بسمه تعالی

فرم شناسنامه خدمت دستگاه اجرایی کد۱۳۵ ضمیمه ۱

۱- عنوان خدمت:ارائه آموزش های عمومی در حوزه سلامت اجتماعی(فضای مجازی)	۲- شناسه خدمت (این فیلد توسط سازمان مدیریت و برنامه ریزی کشور تکمیل می شود.)

۳- ارائه دهنده خدمت

نام دستگاه اجرایی: سازمان بهزیستی کشور /دفتر پیشگیری از آسیب های اجتماعی مرکز توسعه و درمان اعتیاد

نام دستگاه مادر: **وزارت تعاون، کار و رفاه اجتماعی**

۴- مشخصات خدمت

شرح خدمت	تدوین سیاتگذاری-تهیه دستور العمل ها- تهیه بسته آموزشی	
نوع خدمت	■ خدمت به شهروندان (G۲C) ☐ خدمت به کسب و کار (G۲B) ☐ خدمت به دیگردستگاه های دولتی(G۲G)	نوع مخاطبین
ماهیت خدمت	■ حاکمیتی ☐ تصدی گری	
سطح خدمت	■ ملی ☐ منطقه ای ☐ استانی ☐ شهری ☐ روستایی	
رویداد مرتبط با:	☐ تولد ■ آموزش ■ سلامت ☐ مالیات ☐ کسب و کار ☐ تامین اجتماعی ☐ ثبت مالکیت ☐ تاسیسات شهری ☐ بیمه ☐ ازدواج ☐ بازنشستگی ☐ مدارک و گواهینامه‌ها ☐ وفات ☐ سایر	
نحوه آغاز خدمت	☐ تقاضای گیرنده خدمت ☐ فرارسیدن زمانی مشخص ☐ رخداد رویدادی مشخص ☐ تشخیص دستگاه ☐ سایر: ...	
مدارک لازم برای انجام خدمت	تحیلات آکادمیک	
قوانین و مقررات بالادستی	بر اساس مجموعه قوانین و مقررات سازمان بهزیستی-قانوم پنجم توسعه- مجموعه قوانین و مقررات خدمات کشوری	

۵- جزییات خدمت

آمار تعداد خدمت گیرندگان	... خدمت گیرندگان در: ☐ ماه ☐ فصل ■ سال		
متوسط مدت زمان ارایه خدمت:			
تواتر	☐ یکبار برای همیشه ... بار در: ☐ ماه ☐ فصل ■ سال		
تعداد بار مراجعه حضوری			
هزینه ارایه خدمت(ریال) به خدمت گیرندگان	مبلغ(مبالغ)	شماره حساب (های) بانکی	پرداخت بصورت الکترونیک
	۷۰۰/۰۰۰		☐
			☐
	...		☐

۶- نحوه دسترسی به خدمت

آدرس دقیق و مستقیم خدمت در وبگاه در صورت الکترونیکی بودن همه یا بخشی از آن

www.

نام سامانه مربوط به خدمت در صورت الکترونیکی بودن همه یا بخشی از آن:

مراحل خدمت	نوع ارائه	رسانه ارتباطی خدمت
در مرحله اطلاع رسانی خدمت	■ الکترونیکی	☐ اینترنتی (مانند وبگاه دستگاه) ☐ تلفن همراه (برنامه کاربردی) ☐ پست الکترونیک ☐ ارسال پستی ☐ تلفن گویا یا مرکز تماس ☐ پیام کوتاه ■ سایر(باذکرنحوه دسترسی) اتوماسیون

		☐ غیرالکترونیکی	ذکر ضرورت مراجعه حضوری	☐ جهت احراز اصالت فرد ☐ جهت احراز اصالت مدرک ☐ نبود زیرساخت ارتباطی مناسب ☐ سایر:
				مراجعه به دستگاه: ☐ ملی ☐ استانی ☐ شهرستانی
	در مرحله درخواست خدمت	■ الکترونیکی		☐ اینترنتی (مانند وبگاه دستگاه) ☐ تلفن همراه (برنامه کاربردی) ☐ پست الکترونیک ☐ ارسال پستی ☐ تلفن گویا یا مرکز تماس ☐ پیام کوتاه ☐ دفاتر پیشخوان شماره قرارداد واگذاری خدمات به دفاتر پیشخوان: ☐ عناوین مشابه دفاتر پیشخوان ■ سایر(باذکرنحوه دسترسی) اتوماسیون
		☐ غیرالکترونیکی	ذکر ضرورت مراجعه حضوری	☐ جهت احراز اصالت فرد ☐ جهت احراز اصالت مدرک ☐ نبود زیرساخت ارتباطی مناسب ☐ سایر:
				مراجعه به دستگاه: ☐ ملی ☐ استانی ☐ شهرستانی
	مرحله تولید خدمت (فرایند داخل دستگاه یا ارتباط با دیگر دستگاه ها)	■ الکترونیکی		☐ اینترنتی (مانند درگاه دستگاه) ☐ اینترانتی (مانند اینترانت داخلی دستگاه یاERP) ☐ پست الکترونیک ■ سایر (باذکرنحوه دسترسی) اتوماسیون
		☐ غیرالکترونیکی	ذکر ضرورت مراجعه حضوری	
	درمرحله ارائه خدمت	■ الکترونیکی		☐ اینترنتی (مانند وبگاه دستگاه) ☐ تلفن همراه (برنامه کاربردی) ☐ پست الکترونیک ☐ ارسال پستی ☐ تلفن گویا یا مرکز تماس ☐ پیام کوتاه ☐ دفاتر پیشخوان شماره قرارداد واگذاری خدمات به دفاتر پیشخوان: ☐ عناوین مشابه دفاتر پیشخوان ■ سایر(باذکرنحوه دسترسی) اتوماسیون
		☐ غیرالکترونیکی	ذکر ضرورت مراجعه حضوری	☐ جهت احراز اصالت فرد ☐ جهت احراز اصالت مدرک ☐ نبود زیرساخت ارتباطی مناسب ☐ سایر:
				مراجعه به دستگاه: ☐ ملی ☐ استانی ☐ شهرستانی

۷- ارتباط خدمت با سایر سامانه ها (بانکهای اطلاعاتی) در دستگاه	نام سامانه های دیگر	فیلدهای موردتبادل	استعلام الکترونیکی		استعلام غیر الکترونیکی
			برخط online	دسته‌ای (Batch)	
	نیروی انتظامی		☐	☐	☐
	شهرداری		☐	☐	☐
			☐	☐	☐
			☐	☐	☐

۸ - ۱	نام دستگاه دیگر	نام سامانه های دستگاه	فیلدهای	مبلغ	استعلام الکترونیکی	اگر استعلام غیرالکترونیکی

		دیگر	موردتبادل	(درصورت پرداخت هزینه)	برخط online	دسته‌ای (Batch)	است، استعلام توسط:
					☐	☐	☐ دستگاه ☐ مراجعه کننده
					☐	☐	☐ دستگاه ☐ مراجعه کننده
					☐	☐	☐ دستگاه ☐ مراجعه کننده
۹- عناوین فرایندهای خدمت	۱-نیاز سنجی						
	۲-تدوین محتوا						
	۳-تدوین سر فصل های آموزشی						
	۴-تعیین اساتید						
	۵-مکاتبه با استان ها						
	۶-ارائه خدمات						
	۷- نظارت و ارزیابی						

۱۰- نمودار ارتباطی فرایندهای خدمت

۱-ورودی فرایند ⟵ تولید دانش ، تغییر نگرش ، رفتار، مهارت آموزی

فعالیت ها ⟵ تهیه دستورالعمل ⟵ نیاز سنجی ⟵ تدوین محتوا ⟵ تدوین سر فصل های آموزشی ⟵ همکاری با استان

۲-ارائه خدمات ⟵ نظارت ⟵ ارزیابی ⟵ گزارش { به استان – به مراجع ذیصلاح و ذینفع }

۳-خروجی ⟵ تولید محتوا، کتاب، کتابچه، مولتی مدیا، بروشور
⟵ تغییر نگرش
⟵ برگزاری همایش، کارگاه های آموزشی

نام و نام خانوادگی تکمیل کننده فرم: منیر ربیعی مقدم	تلفن: داخلی ۲۵۰۴	پست الکترونیک:	واحد مربوط: مرکز پیشگیری

دستورالعمل برنامه پیشگیری از تهدیدات فضای مجازی

مقدمه:

با توجه به این که اکنون جامعه ما از بسیاری جنبه‌ها به فناوری اطلاعات بصورت مستقیم یا غیر مستقیم وابسته است و فضای مجازی فرصت تبدیل شدن یک جامعه جهانی را به وجود آورده بنابراین لازم است عموم مردم نسبت به این پدیده جهانی آشنایی داشته باشند تا در هنگام استفاده از آن با امنیت خاطر، بیشترین بهره وری را داشته باشند. هزاره جدید، پیچیدگی زیادی دارد، جهانی که ما در آن زندگی می کنیم درحال تغییر است.

از لحاظ لغوی در فرهنگ‌های مختلف فضای مجازی یا سایبر به معنی ، محیطی مجازی و غیرملموس موجود در فضای شبکه‌های بین‌المللی(این شبکه هااز طریق شاهراه‌های اطلاعاتی مثل اینترنت بهم وصل هستند)که دراین محیط تمام اطلاعات راجع به روابط افراد، فرهنگ ها، ملت ها، کشورها و به طور کلی هرآنچه در کره خاکی بصورت فیزیکی ملموس وجود دارد(به صورت نوشته، تصویر، صوت، اسناد)در یک فضای مجازی به شکل دیجیتالی وجودداشته و قابل استفاده و دسترس کاربران می‌باشند و به طریق کامپیوتر، اجزا آن و شبکه‌های بین‌المللی بهم مرتبط می‌باشند.

فضای مجازی یا همان سایبر هنوز در مراحل اولیه است.طبیعی است که ا جرایم و سوء استفاده‌های مرتکب شده در این دنیای مجازی جدید هیچ گاه در دنیای حقیقی دیده نشده است.امنیت نا کافی تکنولوژی همراه با طبیعت مجازی آن فرصت مناسبی را در اختیار افراد شرور قرار می‌دهد. نگران کننده‌ترین جنبه فضای مجازی یا سایبر انتشارسریع اطلاعات در آن می‌باشد، مثلاً در لحظه کوتاهی قسمتی از اطلاعاتی که می‌تواند بطور بالقوه مورد سوءاستفاده قرار گیرد کشف می‌شود.در فضای سایبر برای جستجو و پیداکردن این جرایم مشکلات پیچیده تر می‌شود.دردنیای واقعی دزدی از بانک کاملاً مشخص است چرا که بعد از سرقت در خزانه بانک پولی موجود نیست.ولی در تکنولوژی کامپیوتری شدن یک خزانه می‌تواند بدون هیچ علامتی خالی شود.

این برنامه با هدف آگاهسازی و اطلاع رسانی به آحاد مردم در نظر گرفته شده و قصد اصلی کاهش عوامل خطر و افزایش عوامل محافظ در برابر تهدیدات فضای مجازی است.

ویژگی‌های فضای مجازی

کاربران می‌توانند به هرگونه خدمات اطلاعاتی الکترونیکی دستیابی پیدا کنند، بدون درنظرگرفتن اینکه این اطلاعات و خدمات در کدام نقطه دنیا واقع شده‌است. محیط سایبر زمینه فعالیت های سیاسی، اقتصاد، اجتماعی، آموزشی مهم وابزار ضروری برای انجام کلیه فعالیت ها حتی در سطح بین‌المللی بدون دخالت مستقیم آدمی فراهم آورده‌است. محدوده فعالیت کاربر به مرزهای فیزیکی یک خانه یا یک محل کار وحتی مرزهای یک کشور محدود نبوده ودر یک سطح کم هزینه هرکاربر می‌تواند درهرزمانی ودر هر مکانی با مردم در هر نقطه‌ای از جهان ملاقات کند و اطلاعات مبادله کند، بدون اینکه از محل واقعی و هویت فرد خبر داشته باشد.

امنیت سایبر

با وجود تبادل عظیم اطلاعات حیاتی و یا خصوصی از طریق اینترنت باید دید اینترنت تا چه حد برای ارسال داده‌های حساس،(هر گونه دیتا، فیلم، عکس و غیره) مطمئن است .و امنیت شبکه‌ها وقتی داده‌ها درآن جریان پیدا می‌کنند چگونه است؟چرا که با وجود جریان داده‌ها روی اینترنت طبیعی است که فکر کنیم گوش دادن و گرفتن اطلاعات حساس موجود می‌تواند کار ساده‌ای باشد.اما رمزگذاری روی داده ها می‌توانند از دستیابی شکارچیان آنلاین و هکرها به داده‌ها جلوگیری کند.

ماموریت ما در این برنامه:

ایجاد محیطی امن برای کودکان، نوجوانان، جوانان و خانواده ها و تبادل اطلاعات از طریق برگزاری کارگاه های آموزشی تعاملی، تهیه مطالب متناسب سن کودکان و نوجوانان (برای سنین ۱۷ – ۵ سال) همچنین تهیه مطالب کاربردی برای والدین، سرپرستان – مربیان (در مراکز آموزشی مانند: مهدهای کودک – مدارس – مراکز مراقبتی شبانه روزی و . . .)، تهیه فیلم های آموزشی، طراحی بازی ها در این زمینه، برگزاری سخنرانی در محلات با استفاده از ظرفیت پایگاه ها در زمینه های پیشگیری از سوءاستفاده از طریق آنلاین.

هدف کلی: پیشگیری از تهدیدات فضای مجازی

اهداف اختصاصی:

۱. سعی در ایجاد تغییر رویه زندگی دیجیتال مردم
۲. افزایش آگاهی به گروه مخاطب در مورد استفاده بهینه و همچنین نحوه تشخیص خطرات بالقوه آنلاین
۳. افزایش مشارکت کودکان ، نوجوانان و بزرگسالان در گفتگوهای دو طرفه درباره خطرات آنلاین
۴. توانمند سازی کودکان و نوجوانان جهت پیشگیری از سوء استفاده
۵. کاهش مسائل مرتبط با فضای آنلاین در جامعه
۶. آگاهسازی و اطلاع رسانی
۷. حساس سازی خانواده ها
۸. افزایش مهارت های سواد دیجیتال والدین، سرپرستان و مربیان

استراتژی ها:

۱- جمع آوری اطلاعات در خصوص تهدیدات فضای مجازی

۲- آگاهسازی و اطلاع رسانی

۳- حساس سازی خانواده ها

۴- برگزاری کارگاه های آموزشی و آموزش TOT

۵- آموزش مربیان

۶- آموزش والدین و سرپرستان

۷- طراحی راهکارهای مناسب کشوری

۸- ایجاد هماهنگی های بین بخشی (بین سازمانهای دولتی و غیردولتی محلی)

۹- تهیه کتابچه، فیلم های کوتاه آموزشی، پوستر

فعالیت‌ها

۱ ـ تشکیل تیم مدیریت پروژه کشوری

۲ ـ تدوین استراتژی‌ها و فعالیت‌های کشوری

۳ ـ تشکیل تیم مدیریت پروژه استانی

۴- تدوین استراتژی‌ها و فعالیت‌های استانی

۵- شناسایی منابع، سازمان‌ها و نهادهای همکار

۶ـ معرفی برنامه و ضرورت‌های اجرایی برنامه

۷ـ جلب مشارکت و همکاری سازمان‌ها و نهادها براساس اولویت‌های استراتژیک

۸- عقد تفاهم‌نامه همکاری و مشارکت

۹- جمع‌بندی گزارش‌های استانی

وظایف تیم پروژه استانی

۱ ـ تدوین استراتژی‌ها و فعالیت‌های اجرایی برنامه در استان

۲ ـ تدوین وظایف و عوامل اجرایی برنامه در استان

۳ ـ پیشبرد برنامه در استان

۴ ـ طراحی راهکارهای مناسب استانی

۵ ـ تصمیم‌سازی

۶ ـ ارتباط با تیم پروژه کشوری

۷ ـ فراهم آوردن شرایط تهیه محتوای استانی یا منطقه‌ای مبتنی بر شرایط بومی و فرهنگی

مهارت مسوول:

کارشناس پیشگیری از آسیب های اجتماعی

تعاریف:

فضای مجازی: واژه‌ای است که در دهه ۱۹۸۰ وارد ادبیات علمی تخیلی شد و شاغلان در زمینه کامپیوتر و علاقه‌مندان به سرعت آن را به کار بردند و در دهه ۱۹۹۰ رایج شد. در این دوره، استفاده از اینترنت، شبکه و مخابرات دیجیتال سریعاً در حال رشد بود و لفظ فضای مجازی می‌توانست بسیاری از ایده‌ها و پدیده‌های نوظهور را نمایندگی کند.

لفظ ما در فضای مجازی سایبرنتیک است که از یونانی باستان به معنای فرماندار یا راننده مشتق شده، واژه‌ای که نوربرت وینر برای کار پیشگامانه اش در مخابرات الکترونیک و علم کنترل به کار برد.

بدافزار:[1] برنامه‌های رایانه‌ای هستند؛ به علت آنکه معمولاً کاربر را آزار می‌دهند یا خسارتی بوجود می‌آورند، به این نام مشهورند. برخی از آنان فقط کاربر را می‌آزارند. مثلاً وی را مجبور به انجام کاری تکراری می‌کنند. اما برخی دیگر سیستم رایانه‌ای و داده‌های آن را هدف قرار می‌دهند که ممکن است خساراتی به بار آورند. در عین حال ممکن است هدف آن سخت‌افزار سیستم کاربر باشد.

یک نرم‌افزار برپایهٔ نیت سازنده آن به عنوان یک بدافزار شناخته می‌شود .در ۲۹ مارس سال ۲۰۱۰ شرکت سیمنتک شهر شائوژینگ چین را به عنوان پایتخت بدافزار در دنیا معرفی کرد.

مایکروسافت در می ۲۰۱۱ گزارش داد که از هر ۱۴ دانلود در اینترنت یکی شامل بدافزار است. به ویژه شبکه‌های اجتماعی و

از انواع بدافزارها می‌توان به ویروس‌ها، کرم‌ها، اسب‌های تروآ، جاسوس‌افزارها، آگهی‌افزارها، روت‌کیت‌ها و هرزنامه‌ها اشاره کرد.

شکاف دیجیتال: اصطلاحی است در اشاره به فاصله بین مردمانی که به فناوری دیجیتال و فناوری اطلاعات دسترسی موثری دارند با مردمانی که دسترسی بسیار محدودی به این فناوری‌ها داشته یا اصلاً دسترسی ندارند. این عبارت شامل عدم تعادل در دسترسی فیزیکی به فناوری) تکنولوژی) نیز می‌شود، مانند عدم تعادل در داشتن منابع و مهارت برای دسترسی موثر و مفید به فناوری و محسوب شدن به عنوان شهروند دیجیتال .به عبارت دیگر، شکاف دیجیتال یعنی دسترسی نابرابر برخی از اعضای جامعه به فناوری اطلاعات و ارتباطات .شکاف دیجیتال می‌تواند بر پایه جنسیت، درآمد و نژاد باشد. علاوه بر وجود شکاف در یک جامعه، وجود شکاف دیجیتال بین کشورهای جهان را شکاف دیجیتال جهانی می‌گویند.

سواد دیجیتالی: توانایی درک و استفاده از اطلاعات در اشکال چندگانه از یک گروه از منابع کامپیوتری است این دانش ضروری است، زیرا اینترنت از یک ابزار کار بسته محققانه به یک شبکه باز تحقیقی و انتشاراتی جهانی گسترده و رشد یافته تبدیل شده است .این مهارت ها یک فرد را باسواد دیجیتالی می نماید.

قوانین جرایم سایبری در ایران

قانون جرائم رایانه‌ای

بخش یکم

جرائم و مجازاتها

فصل یکم

[1] Malware

جرائم علیه محرمانگی داده‌ها و سامانه‌های رایانه‌ای و مخابراتی

- مبحث یکم ـ دسترسی غیرمجاز

ماده۱ـ هرکس به طور غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی که به‌وسیله تدابیر امنیتی حفاظت‌شده‌است دسترسی یابد، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون ریال تا بیست میلیون ریال یا هر دو مجازات محکوم خواهدشد.

- مبحث دوم ـ شنود غیرمجاز

ماده۲ـ هر کس به طور غیرمجاز محتوای در حال انتقال ارتباطات غیرعمومی در سامانه‌های رایانه‌ای یا مخابراتی یا امواج الکترومغناطیسی یا نوری را شنود کند، به حبس از شش ماه تا دو سال یا جزای نقدی از ده میلیون ریال تا چهل میلیون ریال یا هر دو مجازات محکوم خواهدشد.

- مبحث سوم ـ جاسوسی رایانه‌ای

ماده۳ـ هر کس به طور غیرمجاز نسبت به داده‌های سری درحال انتقال یا ذخیره‌شده در سامانه‌های رایانه‌ای یا مخابراتی یا حاملهای داده مرتکب اعمال زیر شود، به مجازاتهای مقرر محکوم خواهدشد:

الف) دسترسی به داده‌های مذکور یا تحصیل آنها یا شنود محتوای سری در حال انتقال، به حبس از یک تا سه سال یا جزای نقدی از بیست میلیون ریال تا شصت میلیون ریال یا هر دو مجازات.

ب) در دسترس قراردادن داده‌های مذکور برای اشخاص فاقد صلاحیت، به حبس از دو تا ده سال.

ج) افشاء یا در دسترس قرار دادن داده‌های مذکور برای دولت، سازمان، شرکت یا گروه بیگانه یا عاملان آنها، به حبس از پنج تا پانزده سال.

تبصره۱ـ داده‌های سری داده‌هایی است که افشای آنها به امنیت کشور یا منافع ملی لطمه می‌زند.

تبصره۲ـ آئین‌نامه نحوه تعیین و تشخیص داده‌های سری و نحوه طبقه‌بندی و حفاظت آنها ظرف سه ماه از تاریخ تصویب این قانون توسط وزارت اطلاعات با همکاری وزارتخانه‌های دادگستری، کشور، ارتباطات و فناوری اطلاعات و دفاع و پشتیبانی نیروهای مسلح تهیه و به تصویب هیأت وزیران خواهدرسید.

ماده۴ـ هرکس به قصد دسترسی به داده‌های سری موضوع ماده (۳) این قانون، تدابیر امنیتی سامانه‌های رایانه‌ای یا مخابراتی را نقض کند، به حبس از شش ماه تا دو سال یا جزای نقدی از ده میلیون ریال تا چهل میلیون ریال یا هر دو مجازات محکوم خواهدشد.

ماده۵ـ چنانچه مأموران دولتی که مسؤول حفظ داده‌های سری مقرر در ماده (۳)این قانون یا سامانه‌های مربوط هستند و به آنها آموزش لازم داده شده است یا داده‌ها یا سامانه‌های مذکور در اختیار آنها قرار گرفته است بر اثر بی‌احتیاطی، بی‌مبالاتی یا عدم رعایت تدابیر امنیتی موجب دسترسی اشخاص فاقد صلاحیت به داده‌ها، حاملهای داده یا سامانه‌های مذکور شوند، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج میلیون ریال تا چهل میلیون ریال یا هر دو مجازات و انفصال از خدمت از شش ماه تا دو سال محکوم خواهندشد.

فصل دوم

جرائم علیه صحت و تمامیت داده‌ها و سامانه‌های رایانه‌ای و مخابراتی

- مبحث یکم ـ جعل رایانه‌ای

ماده۶ ـ هر کس به طور غیرمجاز مرتکب اعمال زیر شود، جاعل محسوب و به حبس از یک تا پنج سال یا جزای نقدی از بیست میلیونریال تا یکصد میلیون ریال یا هر دو مجازات محکوم خواهدشد:

الف) تغییر یا ایجاد داده‌های قابل استناد یا ایجاد یا واردکردن متقلبانهٔ داده به آنها.

ب) تغییر داده‌ها یا علائم موجود در کارتهای حافظه یا قابل پردازش در سامانه‌های رایانه‌ای یا مخابراتی یا تراشه‌ها یا ایجاد یا وارد کردن متقلبانهٔ داده‌ها یا علائم به آنها.

ماده۷ـ هرکس با علم به مجعول بودن داده‌ها یا کارتها یا تراشه‌ها از آنها استفاده کند، به مجازات مندرج در ماده فوق محکوم خواهدشد.

- مبحث دوم ـ تخریب و اخلال در داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی

ماده۸ ـ هرکس به طور غیرمجاز داده‌های دیگری را از سامانه‌های رایانه‌ای یا مخابراتی یا حاملهای داده حذف یا تخریب یا مختل یا غیرقابل پردازش کند به حبس از شش ماه تا دو سال یا جزای نقدی از ده میلیون ریال تا چهل میلیون ریال یا هر دو مجازات محکوم خواهدشد.

ماده۹ـ هر کس به طور غیرمجاز با اعمالی از قبیل واردکردن، انتقال دادن، پخش، حذف کردن، متوقف کردن، دستکاری یا تخریب داده‌ها یا امواج الکترومغناطیسی یا نوری، سامانه‌های رایانه‌ای یا مخابراتی دیگری را از کار بیندازد یا کارکرد آنها را مختل کند، به حبس از شش ماه تا دو سال یا جزای نقدی از ده میلیون ریال تا چهل میلیون ریال یا هر دو مجازات محکوم خواهدشد.

ماده۱۰ـ هرکس به طور غیرمجاز با اعمالی از قبیل مخفی کردن داده‌ها، تغییر گذر واژه یا رمزنگاری داده‌ها مانع دسترسی اشخاص مجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی شود، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون ریال تا بیست میلیون ریال یا هر دو مجازات محکوم خواهد شد.

ماده۱۱ـ هرکس به قصد خطر انداختن امنیت، آسایش و امنیت عمومی اعمال مذکور در مواد (۸)، (۹) و (۱۰) این قانون را علیه سامانه‌های رایانه‌ای و مخابراتی که برای ارائه خدمات ضروری عمومی به کار می‌روند، از قبیل خدمات درمانی، آب، برق، گاز، مخابرات، حمل و نقل و بانکداری مرتکب شود، به حبس از سه تا ده سال محکوم خواهدشد.

فصل سوم

سرقت و کلاهبرداری مرتبط با رایانه

ماده۱۲ـ هرکس به طور غیرمجاز داده‌های متعلق به دیگری را برباید، چنانچه عین داده‌ها در اختیار صاحب آن باشد، به جرای نقدی از یک میلیون ریال تا بیست میلیون ریال و در غیر این صورت به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون ریال تا بیست میلیون ریال یا هر دو مجازات محکوم خواهد شد.

ماده۱۳ـ هرکس به طور غیرمجاز از سامانه‌های رایانه‌ای یا مخابراتی با ارتکاب اعمالی از قبیل وارد کردن، تغییر، محو، ایجاد یا متوقف کردن داده‌ها یا مختل کردن سامانه، وجه یا مـال یا منفعت یا خدمات یا امتیازات مالی برای خود یا دیگری تحصیل کند علاوه بر رد مال به صاحب آن به حبس از یک تا پنج سال یا جزای نقدی از بیست میلیون ریال تا یکصد میلیون ریال یا هر دو مجازات محکوم خواهد شد.

فصل چهارم

جرائم علیه عفت و اخلاق عمومی

ماده۱۴ـ هرکس به وسیله سامانه‌های رایانه‌ای یا مخابراتی یا حاملهای داده محتویات مستهجن را منتشر، توزیع یا معامله کند یا به قصد تجارت یا افساد تولید یا ذخیره یا نگهداری کند، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج میلیون ریال تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.

تبصره۱ـ ارتکاب اعمال فوق درخصوص محتویات مبتذل موجب محکومیت به حداقل یکی از مجازاتهای فوق می‌شود. محتویات و آثار مبتذل به آثاری اطلاق می‌گردد که دارای صحنه و صور قبیحه باشد.

تبصره۲ـ هرگاه محتویات مستهجن به کمتر از ده نفر ارسال شود، مرتکب به یک میلیون ریال تا پنج میلیون ریال جزای نقدی محکوم خواهد شد.

تبصره۳ـ چنانچه مرتکب اعمال مذکور در این ماده را حرفهٔ خود قرار داده باشد یا به طور سازمان یافته مرتکب شود چنانچه مفسد فی‌الارض شناخته نشود، به حداکثر هر دو مجازات مقرر در این ماده محکوم خواهد شد.

تبصره۴ـ محتویات مستهجن به تصویر، صوت یا متن واقعی یا غیر واقعی یا متنی اطلاق می‌شود که بیانگر برهنگی کامل زن یا مرد یا اندام تناسلی یا آمیزش یا عمل جنسی انسان است.

ماده۱۵ـ هرکس از طریق سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده مرتکب اعمال زیر شود، به ترتیب زیر مجازات خواهد شد:

الف) چنانچه به منظور دستیابی افراد به محتویات مستهجن، آنها را تحریک، ترغیب، تهدید یا تطمیع کند یا فریب دهد یا شیوه دستیابی به آنها را تسهیل نموده یا آموزش دهد، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون ریال تا بیست میلیون ریال یا هر دو مجازات محکوم خواهد شد. ارتکاب این اعمال در خصوص محتویات مبتذل موجب جزای نقدی از دو میلیون ریال تا پنج میلیون ریال است.

ب) چنانچه افراد را به ارتکاب جرائم منافی عفت یا استعمال مواد مخدر یا روان‌گردان یا خودکشی یا انحرافات جنسی یا اعمال خشونت‌آمیز تحریک یا ترغیب یا تهدید یا دعوت کرده یا فریب دهد یا شیوه ارتکاب یا استعمال آنها را تسهیل کند یا آموزش دهد، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون ریال تا بیست میلیون ریال یا هر دو مجازات محکوم می‌شود. تبصره ـ مفاد این ماده و ماده (۱۴) شامل آن دسته از محتویاتی نخواهد شد که برای مقاصد علمی یا هر مصلحت عقلایی دیگر تهیه یا تولید یا نگهداری یا ارائه یا توزیع یا انتشار یا معامله می‌شود.

فصل پنجم

هتک حیثیت و نشر اکاذیب

ماده۱۶ـ هرکس به وسیله سامانه‌های رایانه‌ای یا مخابراتی، فیلم یا صوت یا تصویر دیگری را تغییر دهد یا تحریف کند و آن را منتشر یا با علم به تغییر یا تحریف منتشر کند، به نحوی که عرفاً موجب هتک حیثیت او شود، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج میلیون ریال تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.

تبصره ـ چنانچه تغییر یا تحریف به صورت مستهجن باشد، مرتکب به حداکثر هر دو مجازات مقرر محکوم خواهد شد.

ماده۱۷ـ هر کس به وسیله سامانه‌های رایانه‌ای یا مخابراتی صوت یا تصویر یا فیلم خصوصی یا خانوادگی یا اسرار دیگری را بدون رضایت او جز در موارد قانونی منتشر کند یا دسترس دیگران قرار دهد، به نحوی که منجر به ضرر یا عرفاً موجب هتک حیثیت او شود، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج میلیون ریال تا چهل میلیون ریال یا هر دو مجازات محکوم خواهدشد.

ماده۱۸ـ هر کس به قصد اضرار به غیر یا تشویش اذهان عمومی یا مقامات رسمی به وسیله سامانه رایانه‌ای یا مخابراتی اکاذیبی را منتشر نماید یا در دسترس دیگران قرار دهد یا با همان مقاصد اعمالی را بر خلاف حقیقت، رأساً یا به عنوان نقل قول، به شخص حقیقی یا حقوقی به طور صریح یا تلویحی نسبت دهد، اعم از اینکه از طریق یادشده به نحوی از انحاء ضرر مادی یا معنوی به دیگری وارد شود یا نشود، افزون بر اعاده حیثیت) در صورت امکان)، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج میلیون ریال تا چهل میلیون ریال یا هر دو مجازات محکوم خواهدشد.

فصل ششم

مسؤولیت کیفری اشخاص

ماده۱۹ـ در موارد زیر، چنانچه جرائم رایانه‌ای به نام شخص حقوقی و در راستای منافع آن ارتکاب یابد، شخص حقوقی دارای مسؤولیت کیفری خواهدبود:

الف) هرگاه مدیر شخص حقوقی مرتکب جرم رایانه‌ای شود.

ب) هرگاه مدیر شخص حقوقی دستور ارتکاب جرم رایانه‌ای را صادر کند و جرم به وقوع بپیوندد.

ج) هرگاه یکی از کارمندان شخص حقوقی با اطلاع مدیر یا در اثر عدم نظارت وی مرتکب جرم رایانه‌ای شود.

د) هرگاه تمام یا قسمتی از فعالیت شخص حقوقی به ارتکاب جرم رایانه‌ای اختصاص یافته‌باشد.

تبصره۱ـ منظور از مدیر کسی است که اختیار نمایندگی یا تصمیم‌گیری یا نظارت بر شخص حقوقی را دارد.

تبصره۲ـ مسؤولیت کیفری شخص حقوقی مانع مجازات مرتکب نخواهدبود و در صورت نبود شرایط صدر ماده و عدم انتساب جرم به شخص خصوصی فقط شخص حقیقی مسؤول خواهدبود.

ماده۲۰ـ اشخاص حقوقی موضوع ماده فوق، با توجه به شرایط و اوضاع و احوال جرم ارتکابی، میزان درآمد و نتایج حاصله از ارتکاب جرم، علاوه بر سه تا شش برابر حداکثر جزای نقدی جرم ارتکابی، به ترتیب ذیل محکوم خواهند شد:

الف) چنانچه حداکثر مجازات حبس آن جرم تا پنج سال حبس باشد، تعطیلی موقت شخص حقوقی از یک تا نُه ماه و در صورت تکرار جرم تعطیلی موقت شخص حقوقی از یک تا پنج سال.

ب) چنانچه حداکثر مجازات حبس آن جرم بیش از پنج سال حبس باشد، تعطیلی موقت شخص حقوقی از یک تا سه سال و در صورت تکرار جرم، شخص حقوقی منحل خواهد شد.

تبصره ـ مدیر شخص حقوقی که طبق بند « ب» این ماده منحل می‌شود، تا سه سال حق تأسیس یا نمایندگی یا تصمیم‌گیری یا نظارت بر شخص حقوقی دیگر را نخواهد داشت.

ماده۲۱ـ ارائه‌دهندگان خدمات دسترسی موظفند طبق ضوابط فنی و فهرست مقرر از سوی کارگروه (کمیته) تعیین مصادیق موضوع ماده ذیل محتوای مجرمانه که در چهارچوب قانون تنظیم شده است اعم از محتوای ناشی از جرائم رایانه‌ای و محتوایی که برای ارتکاب جرائم رایانه‌ای به کار می‌رود را پالایش (فیلتر (کنند. در صورتی که عمداً از پالایش (فیلتر) محتوای مجرمانه خودداری کنند، منحل خواهند شد و چنانچه از روی بی‌احتیاطی و بی مبالاتی زمینهٔ دسترسی به محتوای غیر قانونی را فراهم آورند، در مرتبهٔ نخست به جزای نقدی از بیست میلیون ریال تا یکصد میلیون ریال و در مرتبهٔ دوم به جزای نقدی از یکصد میلیون ریال تا یک میلیارد ریال و در مرتبهٔ سوم به یک تا سه سال تعطیلی موقت محکوم خواهند شد.

تبصره۱ـ چنانچه محتوای مجرمانه به تارنماهای (وب سایتهای) مؤسسات عمومی شامل نهادهای زیر نظر ولی‌فقیه و قوای سگانهٔ مقننه، مجریه و قضائیه و مؤسسات عمومی غیردولتی موضوع قانون فهرست نهادها و مؤسسات عمومی غیردولتی مصوب ۱۳۷۳/۴/۱۹ و الحاقات بعدی آن یا به احزاب، جمعیتها، انجمن‌های سیاسی و صنفی و انجمن‌های اسلامی یا اقلیتهای دینی شناخته‌شده یا به سایر اشخاص حقیقی یا حقوقی حاضر در ایران که امکان احراز هویت و ارتباط با آنها وجود دارد تعلق داشته باشد، با دستور مقام قضائی رسیدگی کننده به پرونده و رفع اثر فوری محتوای مجرمانه از سوی دارندگان، تارنما)وب سایت) مزبور تا صدور حکم نهایی پالایش (فیلتر) نخواهد شد.

تبصره۲ـ پالایش (فیلتر) محتوای مجرمانه موضوع شکایت خصوصی با دستور مقام‌قضائی رسیدگیکننده به پرونده انجام خواهد گرفت. برای اطلاع از مصادیق محتوای مجرمانه اینجا کلیک کنید.

ماده۲۲ـ قوهٔ قضاییه موظف است ظرف یک ماه از تاریخ تصویب این قانون کارگروه (کمیته) تعیین مصادیق محتوای مجرمانه را در محل دادستانی کل کشور تشکیل دهد. وزیر یا نمایندهٔ وزارتخانه‌های آموزش و پرورش، ارتباطات و فناوری اطلاعات، اطلاعات، دادگستری، علوم، تحقیقات و فناوری، فرهنگ و ارشاداسلامی، رئیس سازمان تبلیغات اسلامی، رئیس سازمان صدا و سیما و فرمانده نیروی انتظامی، یک نفر خبره در فناوری اطلاعات و ارتباطات به انتخاب کمیسیون صنایع و معادن مجلس شورای اسلامی و یک نفر از نمایندگان عضو کمیسیون قضائی و حقوقی به

انتخاب کمیسیون قضائی و حقوقی و تأیید مجلس شورای اسلامی اعضای کارگروه (کمیته) را تشکیل خواهند داد. ریاست کارگروه (کمیته) به عهدهٔ دادستان کل کشور خواهد بود.

تبصره۱۱ جلسات کارگروه (کمیته) حداقل هر پانزده روز یک بار و با حضور هفت نفر عضو رسمیت می‌یابد و تصمیمات کارگروه (کمیته) با اکثریت نسبی حاضران معتبر خواهد بود.

تبصره۲ـ کارگروه (کمیته) موظف است به شکایات راجع به مصادیق پالایش (فیلتر) شده رسیدگی و نسبت به آنها تصمیم‌گیری کند.

تبصره۳ـ کارگروه (کمیته) موظف است هر شش ماه گزارشی در خصوص روند پالایش (فیلتر) محتوای مجرمانه را به رؤسای قوای سه‌گانه و شورای عالی امنیت ملی تقدیم کند.

ماده۲۳ـ ارائه‌دهندگان خدمات میزبانی موظفند به محض دریافت دستور کارگروه (کمیته) تعیین مصادیق مذکور در مادهٔ فوق یا مقام قضائی رسیدگیکننده به پرونده مبنی بر وجود محتوای مجرمانه در سامانه‌های رایانه‌ای خود از ادامهٔ دسترسی به آن ممانعت به عمل آورند. چنانچه عمداً از اجرای دستور کارگروه (کمیته) یا مقام قضائی خودداری کنند، منحل خواهند شد. در غیر این صورت، چنانچه در اثر بی احتیاطی و بی‌مبالاتی زمینهٔ دسترسی به محتوای مجرمانه مزبور را فراهم کنند، در مرتبهٔ نخست به جزای نقدی از بیست میلیون ریال تا یکصد میلیون ریال و در مرتبهٔ دوم به یکصد میلیون ریال تا یک میلیارد ریال و در مرتبهٔ سوم به یک تا سه سال تعطیلی موقت محکوم خواهندشد .تبصره ـ ارائه‌دهندگان خدمات میزبانی موظفند به محض آگاهی از وجود محتوای مجرمانه مراتب را به کارگروه (کمیته) تعیین مصادیق اطلاع دهند.

ماده۲۴ـ هرکس بدون مجوز قانونی از پهنای باند بین‌المللی برای برقراری ارتباطات مخابراتی مبتنی بر پروتکل اینترنتی از خارج ایران به داخل یا برعکس استفاده کند، به حبس از یک تا سه سال یا جزای نقدی از یکصد میلیون ریال تا یک میلیارد ریال یا هر دو مجازات محکوم خواهد شد.

فصل هفتم

سایر جرائم

ماده۲۵ـ هر شخصی که مرتکب اعمال زیر شود، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون ریال تا بیست میلیون ریال یا هر دو مجازات محکوم خواهدشد:

الف) تولید یا انتشار یا توزیع و در دسترس قرار دادن یا معاملهٔ داده‌ها یا نرم‌افزارها یا هر نوع ابزار الکترونیکی که صرفاً به منظور ارتکاب جرائم رایانه‌ای به کار می‌رود.

ب) فروش یا انتشار یا در دسترس قراردادن گذر واژه یا هر داده‌ای که امکان دسترسی غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی متعلق به دیگری را بدون رضایت او فراهم میکند.

ج) انتشار یا در دسترس قراردادن محتویات آموزش دسترسی غیرمجاز، شنود غیرمجاز، جاسوسی رایانه‌ای و تخریب و اخلال در داده‌ها یا سیستم‌های رایانه‌ای و مخابراتی. تبصره ـ چنانچه مرتکب، اعمال یادشده را حرفه خود قرار داده باشد، به حداکثر هر دو مجازات مقرر در این ماده محکوم خواهد شد.

فصل هشتم

تشدید مجازاتها

ماده۲۶ـ در موارد زیر، حسب مورد مرتکب به بیش از دو سوم حداکثر یک یا دو مجازات مقرر محکوم خواهد شد:

الف) هر یک از کارمندان و کارکنان اداره‌ها و سازمانها یا شوراها و یا شهرداریها و موسسه‌ها و شرکتهای دولتی و یا وابسته به دولت یا نهادهای انقلابی و بنیادها و مؤسسه‌هایی که زیر نظر ولی‌فقیه اداره می‌شوند و دیوان محاسبات و مؤسسه‌هایی که با کمک مستمر دولت اداره می‌شوند و یا دارندگان پایه قضائی و به طور کلی اعضاء و کارکنان قوای سه‌گانه و همچنین نیروهای مسلح و مأموران به خدمت عمومی اعم از رسمی و غیررسمی به مناسبت انجام وظیفه مرتکب جرم رایانه‌ای شده باشند.

ب) متصدی یا متصرف قانونی شبکه‌های رایانه‌ای یا مخابراتی که به مناسبت شغل خود مرتکب جرم رایانه‌ای شده باشد.

ج) داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی، متعلق به دولت یا نهادها و مراکز ارائه‌دهنده خدمات عمومی باشد.

د) جرم به صورت سازمان یافته ارتکاب یافته باشد.

ه(جرم در سطح گسترده‌ای ارتکاب یافته باشد.

ماده۲۷ـ در صورت تکرار جرم برای بیش از دو بار دادگاه می‌تواند مرتکب را از خدمات الکترونیکی عمومی از قبیل اشتراک اینترنت، تلفن همراه، اخذ نام دامنهٔ مرتبه بالای کشوری و بانکداری الکترونیکی محروم کند:

الف) چنانچه مجازات حبس آن جرم نودویک روز تا دو سال حبس باشد، محرومیت از یک ماه تا یک سال.

ب) چنانچه مجازات حبس آن جرم دو تا پنج سال حبس باشد، محرومیت از یک تا سه سال.

ج) چنانچه مجازات حبس آن جرم بیش از پنج سال حبس باشد، محرومیت از سه تا پنج سال.

بخش دوم

آئین‌دادرسی

فصل یکم

صلاحیت

ماده۲۸ـ علاوه بر موارد پیش‌بینی شده در دیگر قوانین، دادگاههای ایران در موارد زیر نیز صالح به رسیدگی خواهند بود:

الف) داده‌های مجرمانه یا داده‌هایی که برای ارتکاب جرم به کار رفته است به هر نحو در سامانه‌های رایانه‌ای و مخابراتی یا حاملهای دادهٔ موجود در قلمرو حاکمیت زمینی، دریایی و هوایی جمهوری اسلامی ایران ذخیره شده باشد.

ب) جرم از طریق تارنماهای (وب‌سایتهای) دارای دامنه مرتبه بالای کد کشوری ایران ارتکاب یافته باشد.

ج) جرم توسط هر ایرانی یا غیرایرانی در خارج از ایران علیه سامانه‌های رایانه‌ای و مخابراتی و تارنماهای (وب‌سایتهای) مورد استفاده یا تحت کنترل قوای سه‌گانه یا نهاد رهبری یا نمایندگی‌های رسمی دولت یا هر نهاد یا مؤسسه‌ای که خدمات عمومی ارائه می‌دهد یا علیه تارنماهای (وب‌سایتهای (دارای دامنهٔ مرتبه بالای کدکشوری ایران در سطح گسترده ارتکاب یافته باشد.

د) جرائم رایانه‌ای متضمن سوءاستفاده از اشخاص کمتر از هجده سال، اعم از آنکه مرتکب یا بزه‌دیده ایرانی یا غیرایرانی باشد.

ماده۲۹ـ چنانچه جرم رایانه‌ای در محلی کشف یا گزارش شود، ولی محل وقوع آن معلوم نباشد، دادسرای محل کشف مکلف است تحقیقات مقدماتی را انجام دهد .چنانچه محل وقوع جرم مشخص نشود، دادسرا پس از اتمام تحقیقات مبادرت به صدور قرار میکند و دادگاه مربوط نیز رأی مقتضی را صادر خواهد کرد.

ماده۳۰ـ قوه قضائیه موظف است به تناسب ضرورت شعبه یا شعبی از دادسراها، دادگاههای عمومی و انقلاب، نظامی و تجدیدنظر را برای رسیدگی به جرائم رایانه‌ای اختصاص دهد .تبصره ـ قضات دادسراها و دادگاه‌های مذکور از میان قضاتی که آشنایی لازم به‌امور رایانه دارند انتخاب خواهند شد.

ماده۳۱ ـ در صورت بروز اختلاف در صلاحیت، حل اختلاف مطابق مقررات قانون آئین‌دادرسی دادگاه‌های عمومی و انقلاب در امور مدنی خواهدبود.

فصل دوم

جمع‌آوری ادله الکترونیکی

- مبحث اول ـ نگهداری داده‌ها

ماده۳۲ـ ارائه‌دهندگان خدمات دسترسی موظفند داده‌های ترافیک را حداقل تا شش ماه پس از ایجاد و اطلاعات کاربران را حداقل تا شش ماه پس از خاتمه اشتراک نگهداری کنند.

تبصره۱ـ داده ترافیک هرگونه داده‌ای است که سامانه‌های رایانه‌ای در زنجیره ارتباطات رایانه‌ای و مخابراتی تولید میکنند تا امکان ردیابی آنها از مبدأ تا مقصد وجود داشته باشد. این داده‌ها شامل اطلاعاتی از قبیل مبدأ، مسیر، تاریخ، زمان، مدت و حجم ارتباط و نوع خدمات مربوطه می‌شود.

تبصره۲ـ اطلاعات کاربر هرگونه اطلاعات راجع به کاربر خدمات دسترسی از قبیل نوع خدمات، امکانات فنی مورد استفاده و مدت زمان آن، هویت، آدرس جغرافیایی یا پستی یا پروتکل اینترنتی(IP) ، شماره تلفن و سایر مشخصات فردی اوست.

ماده۳۳ـ ارائه‌دهندگان خدمات میزبانی داخلی موظفند اطلاعات کاربران خود را حداقل تا شش ماه پس از خاتمه اشتراک و محتوای ذخیره شده و داده ترافیک حاصل از تغییرات ایجاد شده را حداقل تا پانزده روز نگهداری کنند.

- مبحث دوم ـ حفظ فوری داده‌های رایانه‌ای ذخیره شده

ماده۳۴ـ هرگاه حفظ داده‌های رایانه‌ای ذخیره شده برای تحقیق یا دادرسی لازم باشد، مقام قضائی می‌تواند دستور حفاظت از آنها را برای اشخاصی که به نحوی تحت تصرف یا کنترل دارند صادر کند. در شرایط فوری، نظیر خطر آسیب‌دیدن یا تغییر یا از بین رفتن داده‌ها، ضابطان قضائی می‌توانند رأساً دستور حفاظت را صادر کنند و مراتب را حداکثر تا ۲۴ ساعت به اطلاع مقام قضائی برسانند. چنانچه هر یک از کارکنان دولت یا ضابطان قضائی یا سایر اشخاص از اجرای این دستور خودداری یا داده‌های حفاظت شده را افشاء کنند یا اشخاصی که داده‌های مزبور به آنها مربوط می‌شود را از مفاد دستور صادره آگاه کنند، ضابطان قضائی و کارکنان دولت به مجازات امتناع از دستور مقام قضائی و سایر اشخاص به حبس از نودویک روز تا شش ماه یا جزای نقدی از پنج‌میلیون ریال تا ده‌میلیون ریال یا هر دو مجازات محکوم خواهند شد.

تبصره۱ـ حفظ داده‌ها به منزله ارائه یا افشاء آنها نبوده و مستلزم رعایت مقررات مربوط است.

تبصره۲ـ مدت زمان حفاظت از داده‌ها حداکثر سه ماه است و در صورت لزوم با دستور مقام قضائی قابل تمدید است.

- مبحث سوم ـ ارائه داده‌ها

ماده۳۵ـ مقام قضائی می‌تواند دستور ارائه داده‌های حفاظت‌شده مذکور در مواد (۳۲)، (۳۳) و (۳۴) فوق را به اشخاص یادشده بدهد تا در اختیار ضابطان قرارگیرد. مستنکف از اجراء این دستور به مجازات مقرر در ماده (۳۴) این قانون محکوم خواهد شد.

- مبحث چهارم ـ تفتیش و توقیف داده‌ها و سامانه‌های رایانه‌ای و مخابراتی

ماده۳۶ـ تفتیش و توقیف داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی به موجب دستور قضائی و در مواردی به عمل می‌آید که ظن قوی به کشف جرم یا شناسایی متهم یا ادله جرم وجود داشته باشد.

ماده۳۷ـ تفتیش و توقیف داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی در حضور متصرفان قانونی یا اشخاصی که به نحوی آنها را تحت کنترل قانونی دارند، نظیر متصدیان سامانه‌ها انجام خواهد شد. در غیر این صورت، قاضی با ذکر دلایل دستور تفتیش و توقیف بدون حضور اشخاص مذکور را صادر خواهد کرد.

ماده۳۸ـ دستور تفتیش و توقیف باید شامل اطلاعاتی باشد که به اجراء صحیح آن کمک میکند، از جمله اجراء دستور در محل یا خارج از آن، مشخصات مکان و محدوده تفتیش و توقیف، نوع و میزان داده‌های مورد نظر، نوع و تعداد سخت افزارها و نرم‌افزارها، نحوه دستیابی به داده‌های رمزنگاری یا حذف شده و زمان تقریبی انجام تفتیش و توقیف.

ماده۳۹ـ تفتیش داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی شامل اقدامات ذیل می‌شود:

الف) دسترسی به تمام یا بخشی از سامانه‌های رایانه‌ای یا مخابراتی.

ب) دسترسی به حامل‌های داده از قبیل دیسکت‌ها یا لوحهای فشرده یا کارتهای حافظه.

ج) دستیابی به داده‌های حذف یا رمزنگاری شده.

ماده۴۰ ـ در توقیف داده‌ها، با رعایت تناسب، نوع، اهمیت و نقش آنها در ارتکاب جرم، به روش‌هایی از قبیل چاپ داده‌ها، کپی‌برداری یا تصویربرداری از تمام یا بخشی از داده‌ها، غیرقابل دسترس کردن داده‌ها با روش‌هایی از قبیل تغییر گذرواژه یا رمزنگاری و ضبط حاملهای داده عمل می‌شود.

ماده۴۱ ـ در هریک از موارد زیر سامانه‌های رایانه‌ای یا مخابراتی توقیف خواهد شد:

الف) داده‌های ذخیره شده به سهولت در دسترس نبوده یا حجم زیادی داشته باشد،

ب) تفتیش و تجزیه و تحلیل داده‌ها بدون سامانه سخت افزاری امکان پذیر نباشد،

ج) متصرف قانونی سامانه رضایت داده باشد،

د) تصویربرداری (کپی‌برداری) از داده‌ها به لحاظ فنی امکان‌پذیر نباشد،

هـ) تفتیش در محل باعث آسیب‌داده‌ها شود،

ماده۴۲ ـ توقیف سامانه‌های رایانه‌ای یا مخابراتی متناسب با نوع و اهمیت و نقش آنها در ارتکاب جرم با روش‌هایی از تغییر گذرواژه به منظور عدم دسترسی به سامانه، پلمپ سامانه در محل استقرار و ضبط سامانه صورت می‌گیرد.

ماده۴۳ ـ چنانچه در حین اجراء دستور تفتیش و توقیف، تفتیش داده‌های مرتبط با جرم ارتکابی در سایر سامانه‌های رایانه‌ای یا مخابراتی که تحت کنترل یا تصرف متهم قراردارد ضروری باشد، ضابطان با دستور مقام قضائی دامنه تفتیش و توقیف را به سامانه‌های مذکور گسترش داده و داده‌های مورد نظر را تفتیش یا توقیف خواهند کرد.

ماده۴۴ـ چنانچه توقیف داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی موجب ایراد لطمه جانی یا خسارت مالی شدید به اشخاص یا اخلال در ارائه خدمات عمومی شود ممنوع است.

ماده۴۵ـ در مواردی که اصل داده‌ها توقیف می‌شود، ذی‌نفع حق دارد پس از پرداخت هزینه از آنها کپی دریافت کند، مشروط به این که ارائه داده‌های توقیف‌شده مجرمانه یا منافی با محرمانه بودن تحقیقات نباشد و به روند تحقیقات لطمه‌ای وارد نشود.

ماده۴۶ـ در مواردی که اصل داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی توقیف می‌شود، قاضی موظف است با لحاظ نوع و میزان داده‌ها و نوع و تعداد سخت افزارها و نرم‌افزارهای مـورد نظر و نقش آنها در جرم ارتـکابی، در مهلت متناسب و متعارف نسبت به آنها تعیین تکلیف کند.

ماده۴۷ـ متضرر می‌تواند در مورد عملیات و اقدامهای مأموران در توقیف داده‌ها و سامانه‌های رایانه‌ای و مخابراتی، اعتراض کتبی خود را همراه با دلایل ظرف ده روز به‌مرجع قضائی دستوردهنده تسلیم نماید. به درخواست یادشده خارج از نوبت رسیدگی گردیده و تصمیم اتخاذ شده قابل اعتراض است.

مبحث پنجم ـ شنود محتوای ارتباطات رایانه‌ای

ماده۴۸ـ شنود محتوای در حال انتقال ارتباطات غیرعمومی در سامانه‌های رایانه‌ای یا مخابراتی مطابق مقررات راجع به شنود مکالمات تلفنی خواهد بود.

تبصره ـ دسترسی به محتوای ارتباطات غیرعمومی ذخیره‌شده، نظیر پست الکترونیکی یا پیامک در حکم شنود و مستلزم رعایت مقررات مربوط است.

فصل سوم

استناد پذیری ادله الکترونیکی

ماده۴۹ـ به منظور حفظ صحت و تمامیت، اعتبار و انکارناپذیری ادله الکترونیکی جمع‌آوری شده، لازم است مطابق آئین‌نامه مربوط از آنها نگهداری و مراقبت به عمل آید.

ماده۵۰ـ چنانچه داده‌های رایانه‌ای توسط طرف دعوا یا شخص ثالثی که از دعوا آگاهی نداشته، ایجاد یا پردازش یا ذخیره یا منتقل شده باشد و سامانه رایانه‌ای یا مخابراتی مربوط به نحوی درست عمل کند که به صحت و تمامیت، اعتبار و انکارناپذیری داده‌ها خدشه وارد نشده باشد، قابل استناد خواهد بود.

ماده۵۱ـ کلیه مقررات مندرج در فصل‌های دوم و سوم این بخش، علاوه بر جرائم رایانه‌ای شامل سایر جرائمی که ادله الکترونیکی در آنها مورد استناد قرار می‌گیرد نیز می‌شود.

بخش سوم

سایر مقررات

ماده۵۲ ـ در مواردی که سامانه رایانه‌ای یا مخابراتی به عنوان وسیله ارتکاب جرم به کار رفته و در این قانون برای عمل مزبور مجازاتی پیش‌بینی نشده‌است، مطابق قوانین جزائی مربوط عمل خواهد شد. تبصره ـ در مواردی که در بخش دوم این قانون برای رسیدگی به جرائم رایانه‌ای مقررات خاصی از جهت آئین‌دادرسی پیش‌بینی نشده است طبق مقررات قانون آئین دادرسی کیفری اقدام خواهد شد.

ماده۵۳ـ میزان جزاهای نقدی این قانون بر اساس نرخ رسمی تورم حسب اعلام بانک مرکزی هر سه سال یک بار با پیشنهاد رئیس قوه قضائیه و تصویب هیأت وزیران قابل تغییر است.

ماده۵۴ـ آیین‌نامه‌های مربوط به جمع‌آوری و استنادپذیری ادله الکترونیکی ظرف مدت شش ماه از تاریخ تصویب این قانون توسط وزارت دادگستری با همکاری وزارت ارتباطات و فناوری اطلاعات تهیه و به تصویب رئیس قوه قضائیه خواهد رسید.

ماده۵۵ـ شماره مواد (۱) تا (۵۴) این قانون به عنوان مواد (۷۲۹) تا (۷۸۲ (قانون مجازات اسلامی) بخش تعزیرات) با عنوان فصل جرائم رایانه‌ای منظور و شماره ماده (۷۲۹) قانون مجازات اسلامی به شماره (۷۸۳) اصلاح گردد.

ماده۵۶ـ قوانین و مقررات مغایر با این قانون ملغی است. قانون فوق مشتمل بر ۵۶ ماده و ۲۵ تبصره در جلسه علنی روز سه شنبه مورخ پنجم خردادماه یکهزار و سیصد و هشتاد و هشت مجلس شورای اسلامی تصویب و در تاریخ ۱۳۸۸/۳/۲۰ به تأیید شورای نگهبان رسید.