهنگ-سازمانی جدیدی است که با یکپارچه‌سازی سیستم‌ها و منابع اطلاعاتی سازمان با استفاده از شبکه‌های کامپیوتری، نظام تصمیم‌گیری و روند برنامه‌ریزی و حتی رفتار سازمان را تغییر دهد. به نظر برخی اندیشمندان مدیریت و فناوری اطلاعات، برنامه‌ریزی منابع سازمان یک سیستم اطلاعاتی جامع برای یکپارچه‌سازی رفتارهای اطلاعاتی سازمان است. تسخیر و استیلای اطلاعات و منابع اطلاعاتی در هزاره سوم بر تمامی شئون زندگی فردی، اجتماعی، اقتصادی، سیاسی و فرهنگی انسان، دیگر یک موقعیت، ابزار و توانایی لوکس و تشریفاتی نیست؛ بلکه ضرورت و نیازی است که بشر به عنوان یک مرحله از تاریخ پیشرفت خود به آن دست یافته است. بنابراین جوامع و سازمان‌ها تلاش می‌کنند که با مدیریت صحیح و برنامه‌ریزی بر اساس عناصر و فرآیندهای مشخص، منابع اطلاعاتی خود را ثبت، نگه‌داری، دسته‌بندی، تحلیل و اشاعه نمایند تا متخصصان، برنامه‌ریزان، مدیران و کارشناسان از آنها در تدوین برنامه‌ها و تصمیم‌گیری‌ها استفاده نمایند. این در حالی است که سازمان‌های بزرگ در جوامع پیشرفته سیر تکاملی سیستم‌های اطلاعاتی را پشت سر گذاشته اند. سیستم‌های برنامه‌ریزی منابع سازمان در حقیقت به عنوان سیستم‌های تصمیم‌یار در اختیار مدیریت

سازمان قرار می‌گیرند تا بتواند با مدیریت صحیح اطلاعات در تولید کالا یا عرضه خدمات، کم هزینه‌تر و با کیفیت بالاتری اقدام نماید و نیز از رقیبان خود پیشی بگیرد.

برای استفاده یا پیاده سازی این سیستم‌ها، سازمان‌ها باید مراحلی را پشت سر بگذرانند. برای پیاده‌سازی سیستم برنامه‌ریزی منابع سازمان، اولین گام انجام پروژه امکان‌سنجی و بررسی الزامات یا مقتضیات پیاده-سازی برنامه‌ریزی منابع سازمان است. مرحله امکان سنجی در فرآیند پیاده-سازی برنامه‌ریزی منابع سازمان بسیار پیچیده و گسترده است و نیاز به یک تیم کارشناسی ماهر با امکانات گسترده دارد که باید در قالب یک پروژه انجام شود. بخشی از فرآیند امکان‌سنجی، سنجش الزامات و شناسایی شاخص‌های آن است. سازمان بازرسی کل کشور نیز به دلیل حجم بالای عملیات نظارتی، همواره با تولید اطلاعات روبه‌رو می باشد و نیاز است که این منابع اطلاعاتی با مدیریت بهینه و مناسب ثبت، ذخیره‌سازی و مورد تجزیه و تحلیل قرار گیرند تا مدیران و برنامه‌ریزان بتوانند در تصمیم‌سازی-ها و برنامه‌ها از آنها استفاده نمایند. این سازمان به عنوان یک سازمان دولتی دارای حجم بالایی از عملیات است که در قالب پروژه‌ها و طرح‌هایی در حوزه نظارت و ارزشیابی با فراوانی زیادی در سراسر کشور پراکنده‌اند که در دست بهره‌برداری یا در دست ساخت و مطالعه هستند. تعدد و تنوع آمار و اطلاعاتی که ناشی از این عملیات است چنان بالا است که به‌صورت روزانه حجم فراوانی از داده‌ها را تولید، ثبت و ذخیره‌سازی می‌کند. بر همین اساس نقش مدیریت منابع برنامه‌ریزی سازمانی و به ویژه مؤثرترین آنها که مدیریت بانک‌های اطلاعاتی است در تقویت و موفقیت هر سازمانی بسیار مؤثر است. برنامه‌ریزی منابع سازمان به عنوان یک سیستم اطلاعاتی و عملیاتی در تمامی زوایای اهداف اطلاعاتی مجموعه سازمان یکی از مهمترین سیستم‌های اطلاعاتی محسوب می‌شود و سازمان بازرسی به عنوان یک

سازمان بزرگ و پیچیده باید بـه سـمت ایجـاد و پیـاده‌سـازی سیسـتم‌هـای اطلاعاتی حرکت نماید. چنانچه در هر سازمانی به ویژه سازمان بازرسی که حوزه‌ای حاکمیتی در زمینه نظارت و بازرسی اسـت، داده‌هـا و اطلاعـات بـه هنگام و با دقت بالایی ثبت، طبقه‌بندی، پردازش و به موقع به دسـت مـدیران نرسد، نمی‌توان انتظار داشت که بخش مهمـی از سـازمان در نظـام تصـمیم-گیری و برنامه‌ریزی با دقـت و آگـاهی عمـل نمایـد. بنـابراین ضـرورت ایـن موضوع در سازمان بازرسی به طور کامل آشکار اسـت (حسـینی و فـولادی طرقی، ۱۳۸۹: ٦٨٣).

**موانع و الزامات نظارت الکترونیک در سازمان بازرسی**

با مطالعه در حوزه فناوری اطلاعات و اقدامات انجـام شـده در خصـوص طرح نظارت الکترونیک در سازمان بازرسـی کـل کشـور، پـنج متغیـر بـرای شناسایی محدودیت‌های پیاده‌سـازی برنامـه‌ریـزی منـابع سـازمان در نظـر گرفته می‌شود:

- محدودیت‌های فنی
- محدودیت‌های آموزشی
- محدودیت‌های سیستمی
- محدودیت‌های قانونی و اجرایی
- محدودیت‌های فرهنگی.

**آسیب شناسی موانع نظارت و بازرسی**

موانع موجـود در مسـیر نظـارت و بازرسـی کـارآیی و اثربخشـی آن در سازمان‌ها بسیار زیاد است که در ادامه این بخش از کتاب به بررسی تعدادی از این موانع خواهیم پرداخت. در این بخش موانع بازرسی را در قالـب موانـع اجرایی، ساختاری و فرهنگی تشریح خواهند شد.

**موانع اجرایی نظارت و بازرسی:**

از مهمترین موانع اجرایی نظارت و بازرسی، ناکارآمدی مکانیسم‌های سنتی نظارت و عدم توجه به سیستم‌های جدید نظارتی است. سیستم‌های کنونی نظارت و بازرسی در کشور، متناسب با نیازهای جدید پیشرفت نکرده است و این سیستم با اجرای روش‌های سنّتی و قدیمی، توان پاسخگویی به این نیازها را ندارد. آنچه ضروری به نظر می‌رسد این است که از سیستم‌های جدید که کشورهای پیشرفته برای نظارت و بازرسی استفاده می نمایند بهره-گیری نماید همان‌طور که ریاست قوه قضائیه بیان نمودند که: «ما در نظام خود عملاً دارای دستگاه‌های نظارتی مختلفی هستیم، اما با وجود تعداد زیاد دستگاه‌های نظارتی و تلاش‌های فراوان نهادها، به نتیجه نظارت‌ها که نگاه می کنیم متوجه می‌شویم، محصول به اندازه این تلاش‌ها نیست. در صورتی که کشورهای دیگر با تشکیلات نظارت و بازرسی کمتر، نتیجه بیشتری می‌گیرند و دستگاه‌های اجرایی‌شان سلامت بیشتری دارد». یکی دیگر از موانع اجرایی نظارت و بازرسی، نبود معیارهای شفاف و مشخص برای سنجش و نظارت سازمان‌ها خصوصاً بخش خدمات دولتی می‌باشد. در طراحی سازمان‌ها بر اساس نظریه سیستمی اولین و مهمترین امر شناخت اهداف و قابل سنجش نمودن آن است. زیرا سیستم بایستی بتواند به صورت خودکار یا به طرق دیگر خروجی‌ها را کمی نموده و آنرا با هدف مقایسه نماید و مغایرت را برطرف کند. این امر در سیستم‌های اداری و اجتماعی و حتی صنعتی بسیار پیچیده است. در این روش در شروع کار مشکلاتی مانند تعریف هدف، کمی کردن اهداف و خروجی‌ها، مقایسه آنها، اصلاح مغایرت‌ها، زمان انجام این عملکرد و به‌روز نگه داشتن سیستم وجود دارد که با گذر از این مرحله بسیاری از مشکلات دیگر را نخواهیم داشت. با هدف‌گذاری صحیح و اخذ خروجی صحیح از سیستم و در همه زیر سیستم‌ها، در حقیقت سازمانه‌های نظارت و بازرسی واحدهای کنترل‌گری را در تمام نقاط سازمان نصب

نموده، بدون این‌که نیاز به حضور فیزیکی داشته باشند. با این نحوه عملکرد از آنجایی‌که آسیب‌شناسی نظارت و بازرسی در سازمان‌ها موانع موجود بر راه نظارت و بازرسی کارآ و اثر بخش در سازمان‌ها بسیار زیاد است. یکی دیگر از موانع اجرایی نظارت و بازرسی، ناکار آمدی مکانیسم‌های سنتی نظارت و عدم توجه به سیستم‌های جدید نظارتی می‌باشد. سیستم‌های کنونی نظارت و بازرسی در کشور متناسب با نیازهای جدید پیشرفت نکرده است و لذا توان پاسخگویی به این نیازها را ندارد. آنچه ضروری به نظر می‌رسد این است که از سیستم‌های جدید که کشورهای پیشرفته برای نظارت و بازرسی استفاده می‌نمایند بهره‌گیری نماید همان‌طور که ریاست سابق قوه قضائیه بیان نمودند: «ما در نظام خود عملاً دارای دستگاه‌های نظارتی مختلفی هستیم، اما با وجود تعداد زیاد دستگاه‌های نظارتی و تلاش‌های فراوان نهادها، به نتیجه نظارت‌ها که نگاه می‌کنیم متوجه می‌شویم، محصول به اندازه این تلاش‌ها نیست. در صورتی که کشورهای دیگر با تشکیلات نظارتی کمتر نتیجه بیشتری می‌گیرند و دستگاه‌های اجرایی‌شان سلامت بیشتری دارد».[۱]

عدم شفافیت در سنجش و نظارت سازمان‌ها:

در طراحی سازمان‌ها بر اساس نظریه سیستمی اولین و مهمترین امر شناخت اهداف و قابل سنجش نمودن آن است. زیرا سیستم بایستی بتواند به‌صورت خودکار یا به طرق دیگر خروجی‌ها را کمی نموده و آن را با هدف مقایسه نماید و مغایرت را برطرف کند. این امر در سیستم‌های اداری و اجتماعی و حتی صنعتی بسیار پیچیده است. در بسیاری از سازمان‌های کشور، فعالیت‌ها دارای شفافیت لازم نیست و به گونه ای عمل می‌شود که ناظران بیرونی و نهادهای نظارتی از ماهیت وظایف و چگونگی انجام آنها بی-

[۱] سخنرانی آیت الله سید محمود هاشمی شاهرودی رئیس قوه قضائیه در مراسم افتتاح مرکز ارتباطات مردمی سازمان بازرسی کل کشور، ۱۳۸٤/٦/۲۷.

اطلاع هستند. همین امر سبب می‌شود تا نتوان در مورد عملکرد این سازمان-ها قضاوت صحیحی داشت، زیرا مبنای قضاوت صحیح، وجود اطلاعات شفاف در مورد ماهیت، هدف، چگونگی انجام وظایف و نحوه ارزیابی نتایج حاصل از عملکرد می‌باشد. پس بنابر این بایستی، روند انجام فعالیت‌های سازمان‌های مختلف کشور به روشنی مشخص گردد تا امر نظارت و بازرسی تسهیل شود. نبود معیارهای شفاف و مشخص برای سنجش و نظارت سازمان‌ها و بخش خدمات دولتی یکی از چالش‌های امر نظارت و بازرسی است.

بالا بودن هزینه‌های نظارتی و عدم توجه به تحلیل هزینه فایده:

سیستم‌های بازرسی و نظارتی غالباً هزینه‌بر هستند. اما وجود این سیستم‌ها بسیار ضروری می‌باشد چرا که هر سیستمی بدون وجود سیستم-های نظارتی روبه فساد رفته و منجر به بی‌نظمی درون خود می‌شود و در نهایت به اضمحلال کشیده خواهد شد. اما این سیستم‌های نظارتی تا چه حد در برابر هزینه‌هایی که به جامعه تحمیل می‌نمایند به جامعه سود می‌رسانند؟ برخی از بازرسی‌هایی که در سازمان‌ها انجام می‌شود صرفاً در مورد مسائل کم اهمیت بوده و بایستی نسبت به ماهیت آنها تجدید نظر نمود. زیرا علاوه بر تحمیل هزینه بر جامعه و سازمان موجب می شود تا سیستم‌های نظارتی از بررسی مسائل اساسی که جنبه راهبردی دارند و تاثیر بسیار مهمتری بر عملکرد سازمان‌ها دارند باز بمانند.

عدم تفویض اختیارات لازم به بازرسان:

در صورتی که سازمان‌های نظارتی از اختیارات لازم در خصوص ارزیابی و بازرسی سازمان‌ها و افراد برخوردار نباشند، مدیران و کارکنان سازمان‌ها همکاری لازم را با این نهادهای نظارتی نخواهند داشت. البته در قوانین اختیارات زیادی به سازمان‌های نظارتی تفویض شده است، اما باید توجه داشت که این اختیارات، صرفاً توسط بازرسان و مدیران نظارتی توانا

می‌تواند به درستی مورد استفاده قرار گرفته و موجبات همکاری سازمان‌ها را در امر نظارت فراهم آورد.

عدم وجود ضمانت‌های اجرایی:

ضمانت اجرایی، عکس العمل عدم رعایت قانون می‌باشد که به زیان متخلف از سوی قانون‌گذار وضع شده است و اساساً الزام‌آور بودن هر قاعده حقوقی مستلزم مقرون بودن آن به ضمانت اجرای مادی است. ضمانت اجرا که برخی حقوقدانان از واژه جزا برای آن استفاده می نمایند، جوهر قانون است و اگر مواد قانون با ضمانت اجرا همراه نباشد، غالباً موجب یا انگیزه‌ای برای تبعیت از آن وجود نخواهد داشت و قانون به حد پند و اندرز تنزل خواهد یافت. اگرچه ماهیت قانون نیز باید به گونه‌ای باشد که پیشاپیش از موارد نقض آن بکاهد. فقدان ضمانت اجرایی برای گزارش‌های سازمان بازرسی کل کشور همواره به عنوان یکی از نکات مورد نقد در قانون تشکیل این سازمان مورد توجه بوده است. با عنایت به مفاد ماده ۱۰ قانون تشکیل سازمان بازرسی کل کشور و مواد ۲ و ٤٠ آئین بازرسی، بخش پایانی گزارش‌های تنظیمی توسط هیئت‌های بازرسی مشتمل بر پیشنهادهایی است که شرایط آن نیز در ماده ٤٢ آیین بازرسی ذکر گردیده و گزارش‌های این دستگاه عالیه نظارتی بدون فصل نظریه و پیشنهاد به هیچ مرجعی ارسال نمی‌گردد. بر همین اساس، منظور از ضمانت اجرا در قانون تشکیل سازمان بازرسی کل کشور، ضمانت اجرای پیشنهادهای راهبردی در گزارش‌های تنظیمی توسط این سازمان می‌باشد. لذا جهت تبیین بهتر موضوع باید گفت که پیشنهادهای مندرج در گزارش‌های بازرسی شامل دو قسم است: اول پیشنهادهای قضائی که شامل تعقیب کیفری، تعقیب اداری یا انضباطی، ابطال مصوبات و بخشنامه‌ها می‌باشد. دوم پیشنهادهای اجرایی که شامل اصلاح ساختار، سیاست‌گذاری، تشویق، تغییر سمت و... می‌باشد. در خصوص پیشنهادهای قضائی که عموماً ناظر بر تخلفات و جرایم می باشد، نظارت

سازمان بازرسی کل کشور در واقع نظارت استطلاعی محسوب می‌شود و ضمانت اجرایی خاصی در قانون برای اینگونه پیشنهادها پیش بینی نشده است. به‌جز آن‌که بر اساس مواد ۲ و ۹ قانون تشکیل سازمان بازرسی کل کشور، مراجع قضائی، هیئت‌های رسیدگی به تخلفات اداری و دیوان عدالت اداری بایستی به گزارش‌های این سازمان خارج از نوبت رسیدگی نمایند. در مورد پیشنهادهای اجرایی نیز بر اساس ماده ۱۰ قانون تشکیل سازمان بازرسی کل کشور، وزیر یا مسئول دستگاه مربوط، موظف است از تاریخ دریافت گزارش هیئت بازرسی، حداکثر ظرف مدت ده روز، عملیات اجرایی را جهت انجام پیشنهادهای مندرج در گزارش مزبور شروع و مفاد جریان کار را مرتباً به اطلاع سازمان برساند. اما در قانون تشکیل سازمان بازرسی کل کشور برای این تکلیف قانونی ضمانت اجرایی مشخص نگردیده است (مخلص الائمه، ۱۳۸۷: ۵۸).

یکی از دلایل عدم همکاری لازم توسط مدیران و کارکنان سازمان‌های مختلف با سازمان نظارت و بازرسی کل کشور را نیز می‌توان در همین نبود ضمانت‌های اجرایی لازم برای امر نظارت و بازرسی دانست. همان‌طور که بیان شد، براساس قانون فعلی ضمانت‌های اجرایی پیش بینی شده عبارتند از تعقیب جزایی، تعلیق از خدمت و انجام پیشنهادهای سازمان در رفع نواقص، اما زمانی که سازمان بازرسی کل کشور از مدیران می‌خواهد تا اسناد و مدارکی را در اختیار بگذارند و یا مدیری تعلیق بشود به دلیل ناکارایی ضمانت اجرایی، دستگاه‌ها از انجام این دستورات استنکاف می‌کنند. در صورتی که باید در قوانین جدید ضمانت‌های اجرایی بهتری پیش‌بینی شود و با افراد و سازمان‌هایی که همکاری لازم را نمی‌نمایند یا سعی در وارونه جلوه دادن عملکرد ضعیف خود دارند، برخورد قانونی متناسب صورت گیرد تا مشکل عدم همکاری با سازمان نظارت و بازرسی حل شده و بازرسی‌ها از اثربخشی بیشتری برخوردار شوند.

بروکراسی در سازمان‌های نظارتی:

یکی از مشکلات ساختارهای نظارتی در کشور بروکراسی شدیدی است که در این سازمان‌ها حاکم است و معایب بروکراسی در کاهش اثربخشی سیستم نظارت و بازرسی نیز بر کسی پوشیده نیست. در بروکراسی، قوانین که برای رسیدن به هدف به‌وجود آمده‌اند پس از مدتی خود هدف می‌شوند. از سوی دیگر بروکراسی دارای خشکی و انعطاف ناپذیری ذاتی است و با ساختاری خشک خود میل به جاودانگی و توسعه دارد که سازمان‌های بسیار بزرگ با بازدهی اندک ایجاد می‌نماید و از همه بدتر این‌که طبق نظر «وایت»، بروکراسی آن قدر وسیع می‌گردد که به ارباب رجوع پس از مراجعه به سازمان حالت ترس دست می‌دهد. این معایب برای همه سازمان‌ها مشکل‌ساز و برای سازمان نظارت و بازرسی مشکل‌سازتر هستند زیرا این سازمان ناظر بر حسن اجرای امور است و در صورت هرگونه تعلل در کار این سازمان و هر عاملی که موجب عدم کارایی این سازمان گردد، نتایج زیان-بارتری را در پی خواهد داشت. بر این اساس روش‌های متداول این سازمان بایستی مورد بازنگری قرار گرفته و دوباره‌کاری‌ها و فعالیت‌های زاید از فرآیند کار حذف شود، همچنین بایستی بررسی‌های تطبیقی در مورد سازمان‌های نظارتی سایر کشورها نیز صورت گیرد تا روش‌های جدید با بروکراسی کمتر جایگزین روش‌های فعلی شوند و سازمان بتواند با سرعت عمل و کارایی بیشتری وظایف خود را به انجام رساند.

فرآیند اجرای طرح نظارت الکترونیک

با توجه به روند رو به رشد روش‌های زندگی و تقویت روز افزون نظام تفکر و تولید اندیشه‌های جدید در جوامع انسانی، رسیدن به راه‌های اصلی اطلاعاتی، امری بدیهی به نظر می‌رسید که با ظهور صنعت اطلاعات و راه-اندازی شبکه جهانی اینترنت، فاصله تفکرات انسانی بیش از گذشته کوتاه شد، حال آن‌که لزوم استفاده از صنایع مدرن در بسیاری از نقاط جهان، به

درستی شناخته نشده است. موج سوم، کتاب معروف الوین تافلر، تمدن بشر را از سه موج پیاپی تاثیر گرفته می‌داند که با هر موج، تاریخ تمدن وارد فصل جدیدی از مراحل سیستماتیک خود می‌شود (Arvin, ۱۹۸۰). همچنین با آغاز هزاره سوم میلادی، مقوله دانش و اطلاعات وارد ابعاد تازه‌ای از مباحث بشری گشته که در اکثر نشست‌های علمی جهان، سخن از گذار جوامع انسانی به جوامع تکنولوژیک اطلاعاتی و پردازش داده‌های انفورماتیکی به میان آمده است. همچنین فرآیند اجرای طرح نظارت و بازرسی الکترونیک شامل مراحل ذیل می‌باشد:

۱- آموزش و تسلط کارشناسان و بازرسان سازمان بازرسی به علوم کامپیوتر و فناوری اطلاعات.

۲- برگزاری میزگردها، نشست‌ها، همایش‌ها و سمینارهای درون سازمانی جهت بررسی و معرفی طرح نظارت و بازرسی الکترونیکی.

۳- اطلاع‌رسانی درون سازمانی و فرهنگ سازی و بسترسازی، به منظور توجیه و آموزش کلیه مدیران و همکاران سازمان بازرسی.

٤- تبیین راهکارهای قانونی، اداری یا علمی و ضرورت آموزش تمامی مدیران دستگاه‌های اجرایی کشور نسبت به استفاده از ابزاری رایانه‌ای و فناوری اطلاعات.

٥- تجهیز بخش‌های اداری و عملیاتی سازمان بازرسی به ابزار پیشرفته رایانه‌ای و بسترسازی ارتباطات شبکه‌ای و راه اندازی سیستم نظارت و بازرسی الکترونیک در سازمان بازرسی.

٦- آموزش تکیملی کارشناسان سازمان بازرسی در بخش ستاد خبری و برقراری ارتباط شبکه‌ای آن با بخش‌های مدیریتی مرتبط.

۷- برگزاری سمینارها و میزگردهای مشترک سازمان بازرسی با هر یک از دستگاه‌های اجرایی در خصوص اجرایی شدن طرح نظارت و بازرسی الکترونیک.

۸- برگزاری میزگردهای علمی و سمینارهای برون سازمانی در خصوص موضوعات ذیل، در راستای تحقق طرح:

۸-۱- جایگاه نظارت و بازرسی در تجارت الکترونیک

۸-۲- جایگاه نظارت و بازرسی در تجارت جهانی

۸-۳- چگونگی نظارت و بازرسی در مدیریت مجازی و الکترونیک

۸-٤- دولت الکترونیک و نقش و جایگاه نظارت و بازرسی در آن (احمدی گرجی، ١٣٨٦).

آنچه که پس از انقلاب صنعتی حادث شد، بهبود شرایط مادی زندگی بشر را به همراه داشت، لکن در عصر حاضر که نوع نگاه جامعه، انقلابی دیگر را در جستجوی پردازش داده‌ها و کسب دانش برای کمک به ارتقای سطح معنوی زندگی دنبال می‌کند، حادثه جدید را در ابعاد فراصنعتی ایجاد خواهد نمود. بنابراین لزوم تغییرات سریع و همه جانبه در سازمان‌ها، جوامع و به تبع آن در امور نظارت بر اجراییات، بیش از پیش جلوه‌گر شده و مورد توجه صاحب‌نظران قرار گرفته است. لذا در این بخش از کتاب، ابتدا به عوامل اهمیت و ضرورت اطلاعات در عصر حاضر و نقش آن در تصمیم‌گیری و توسعه اشاره خواهد شد و سپس نظام اطلاع‌رسانی در کشور ایران تحت بررسی قرار خواهد گرفت. آن‌گاه نقش اطلاعات در نظارت و بازرسی بر زیرگروه‌های اجرایی تحلیل شده و عملکرد سیستم‌های اطلاع‌رسانی در چند کشور مورد بررسی قرار خواهد گرفت و در پایان، پیشنهادهایی برای ایجاد یک نظام توانمند نظارت الکترونیک، بازرسی و اطلاع‌رسانی ارائه می‌گردد.

**الزامات و راهکارهای نظارت الکترونیک**

در این بخش از کتاب، پیشنهادهای کاربردی، الزامات و راهکارهای نظارت الکترونیک در سازمان بازرسی کل کشور با توجه به الزامات مورد نیاز و مطروحه در بخش‌های قبلی کتاب ارائه شده است:

راهکارهای قانونی نظارت الکترونیک:

با توجه به این‌که تدوین و طراحی سند برنامه‌ریزی منابع سازمان از جمله اسناد بالادستی یک سازمان محسوب می‌گردد، لازم است تحقق این مهم در مرحله اول به عنوان یکی از اهداف سازمان بازرسی کل کشور تعریف و اهتمام و جدیت لازم در انجام آن مد نظر قرار گیرد. با توجه به این‌که فناوری‌های مدیریت اطلاعاتی نظیر سیستم برنامه‌ریزی منابع سازمان در کشور و به طبع آن در سازمان‌های دولتی نوپا است و یکی از مهمترین آسیب‌های فناوری اطلاعات در سطح دستگاه‌های دولتی، عدم شفافیت و بلوغ سیاست‌گذاری‌های قانونی و حقوقی می‌باشد و از طرفی شخصیت تربیت شده کارشناسان سازمان (ناشی از نوع مأموریت) استنادپذیری قانونی و مقرراتی است، اهمیت اطلاع‌رسانی و شفاف‌سازی قوانین و مقررات موجود کشور در زمینه مدیریت اطلاعات، تأثیر بسیار بالایی در افزایش سطح پذیرش و آستانه تحمل سازمانی داشته و لازم است کمیته حقوقی پروژه برنامه‌ریزی منابع سازمان با هدف جمع‌آوری قوانین، مقررات، مصوبات، دستورالعمل‌ها، نامه‌ها، آیین نامه‌ها و... تشکیل و نسبت به اجرایی شدن برنامه‌ریزی انجام در لایه افکار سازمانی اقدام نماید. لازم به ذکر است اطلاع‌رسانی قانونی باید به موقع و متناسب با فازهای پیشرفت پروژه انجام گردد تا تأثیرگذاری لازم محقق شود.

راهکارهای فنی نظارت الکترونیک:

یکی از آسیب‌های تأثیرگذار در مسیر تحقق سیستم نظارت و بازرسی الکترونیک در سازمان بازرسی کل کشور، نگرانی از مخاطرات امنیتی می‌باشد. متأسفانه ضعف شناختی لایه‌های کاربری سازمان از استانداردهای امنیت اطلاعات در فضای فیزیکی و دیجیتال و بحران‌های فکری و مدیریتی ناشی از عدم شناخت موضوع مورد اشاره، تأثیر زیادی در تصمیم‌گیری‌های این سازمان داشته و ضروری است مجموعه حفاظت اطلاعات سازمان، با

بهره‌گیری از متخصصین مجرب نسبت به افزایش سطح امنیت انتقال اطلاعات در فضای مجازی و تأمین امنیت داده‌ها در سیستم نظارت الکترونیک و همچنین ارتقای سیستم اطلاع‌رسانی و فرهنگ‌سازی و رعایت نکات و مسائل امنیتی و سازمانی اقدام نماید.

راهکارهای آموزشی نظارت الکترونیک:

نظام آموزشی سازمان بازرسی کل کشور همانند بسیاری از سازمان‌های دولتی، اهداف آماری و افزایش سطح رفاهی کارکنان را بیش از تولید منابع فکری مورد نیاز سازمان دنبال می‌کند. لذا لازم است آموزش‌های سازمان در دو سطح فنی و غیر فنی برنامه‌ریزی و اجرا گردد. در سطح فنی چگونگی و در سطح غیر فنی چرایی استفاده از یک فناوری آموزشی و اطلاع‌رسانی مطرح می‌گردد. با توجه به وجود پتانسیل‌های بالای فکری در سازمان بازرسی کل کشور، ارائه استانداردهای کاربردی و نه نظری در فعالیت آموزشی، می‌تواند تأثیر شگرفی در تحرک‌پذیری لایه‌های مختلف سازمان داشته باشد. با توجه به ماهیت ریسک‌پذیری پروژه‌های برنامه‌ریزی منابع سازمان و لزوم افزایش شجاعت مدیران و کاهش استرس‌های طبیعی ناشی از تفکرهای نوین، لازم است آموزش استانداردهای مدیریت ریسک، مدیریت ارزش، مدیریت استرس، مدیریت تضاد، مدیریت تعارض‌های سازمان و مدیریت استراتژیک و نظارت الکترونیک در سطح مدیران برنامه‌ریزی و عملیاتی گردد.

راهکارهای فرهنگی نظارت الکترونیک:

با توجه به اینکه افکار کارشناسی سازمان به دلیل تنوع مأموریت‌های محوله، تمرکز بر موضوع خاص را نمی‌پذیرد، لازم است کمیته‌ای به موازات تشکیلات اجرایی طرح نظارت الکترونیک سازمان، در جهت اطلاع‌رسانی مستمر و شفاف‌سازی گام به گام مراحل عملیات، با رویکرد فرهنگ‌سازی و

آموزش نظارت و بازرسی الکترونیک و همراهی لایه‌های مختلف سازمانی تشکیل گردد.

راهکارهای سیستمی نظارت الکترونیک:

با توجه به طیف گسترده‌ای از تخصص‌های کارشناسی فعال در سازمان بازرسی کل کشور، ضروری است نظام پیشنهادهای سازمان با هدف جمع-آوری نقطه نظرات، تجارب و ایده‌های جدید در افکار کارشناسان و بازرسان مجربی که در سازمان رشد کرده‌اند، در خصوص بهره‌برداری در سیستم نظارت الکترونیک راه اندازی شود.

سایر پیشنهادهای کاربردی:

موضوعات و مسائلی که در بخش قبلی به آن اشاره شد، بیانگر نقش بسزای اطلاعات در تصمیم‌گیری‌های مدیریت، اهمیت شایان توجه آن در پیشرفت جوامع در حال توسعه و از میان برداشتن فاصله موجود بین این کشورها با جوامع بسیار پیشرفته است. بررسی و طرح مسائل مبتلا به نظام ملی اطلاع‌رسانی در کشور از دیدگاه صاحبنظران و کارشناسان امر که حاصل سال‌ها تجربه، مطالعه و مواجهه آنان با این موضوع می‌باشد و همچنین تلاش همه جانبه سایر کشورها در این زمینه، همگی بر لزوم یک نظام اطلاع‌رسانی کارآمد برای استفاده هرچه بیشتر از منابع و امکانات محدود تاکید دارد. بدیهی است که فقدان چنین نظامی موجب ناکارآمدی برنامه‌ریزی توسعه ملی خواهد بود، لذا توجه به مطالب فوق‌الذکر، نکات و پیشنهادهای زیر قبل از هرگونه بازنگری و تصمیم‌گیری در این زمینه مفید و لازم به نظر می‌رسد.

۱- تلاش و توجه جدی سیاست‌گذاران و دست‌اندرکاران به منظور تدوین یک خط مشی ملی در فناوری اطلاعات به منظور ایجاد نظام ملی اطلاع‌رسانی که می‌تواند سهم بسزایی در توسعه همه جانبه بخش‌های مختلف جامعه داشته باشد (مرغلانی، ۱۳۷۶: ۳۱).

۲- دستگاه مسئول اطلاع‌رسانی و فناوری اطلاعات در کشور به دلیل اثر فرابخشی آن باید زیرنظر بالاترین مرجع تصمیم‌گیری اجرایی کشور باشد که این خود، حاکی از اهمیت به کارگیری اطلاعات در کشور خواهد بود (میقانی، ۱۳۷۷: ۱۲۳).

۳- ایجاد تشکیلات و سازمان اجرایی مناسب، با نقش هماهنگ‌کنندگی در سطح ملی و با وظایف و اختیارات لازم، امکانات و نیروی متخصص مورد نیاز و توجه به جایگاه مناسب شغلی کارکنان آن، تا هماهنگی لازم در زمینه مدیریت و سازماندهی فعالیت‌های مرتبط با اطلاعات را تحقق بخشد.

٤-وضع قوانین و مقررات و مکانیسم‌های لازم که براساس آن وزارتخانه‌ها، سازمان‌ها و دستگاه‌های مختلف (به ویژه دولتی) مکلف به همکاری مستمر و نزدیک با نهاد مسئول اطلاع‌رسانی در کشور شوند و به کارگیری روش‌هایی که به تقویت این همکاری کمک نماید.

٥- اعمال مدیریت داده‌ها به طور اصولی و دقیق در جهت تعیین نیاز کاربران اطلاعات و هدایت تولیدات اطلاعاتی به سوی کاربردی شدن هر چه بیشتر آنها.

٦- ایجاد و توسعه شبکه‌های داخلی اطلاع‌رسانی و مجموعه‌های اطلاعاتی در مؤسسات دولتی و غیردولتی و همکاری با پایگاه‌ها و شبکه‌های جهانی اطلاع‌رسانی.

۷- فراهم نمودن بستر فرهنگی به منظور برقراری فضای مبتنی بر اعتماد در عموم، از طریق رعایت رازداری، تعهد در اطلاع‌رسانی عمومی در حد معیّن و بی‌طرفی و استقلال در نظام اطلاع‌رسانی.

۸- استفاده از روش‌های روزآمد داده‌پردازی اطلاعات در امور نظارت بر عملیات‌های اجرایی واحدهای مختلف اجرایی در کشور.

۹- استفاده از نتایج حاصله از فناوری نظارت در امور تصمیم‌گیری و مدیریت سیستم‌ها.

۱۰- ایجاد یک سیستم یکپارچه برای کنترل امور اجرایی، که راهگشای پاسخگویی مسئولین کشور به مردم عزیز باشد.

همچنین پیشنهادهای ذیل می‌تواند راهبردهایی سودمند برای تحقق طرح نظارت و بازرسی الکترونیک در سازمان بازرسی کل کشور باشد:

۱- بررسی و مشخص نمودن میزان شکاف دیجیتالی بین لایه‌های مختلف سازمان و اهداف مورد نظر در پروژه.

۲- بررسی و تشخیص دقیق آمادگی الکترونیکی سازمان بازرسی کل کشور.

۳- بررسی راهکارهای استفاده از امضاء الکترونیکی در سازمان و تخصیص هویت الکترونیکی به کارشناسان.

٤- بررسی میدانی عوامل روحی تأثیرگذار در تحقق برنامه‌ریزی منابع سازمان با توجه به تنوع تخصص در سازمان بازرسی کل کشور.

محدودیت‌های قانونی و آموزشی، مهمترین محدودیت‌های اجرای طرح نظارت الکترونیک هستند و مدیران، بازرسان و کارکنان از آگاهی فرهنگی و شناخت لازم از به‌کارگیری سیستم مذکور برخوردار می‌باشند که از جمله نقاط قوت به‌کارگیری این ابزار نظارتی است. همچنین، محدودیت‌های فنی، ضعف در سیستم آموزشی، نگرش سیستمی، فضای قانونی و فرهنگی از اهمیت یکسانی در سازمان بازرسی کل کشور برخوردار نیستند و محدودیت‌های قانونی، آموزشی، سیستمی، فنی و فرهنگی به عنوان عوامل و موانع تحقق نظام بازرسی و نظارت الکترونیک هستند.

از آنجایی که نظارت و بازرسی نقش عمده‌ای در تغییر ساختار و اصلاح یک حکومت بازی می‌کند، تدوین قوانینی که قابلیت برطرف کردن نیازها در بُعد ملی را داشته باشد موجب استحکام و تثبیت موقعیت بین‌المللی کشور

خواهد شد. انتقادات زیادی که از ساختار اقتصادی، اجتماعی و خط مشی‌های سیاسی اتخاذ شده در مورد کارآیی مؤسسات دولتی در رسانه‌های گروهی انجام می‌شود نشانگر آن است که مشکلات حل نشده زیادی وجود دارد که غیر مستقیم روی امر نظارت و بازرسی تأثیر می‌گذارد و از کارآمدی آن می‌کاهد. اصولاً بازرسی به دو منظور در نهادهای جمهوری اسلامی ایران پیش‌بینی شده است که عبارتند از حسن جریان امور و اجرای صحیح قوانین در دستگاه‌های اداری. وظیفه مهمتر بازرسی در مواقعی است که نقض قانون به‌طور آشکار و یا غیر آشکار صورت گرفته است اما یا شاکی وجود ندارد و یا شرایط طرح شکایت برای شاکی مساعد نیست. در واقع بازرسی نیازهای جامعه را درک می‌کند و این نیازها را با دستگاه‌های اداری و اجرایی تطبیق می‌دهد و در صورت لزوم موارد عدم تطابق را پیگیری می‌نماید. بنابراین ضروری است که مشخص شود چگونه می‌توان پوشش، کیفیت و تاثیر نظارت و بازرسی را افزایش داد. نکته مهم برای موفقیت کار بازرسی توجه به اخلاقیات در جامعه است و این موضوعی نیست که بتوان برای آن به‌طور مرتب قانون و مقررات تهیه کرد و رفتار روزانه افراد را تحت نظر داشت. در واقع براساس تجربیات به‌دست آمده در سایر کشورها، نظارت بیش از حد و افزایش حجم قوانین موجب بروز رفتارهای نامناسب انسانی و یا محافظه‌کاری توأم با کم‌کاری شدید خواهد شد. بنابراین، اصول کار بایستی افزایش اعتماد عمومی و جلب مشارکت مردم در امور با دادن امنیت کافی به آنان برای ابراز نظریاتشان در جهت اصلاحات باشد. یک عامل بسیار مهم و در عین حال ظریف، کاهش فاصله گفتار و رفتار به وسیله رهبران سیاسی و در اختیار عامه قرار دادن نتایج کلی بازرسی برای رفع شبهات است.

## ارجاعات و منابع

- احمدی گرجی، حسینعلی (١٣٨٦). طرح نظارت الکترونیک (دیجیتالی یا مجازی).
- باستانی، برومند (١٣٨٣). جرایم کامپیوتری و اینترنتی. تهران: انتشارات بهنامی.
- باقری، آیت (١٣٨٧). لزوم تغییر ساختار اداری به منظور مبارزه با فساد اداری، تهران.
- بختیاروند، مصطفی (١٣٨٦). ماهیت و جایگاه مرکز گواهی ریشه در تراکنش‌های الکترونیکی، مجلس و پژوهش، سال ١٤، شماره ٥٥.
- پرنیان، حمیدرضا (١٣٨٣). ارتباطات و فناوری اطلاعات و نقش آن در نظارت کارآمد، مجموعه مقالات سومین همایش نظارت کارآمد.
- جلالی فراهانی، امیر حسین (١٣٨٩). کنوانسیون جرایم سایبر و پروتکل الحاقی آن، چاپ اول.
- حسینی، میرزاحسن و فولادی طرقی، مهدی (١٣٨٩). بررسی موانع و محدودیت‌های اجرای نظارت الکترونیکی، فصل‌نامه مطالعات مدیریت انتظامی، سال پنجم، شماره چهارم.
- خداقلی، زهرا (١٣٨٣). جرایم کامپیوتری، تهران: انتشارات آریان.
- خدمتی، ابوطالب، نظارت و بازرسی در اسلام، مجله معرفت، شماره ٢٧.
- خرم آبادی، عبدالصمد (١٣٨٤). جرایم فناوری اطلاعات، پایان نامه مقطع دکتری، دانشگاه حقوق و علوم سیاسی دانشگاه تهران.
- دادگر، داود (١٣٨٠). مبانی بازرسی و تهیه گزارش‌های ویژه نظارتی، دومین همایش علمی و پژوهشی نظارت و بازرسی.
- شیرزاد، کامران (١٣٨٨). 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.
- عبداللّهی، جواد (۱۳۸۳). موانع و محدودیت‌های اعمال نظارت کارآمد، مجموعه مقالات سومین همایش نظارت کارآمد.
- مخلص الائمه، فرزاد (۱۳۸۷). نقد قانون تشکیل سازمان نظارت و بازرسی کل کشور.
- مرغلانی، محمد (۱۳۷٦). عوامل موثر بر انتقال فناوری اطلاعات در کشورهای در حال توسعه، ترجمه: عباس گیلوری، نشریه اطلاع‌رسانی دوره۱۳، شماره ۱۲.
- میقانی، بهزاد (۱۳۷۷). نظام انفورماتیک کشور، نشریه انفورماتیک، شماره ۷۰.
- ولیدی، محمد صالح (۱۳۸۲). بایسته‌های حقوق جزای عمومی، تهران: انتشارات خورشید، چاپ اول.

- Robbins, Stephen p, Organization theory ,۱۰th ed, prentice hall Publication,۲۰۰۳, p. ٤٦٥.