مواد کتاب تعزیرات قانون مجازات اسلامی

فصل جرایم رایانه ای

به انضمام آیین دادرسی و آیین نامه مربوطه

با آخرین اصلاحات

از جمله:

قانون کاهش مجازات حبس تعزیری

تصویب نامه تعدیل میزان مبالغ مجازات نقدی جرایم و تخلفات مندرج در قوانین و مقررات مختلف

تدوین: دکتر جواد جاویدنیا

تیرماه ۱۴۰۰

فهرست

کتاب تعزیرات قانون مجازات اسلامی- فصل جرائم رایانه‌ای[1]

بخش یکم ـ جرائم و مجازاتها

فصل یکم ـ جرائم علیه محرمانگی داده‌ها و سامانه‌های رایانه‌ای و مخابراتی

مبحث یکم ـ دسترسی غیرمجاز

ماده۷۲۹(ماده۱)ـ 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 یک‌سال یا جزای نقدی از **بیست میلیون (۲۰.۰۰۰.۰۰۰) ریال تا هشتاد میلیون (۸۰.۰۰۰.۰۰۰) ریال**[2] یا هر دو مجازات محکوم خواهدشد.[3]

مبحث دوم ـ شنود غیرمجاز

ماده۷۳۰(ماده۲)ـ 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 **بیست و پنج**

---

[1] مصوب ۱۳۸۸/۳/۵ مجلس شورای اسلامی- روزنامه رسمی شماره ۱۸۷۴۲مورخ ۱۳۸۸/۴/۱۷

توضیح اینکه طبق مصوبه مذکور این قسمت به عنوان مواد ۷۲۹ الی ۷۸۲ قانون مجازات اسلامی الحاق گردیده است.

[2] اصلاحی به موجب تصویبنامه ۱۳۹۹/۱۱/۸ هیات وزیران درخصوص «تعدیل میزان مبالغ مجازات نقدی جرایم و تخلفات مندرج در قوانین و مقررات مختلف» موضوع ابلاغیه شماره ۱۵۷۳۹۷۳/ت۵۷۷۵۲ه – ۱۳۹۹/۱۲/۲۵

[3] **نظریه مشورتی اداره کل حقوقی قوه قضائیه به شماره ۷/۹۳/٦٥٦ -۱۳۹۳/۳/۲٤ روزنامه رسمی ۲۰۲۹۲-۱۳۹۳/۸/۱٤**

سؤال:

۱- درماده ۱ قانون جرایم رایانه ای اشاره دارد به دسترسی غیر مجاز به داده ها. حال، منظور از دسترسی غیرمجاز چیست؟ و این دسترسی به صورت مجازی را از طریق رهگذر سامانه‌های رایانه‌ای می باشد یا می تواند از طریق فیزیکی و اسنادی نیز صورت پذیرد توضیحاً اینکه برخی از همکاران معتقدند که دسترسی غیرمجاز با توجه به فصل یکم قانون جرایم رایانه ای تحت عنوان جرایم علیه محرمانگی و داده ها و سیستم های رایانه ای و مخابراتی تنها از طریق دانش فنی و نرم افزاری و از طریق کنش روی دادهها در محیط مجازی می باشد.

۲ اگر فردی از طریق فیزیکی رمز ورودی به ایمیل شخصی را بدست آورد با فریب یا سوء استفاده از اعتماد صاحب ایمیل آیا مشمول ماده ۱ قانون جرایم رایانه ای می شود؟

نظریه مشورتی اداره کل حقوقی قوه قضائیه

۱- با توجه به اطلاق ماده یک قانون جرائم رایانه ای، صرف دسترسی غیرمجاز به داده ها یا سامانه های رایانه ای یا مخابراتی که به وسیله تدابیر امنیتی حفاظت شده باشد مشمول مقررات ماده مذکور می باشد و طریق دسترسی اعم از مستقیم (فیزیکی) یا با واسطه (از طریق شبکه) تأثیری در قضیه ندارد.

۲- در فرض سؤال صرف به دست آوردن رمز ورودی به ایمیل اشخاص جرم نیست ولی چنانچه از طریق رمزی که به دست آورده، به طور غیر مجاز به داده یا سامانه دسترسی پیدا کند، می تواند از مصادیق جرم موضوع ماده یک قانون جرائم رایانه ای باشد. به هر حال تشخیص مصداق با قاضی رسیدگی کننده است.

میلیون (۲۵.۰۰۰.۰۰۰) ریال تا یکصد و پنجاه میلیون (۱۵۰.۰۰۰.۰۰۰) ریال[1] یا هر دو مجازات محکوم خواهدشد.

مبحث سوم ـ جاسوسی رایانه‌ای

ماده۷۳۱(ماده۳)ـ 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 **شصت میلیون (۶۰.۰۰۰.۰۰۰) ریال تا یکصد و هشتاد میلیون (۱۸۰.۰۰۰.۰۰۰) ریال**[2] 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.

ماده۷۳۲(ماده٤)ـ 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 **بیست و پنج میلیون (۲۵.۰۰۰.۰۰۰) ریال تا یکصد و پنجاه میلیون (۱۵۰.۰۰۰.۰۰۰) ریال**[3] یا هر دو مجازات محکوم خواهدشد.

ماده۷۳۳ (ماده۵)ـ 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 **پانزده میلیون (۱۵.۰۰۰.۰۰۰) ریال تا یکصد میلیون (۱۰۰.۰۰۰.۰۰۰) ریال**[4] یا هر دو مجازات و انفصال از خدمت از شش ماه تا دو سال محکوم خواهندشد.

---

[1] اصلاحی به موجب تصویبنامه ۱۳۹۹/۱۱/۸ هیات وزیران درخصوص «تعدیل میزان مبالغ مجازات نقدی جرایم و تخلفات مندرج در قوانین و مقررات مختلف» موضوع ابلاغیه شماره ۱۵۷۳۹۷۳/ت۵۷۷۵۲ه – ۱۳۹۹/۱۲/۲۵

[2] همان

[3] همان

[4] همان

فصل دوم ـ جرائم علیه صحت و تمامیت داده‌ها و سامانه‌های رایانه‌ای و مخابراتی

مبحث یکم ـ جعل رایانه‌ای

ماده ۷۳۴ (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 **پنجاه میلیون (۵۰.۰۰۰.۰۰۰) ریال تا دویست و پنجاه میلیون (۲۵۰.۰۰۰.۰۰۰) ریال**[۱] 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.

ماده ۷۳۵(ماده۷)ـ 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

ماده ۷۳۶ (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 **بیست و پنج میلیون (۲۵.۰۰۰.۰۰۰) ریال تا یکصد میلیون (۱۰۰.۰۰۰.۰۰۰) ریال**[۲] یا هر دو مجازات محکوم خواهدشد.

ماده ۷۳۷(ماده۹)ـ 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 **بیست و پنج میلیون (۲۵.۰۰۰.۰۰۰) ریال تا یکصد میلیون (۱۰۰.۰۰۰.۰۰۰) ریال**[۳] یا هر دو مجازات محکوم خواهدشد.

ماده ۷۳۸(ماده۱۰)ـ 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 **بیست میلیون (۲۰.۰۰۰.۰۰۰) ریال تا هشتاد میلیون (۸۰.۰۰۰.۰۰۰) ریال**[۴] یا هر دو مجازات محکوم خواهد شد.

ماده ۷۳۹(ماده۱۱)ـ هرکس به قصد خطر انداختن امنیت، آسایش و امنیت عمومی اعمال مذکور در مواد (۷۳۶)، (۷۳۷) و (۷۳۸) این قانون را علیه سامانه‌های رایانه‌ای و مخابراتی که برای ارائه خدمات ضروری عمومی به کار می‌روند، از

---

[۱] همان

[۲] همان

[۳] همان

[۴] همان

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 ـ سرقت و کلاهبرداری مرتبط با رایانه

ماده۷٤۰(ماده۱۲)ـ هرکس به طور غیرمجاز داده‌های متعلق به دیگری را برباید، چنانچه عین داده‌ها در اختیار صاحب آن باشد، به جرای نقدی از **شش میلیون (٦.۰۰۰.۰۰۰) ریال تا پنجاه میلیون (۵۰.۰۰۰.۰۰۰) ریال**[1] و در غیر این صورت به حبس از نود و یک روز تا یک سال یا جزای نقدی از **بیست میلیون (۲۰.۰۰۰.۰۰۰) ریال تا هشتاد میلیون (۸۰.۰۰۰.۰۰۰) ریال**[2] یا هر دو مجازات محکوم خواهد شد.

ماده۷٤۱(ماده۱۳)ـ 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 **پنجاه میلیون (۵۰.۰۰۰.۰۰۰) ریال تا دویست و پنجاه میلیون (۲۵۰.۰۰۰.۰۰۰) ریال**[3] یا هر دو مجازات محکوم خواهد شد.[4]

---

[1] همان

[2] همان

[3] همان

[4] **نظریه مشورتی اداره کل حقوقی قوه قضائیه** به **شماره ۷/۹۳/۱۱٦۱ -۱۳۹۳/۵/۱۸ روزنامه رسمی ۲۰۳۱۵-۱۳۹۳/۹/۱۱**

سؤال:

۱- نظر به آنکه مطابق ماده۷۴۱ قانون مجازات اسلامی الحاقی۸۸/۳/۵ درخصوص کلاهبرداری مرتبط با رایانه قید شده هر کس به طور غیر مجاز از سامانه‌های رایانه‌ای یا مخابراتی با ارتکاب اعمالی از قبیل وارد کردن تغییر و ... وجه یا مال یا منفعت یا خدمات یا امتیازات مالی برای خود یا دیگری تحصیل کند، آیا منظور از کلمه وارد کردن در متن ماده به طور مطلق است؟ یعنی هرگونه وارد کردن اعم از اینکه کلاهبردار داده‌ها را با این فرض که در دسترس او باشد یا داده‌ها در دسترس او نبوده و با استفاده از فرامین یا افعالی آنها را وارد کند، می‌باشد یا صرفا عمل وارد کردن ناظر به آن است که کلاهبردار اطلاعات و داده‌ها را در اختیار نداشته و با توسل به وسایل متقلبانه اعم از هک کردن یا روش های دیگر آنها را تحصیل وارد نماید؟

۲- در فرض سوال چنانچه فردی یک عابر بانک را که متعلق به دیگری است سرقت نماید سپس با مراجعه به باجه خود پرداز با وارد کردن رمز که روی کارت نوشته شده است وجوه آن را سرقت نماید آیا امر فوق مشتمل بر یک عنوان که همان سرقت است، می‌باشد یا اینکه سرقت توام با کلاهبرداری مرتبط با رایانه را نیز شامل می‌گردد؟

نظریه مشورتی اداره کل حقوقی قوه قضائیه

۱- منظور از فعل وارد کردن، در ماده ۷۴۱ الحاقی مصوب ۱۳۸۸/۳/۵ قانون مجازات اسلامی در فصل مربوط به جرائم رایانه ای ، وارد کردن داده ها به هر ترتیبی است که منتهی به تحصیل وجه یا مال یا منفعت یا خدمات یا امتیازات مالی برای خود یا اشخاص دیگر باشد؛ اعم از اینکه شخص مذکور قبلاً اطلاعات مربوط به داده ها را در اختیار داشته یا به وسائل متقلّبانه، اطلاعات مورد نظر خود را کسب نماید.

۲- چون ملاک تحقق جرائم مندرج در قانون جرایم رایانه ای، استفاده از سامانه های رایانه‌ای یا مخابراتی یا حاملهای داده است و در فرض سؤال به لحاظ اینکه سرقت انجام شده با استفاده غیر مجاز از داده‌های رایانه‌ای و وارد نمودن رمز کارت عابر بانک دیگری صورت گرفته است،موضوع مشمول ماده۷۴۱ الحاقی به قانون مجازات اسلامی (موضوع ماده۱۳ قانون جرایم رایانه ای مصوب ۱۳۸۸/۳/۵) است.

فصل چهارم ـ جرائم علیه عفت و اخلاق عمومی

ماده۷۴۲(ماده۱۴)ـ 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 **پانزده میلیون (۱۵.۰۰۰.۰۰۰) ریال تا یکصد میلیون (۱۰۰.۰۰۰.۰۰۰) ریال**[۱] 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 می گردد که دارای صحنه و صور قبیحه باشد.

تبصره۲ـ هرگاه محتویات مستهجن به کمتر از ده نفر ارسال شود، مرتکب به **پنج میلیون (۵.۰۰۰.۰۰۰) ریال تا بیست میلیون (۲۰.۰۰۰.۰۰۰) ریال**[۲] 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.

تبصره٤ـ 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.

ماده۷۴۳(ماده۱۵)ـ 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 **بیست میلیون (۲۰.۰۰۰.۰۰۰) ریال تا هشتاد میلیون (۸۰.۰۰۰.۰۰۰) ریال**[۳] یا هر دو مجازات محکوم خواهد شد.

ارتکاب این اعمال در خصوص محتویات مبتذل موجب جزای نقدی از **پنج میلیون (۵.۰۰۰.۰۰۰) ریال تا بیست میلیون (۲۰.۰۰۰.۰۰۰) ریال**[٤] 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

---

[۱] اصلاحی به موجب تصویبنامه ۱۳۹۹/۱۱/۸ هیات وزیران درخصوص «تعدیل میزان مبالغ مجازات نقدی جرایم و تخلفات مندرج در قوانین و مقررات مختلف» موضوع ابلاغیه شماره ۱۵۷۳۹۷۳/ت۵۷۷۵۲ه – ۱۳۹۹/۱۲/۲۵

[۲] همان

[۳] همان

[٤] همان

آموزش دهد، به حبس از نود و یک روز تا یک سال یا جزای نقدی از **بیست میلیون (۲۰.۰۰۰.۰۰۰) ریال تا هشتاد میلیون (۸۰.۰۰۰.۰۰۰) ریال**[۱] یا هر دو مجازات محکوم می‌شود.

تبصره ـ مفاد این ماده و ماده (۷۴۲) 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 ـ هتک حیثیت و نشر اکاذیب

ماده۷۴۴(ماده۱۶)ـ 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 **چهل و پنج و نیم روز تا یک سال**[۲] یا جزای نقدی از **پانزده میلیون (۱۵.۰۰۰.۰۰۰) ریال تا یکصد میلیون (۱۰۰.۰۰۰.۰۰۰) ریال**[۳] 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.

ماده۷۴۵(ماده۱۷)ـ 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 **بیست میلیون (۲۰.۰۰۰.۰۰۰) ریال تا یکصد و پنجاه میلیون (۱۵۰.۰۰۰.۰۰۰) ریال**[۴] یا هر دو مجازات محکوم خواهدشد.

ماده۷۴۶(ماده۱۸)ـ 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 **بیست میلیون (۲۰.۰۰۰.۰۰۰) ریال تا یکصد و پنجاه میلیون (۱۵۰.۰۰۰.۰۰۰) ریال**[۵] یا هر دو مجازات محکوم خواهدشد.

---

[۱] همان

[۲] اصلاحی به موجب تبصره اصلاحی ماده ۱۰۴ قانون مجازات اسلامی که مقرر داشته است: «حداقل و حداکثر مجازات‌های حبس تعزیری درجه چهار تا درجه هشت مقرر در قانون برای جرائم قابل گذشت به نصف تقلیل می‌یابد»؛ مجازات قبلی: « نود و یک روز تا دو سال »

[۳] اصلاحی به موجب تصویبنامه ۱۳۹۹/۱۱/۸ هیات وزیران درخصوص «تعدیل میزان مبالغ مجازات نقدی جرایم و تخلفات مندرج در قوانین و مقررات مختلف» موضوع ابلاغیه شماره ۱۵۷۳۹۷۳/ت۵۷۷۵۲ه – ۱۳۹۹/۱۲/۲۵

[۴] همان

[۵] همان

فصل ششم ـ مسؤولیت کیفری اشخاص

ماده۷۴۷(ماده۱۹)ـ 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 [اشتباه تایپی صحیح آن شخص حقوقی است] فقط شخص حقیقی مسؤول خواهدبود.

ماده۷۴۸(ماده۲۰)ـ 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.

ماده۷۴۹(ماده۲۱)ـ 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 **شصت میلیون (۶۰.۰۰۰.۰۰۰) ریال تا دویست و پنجاه میلیون (۲۵۰.۰۰۰.۰۰۰) ریال**[1] و در مرتبهٔ دوم به جزای نقدی از یکصد میلیون (۱۰۰.۰۰۰.۰۰۰) ریال تا یک میلیارد (۱.۰۰۰.۰۰۰.۰۰۰) 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 سه‌گانهٔ مقننه، مجریه و قضائیه و مؤسسات عمومی غیردولتی موضوع قانون فهرست نهادها و مؤسسات عمومی

[1] همان

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.

ماده۷۵۰(ماده۲۲)ـ 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.

تبصره۱ـ 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.

ماده۷۵۱(ماده۲۳)ـ 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 **شصت میلیون (۶۰.۰۰۰.۰۰۰) ریال تا دویست و پنجاه میلیون (۲۵۰.۰۰۰.۰۰۰) ریال**[1] و در مرتبهٔ دوم به یکصد میلیون (۱۰۰.۰۰۰.۰۰۰) ریال تا یک میلیارد (۱.۰۰۰.۰۰۰.۰۰۰) 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.

---

[1] همان

ماده۷۵۲(ماده۲٤)ـ 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 (۱۰۰.۰۰۰.۰۰۰) ریال تا یک میلیارد (۱.۰۰۰.۰۰۰.۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد.

فصل هفتم ـ سایر جرائم

ماده۷۵۳(ماده۲۵)ـ هر شخصی که مرتکب اعمال زیر شود، به حبس از نود و یک روز تا یک سال یا جزای نقدی از **بیست میلیون (۲۰.۰۰۰.۰۰۰) ریال تا هشتاد میلیون (۸۰.۰۰۰.۰۰۰) ریال**[1] 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 ـ تشدید مجازاتها

ماده۷۵٤(ماده۲٦)ـ 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.

---

[1] همان

ماده۷۵۵(ماده۲۷)ـ 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.

مواد ۷۵٦ الی ۷۷۹ ـ نسخ شد.[1]

---

[1] به موجب ماده ٦٩٨ قانون آیین دادرسی جرائم نیروهای مسلح و دادرسی الکترونیکی مصوب ۱۳۹۳/۷/۸کمیسیون قضائی و حقوقی مجلس شورای اسلامی منتشره در روزنامه رسمی شماره ۲۰۲۹۷ مورخ ۱۳۹۳/۸/۲۰ نسخ شد.

متن مواد حذف شده به شرح ذیل است:

بخش دوم ـ آئین‌دادرسی

فصل یکم ـ صلاحیت

ماده۷۵٦(ماده۲۸)ـ 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.

ماده۷۵۷(ماده۲۹)ـ 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.

ماده۷۵۸(ماده۳۰)ـ 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.

ماده۷۵۹ (ماده۳۱)ـ در صورت بروز اختلاف در صلاحیت، حل اختلاف مطابق مقررات قانون آئین‌دادرسی دادگاه‌های عمومی و انقلاب در امور مدنی خواهدبود.

فصل دوم ـ جمع‌آوری ادله الکترونیکی

مبحث اول ـ نگهداری داده‌ها

ماده ۷۶۰(ماده۳۲)ـ 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.

ماده ۷۶۱(ماده۳۳)ـ 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

ماده۷۶۲(ماده۳٤)ـ 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 (۵.۰۰۰.۰۰۰) ریال تا ده‌میلیون (۱۰.۰۰۰.۰۰۰) 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

ماده۷۶۳(ماده۳۵)ـ مقام قضائی می‌تواند دستور ارائه داده‌های حفاظت‌شده مذکور در مواد (۷۶۰)، (۷۶۱) و (۷۶۲) فوق را به اشخاص یادشده بدهد تا در اختیار ضابطان قرارگیرد. مستنکف از اجراء این دستور به مجازات مقرر در ماده (۷۶۲) این قانون محکوم خواهد شد.

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

ماده۷۶٤(ماده۳٦)ـ 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.

ماده۷۶۵(ماده۳۷)ـ 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.

ماده۷٦٦(ماده۳۸)ـ 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.

ماده۷٦۷(ماده۳۹)ـ 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.

ماده۷٦۸ (ماده٤٠)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.

ماده۷٦۹ (ماده٤١)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،

ماده۷۷۰ (ماده٤٢)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.

ماده۷۷۱ (ماده٤٣)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.

ماده۷۷۲(ماده٤٤)ـ 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.

ماده۷۷۳(ماده٤٥)ـ 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.

ماده۷۷٤(ماده٤٦)ـ 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 مورد نظر و نقش آنها در جرم ارتکابی، در مهلت متناسب و متعارف نسبت به آنها تعیین تکلیف کند.

بخش سوم ـ سایر مقررات

ماده ۷۸۰ (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.

ماده ۷۸۱ (ماده۵۳)ـ 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.

ماده ۷۸۲ (ماده٥٤)ـ 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.

ماده ۷۸۳ (اصلاحی ۱۳۷۷/۲/۲۷) ـ کلیه قوانین مغایر با این قانون از جمله قانون مجازات عمومی مصوب سال ۱۳۰۴ و اصلاحات و الحاقات بعدی آن ملغی است .[1]

ماده ۷۷۵ (ماده٤٧)ـ 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

ماده ۷۷٦(ماده٤٨)ـ 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 ـ استناد پذیری ادله الکترونیکی

ماده ۷۷۷ (ماده٤٩)ـ 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.

ماده۷۷۸ (ماده۵۰)ـ 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.

ماده۷۷۹ (ماده۵۱)ـ 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.

[1] **از قانون کتاب پنجم قانون مجازات اسلامی (تعزیرات و مجازات‌های بازدارنده) مصوب ۱۳۷۵/۳/۲:**

ماده ۲۳۳ – این قانون به عنوان کتاب پنجم – تعزیرات و مجازات‌های بازدارنده به قانون مجازات اسلامی مصوب آذر ماه ۱۳۷۰ الحاق می‌گردد وشماره مواد ۱ تا ۲۳۳ آن به ۴۹۸ تا ۷۳۰ اصلاح می‌گردد.

قانون فوق مشتمل بر دویست و سی و سه ماده و چهل و چهار تبصره در جلسه روز چهارشنبه دوم خرداد ماه یک هزار و سیصد و هفتاد و پنج مجلس‌شورای اسلامی تصویب و در تاریخ ۱۳۷۵.۳.۶ به تأیید شورای نگهبان رسیده است.

از قانون جرایم رایانه ای مصوب ۱۳۸۸/۳/۵:

ماده ۵۵ ـ 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.

ماده ٥٦ ـ 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.

آیین دادرسی جرائم رایانه ای

مفاد بخش دهم قانون آیین دادرسی کیفری الحاقی ۱۳۹۳

ماده٦٦٤ـ علاوه بر موارد پیش‌بینی شده در دیگر قوانین، دادگاههای ایران صلاحیت رسیدگی به موارد زیر را دارند:

الف ـ داده‌های مجرمانه یا داده‌هایی که برای ارتکاب جرم به‌کار رفته‌اند که به هر نحو در سامانه‌های رایانه‌ای و مخابراتی یا حاملهای داده موجود در قلمرو حاکمیت زمینی، دریایی و هوایی جمهوری‌اسلامی‌ایران ذخیره شود.

ب ـ جرم از طریق تارنماهای دارای دامنه مرتبه‌بالای کد کشوری ایران (ir .) ارتکاب یابد.

پ ـ جرم توسط تبعه ایران یا غیرآن در خارج از ایران علیه سامانه‌های رایانه‌ای و مخابراتی و تارنماهای 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 دارای دامنه مرتبه بالای کد کشوری ایران در سطح گسترده ارتکاب یابد.

ت ـ جرائم رایانه‌ای متضمن سوءاستفاده از اشخاص کمتر از هجده سال، اعم از اینکه بزه دیده یا مرتکب ایرانی یا غیرایرانی باشد و مرتکب در ایران یافت شود.

ماده٦٦٥ـ چنانچه جرم رایانه‌ای درصلاحیت دادگاههای ایران در محلی کشف یا گزارش شود، ولی محل وقوع آن معلوم نباشد، دادسرای محل کشف مکلف است تحقیقات مقدماتی را انجام دهد. درصورتی‌که محل وقوع جرم مشخص نشود، دادسرا پس از اتمام تحقیقات مبادرت به صدور قرار و درصورت اقتضاء صدور کیفرخواست می‌کند و دادگاه مربوط نیز رأی مقتضی را صادر می‌کند. [1]

---

[1] **مرجع تصویب: هیئت عمومی دیوانعالی کشور سه‌شنبه،٢٤ اردیبهشت ۱۳۹۲ شماره ویژه نامه: ۵۷۱ سال شصت و نه شماره ۱۹۸٦۲**

رأی وحدت رویه شماره ۷۲۹ هیأت عمومی دیوانعالی کشور،درخصوص تعیین‌صلاحیت دادگاه صالح به رسیدگی در جرایم رایانه‌ای

شماره۱۱۰/۱۵۲/۷۸۲۷/۱ ۱۳۹۲/۲/۱۸

مدیرعامل محترم روزنامه رسمی کشور

گزارش وحدت رویه ردیف ۲۱/۹۱ هیأت عمومی دیوان عالی کشور با مقدمه مربوط و رأی آن به شرح ذیل تنظیم و جهت چاپ و نشر ایفاد می‌گردد.

معاون قضائی دیوان عالی کشور ـ ابراهیم ابراهیمی

الف: مقدمه

جلسه هیأت عمومی دیوان عالی کشور درمورد پرونده وحدت رویه ردیف ۲۱/۹۱ رأس ساعت ۹ روز سه‌شنبه مورخ ۱۳۹۱/۱۲/۱ به ریاست حضرت آیت‌الله احمد محسنی گرکانی رئیس دیوان عالی کشور و حضور حجۀ الاسلام والمسلمین جناب آقای محسنی اژیه دادستان کل کشور و شرکت رؤساء ، مستشاران و اعضاء معاون کلیه شعب دیوان عالی کشور، در سالن هیأت عمومی تشکیل و پس از تلاوت آیاتی از کلام‌الله مجید و قرائت گزارش پرونده و طرح و بررسی نظریات مختلف اعضای شرکت‌کننده درخصوص مورد و استماع نظریه دادستان کل کشور که به ترتیب ذیل منعکس می‌گردد، به صدور رأی وحدت رویه قضائی شماره ۷۲۹ ـ ۱۳۹۱/۱۲/۱ منتهی گردید.

ب: گزارش پرونده

احتراماً به عرض می‌رساند: براساس گزارش رسیده، برای رسیدگی به بزه کلاهبرداری الکترونیکی در مواردی که مبدأ انتقال وجه و مقصد آن در حوزه‌های قضایی مختلف بوده بین دادسراهای شهرستان‌های مربوطه اختلاف در صلاحیت حاصل‌شده و شعب دیوان عالی کشور در مقام حل اختلاف

ماده٦٦٦ـ قوه قضائیه موظف است به تناسب ضرورت، شعبه یا شعبی از دادسراها، دادگاههای کیفری یک، کیفری دو، اطفال و نوجوانان، نظامی و تجدیدنظر را برای رسیدگی به جرائم رایانه‌ای اختصاص دهد.

تبصره ـ مقامات قضائی دادسراها و دادگاههای مذکور از میان قضاتی که آشنایی لازم به امور رایانه دارند انتخاب می‌شوند.

ماده٦٦٧ـ ارائه دهندگان خدمات دسترسی موظفند داده‌های ترافیک را حداقل تا شش‌ماه پس از ایجاد حفظ نمایند و اطلاعات کاربران را حداقل تا شش‌ماه پس از خاتمه اشتراک نگهداری کنند.

تبصره ۱ـ 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.

و تعیین دادسرای صالح با استنباط از ماده ۵۴ قانون آیین دادرسی دادگاه‌های عمومی و انقلاب در امور کیفری آراء متهافت صادر کرده‌اند که خلاصه جریان آن ذیلاً بیان می‌گردد:

۱ـ شعبه یازدهم دیوان عالی کشور درموردی که بین دادسرای عمومی و انقلاب اصفهان «محل اقامت شاکی/مبدأ انتقال وجه» و دادسرای عمومی کرج «مقصد انتقال وجه» اختلاف در صلاحیت ایجاد گردیده، به موجب دادنامه شماره ۰۰۹۹۰ ـ ۱۳۹۱/۱۰/۱۰ با این استدلال که «محل کار و اقامت شاکی، محل برقرارشدن تماس تلفنی و فریب خوردن شاکی و همچنین محل انجام عملیات بانکی و انتقال وجه از حساب شاکی به حساب مورد نظر متهم، اصفهان بوده است...» صلاحیت دادسرای عمومی و انقلاب اصفهان را تأیید کرده است. شعبه سی و دوم دیوان عالی کشور نیز در این موارد عقیده به صلاحیت دادسرای مبدأ جرم داشته و با این استدلال که «جرم مورد ادعا به محض برداشت وجه از حساب شاکی در مبدأ تحقق یافته و حساب مقصد که وجه مذکور به آن واریز شده در صلاحیت تأثیری نخواهد گذاشت» صلاحیت آن دادسرا را مورد تأیید قرار داده است.

۲ـ شعبه هفدهم دیوان عالی کشور برعکس عقیده شعب یازدهم و سی و دوم اعتقاد به صلاحیت دادسرای مقصد انتقال وجه داشته و در مورد مشابه که بین دادسراهای عمومی و انقلاب اسفراین «مبدأ انتقال وجه» و تهران «مقصد انتقال وجه» اختلاف در صلاحیت حاصل‌شده طبق دادنامه شماره ۰۰۶۴۳ ـ ۱۳۹۱/۱۱/۳ به این استدلال که «مقدمات ارتکاب بزه عنوان شده و از جمله طراحی نقشه و عملیات اجرایی در حوزه قضایی تهران تدارک شده و نتیجه اقدامات مزبور نیز که بردن مال غیر به نحو متقلبانه بوده است در همین حوزه بدست آمده و امکان برداشت و تحصیل وجوه فراهم گردیده است...» با اعلام صلاحیت دادسرای عمومی و انقلاب تهران، حل اختلاف نموده است. همچنین شعبه ششم دیوان عالی کشور در این موارد به همین نحو حل اختلاف کرده است.

با توجه به مراتب فوق در اجرای ماده ۲۷۰ قانون آیین دادرسی دادگاه‌های عمومی و انقلاب در امور کیفری تقاضای طرح موضوع را در هیأت عمومی دیوان عالی کشور به منظور ایجاد وحدت رویه قضائی دارد.

معاون قضائی دیوان عالی کشور ـ حسینعلی نیّری

ج: نظریه دادستان کل کشور: تأیید رأی شعبه هفدهم دیوان عالی کشور

د: رأی وحدت رویه شماره ۷۲۹ ـ ۱۳۹۱/۱۲/۱ هیأت عمومی دیوان عالی کشور

نظر به اینکه در صلاحیت محلی، اصل صلاحیت دادگاه محل وقوع جرم است و این اصل در قانون جرایم رایانه‌ای نیز ـ مستفاد از ماده ۲۹ ـ مورد تأکید قانون‌گذار قرار گرفته، بنابراین در جرم کلاهبرداری مرتبط با رایانه هرگاه تمهید مقدمات و نتیجه حاصل از آن در حوزه‌های قضائی مختلف صورت گرفته باشد، دادگاهی که بانک افتتاح‌کننده حساب زیان‌دیده از بزه که پول به طور متقلبانه از آن برداشت شده در حوزه آن قرار دارد صالح به رسیدگی است. بنا به مراتب آراء شعب یازدهم و سی و دوم دیوان عالی کشور که براساس این نظر صادرشده به اکثریت آراء صحیح و قانونی تشخیص و تأیید می‌گردد. این رأی طبق ماده ۲۷۰ قانون آیین دادرسی دادگاه‌های عمومی و انقلاب در امور کیفری در موارد مشابه برای شعب دیوان عالی کشور و دادگاه‌ها لازم‌الاتباع است. هیأت عمومی دیوان عالی کشور

تبصره۲ـ اطلاعات کاربر، هرگونه اطلاعات راجع به کاربر خدمات دسترسی از قبیل نوع خدمات، امکانات فنی مورد استفاده و مدت زمان آن، هویت، نشانی جغرافیایی یا پستی یا قرارداد اینترنت (IP)، شماره تلفن و سایر مشخصات فردی را شامل می‌شود.

ماده٦٦٨ـ ارائه‌دهندگان خدمات میزبانی داخلی موظفند اطلاعات کاربران خود را حداقل تا شش‌ماه پس از خاتمه اشتراک و محتوای ذخیره شده و داده ترافیک حاصل از تغییرات ایجادشده را حداقل تا پانزده روز نگهداری کنند.

ماده٦٦٩ـ هرگاه حفظ داده‌های رایانه‌ای ذخیره‌شده برای تحقیق یا دادرسی لازم باشد، مقام‌قضائی می‌تواند دستور حفاظت از آنها را برای اشخاصی که به نحوی تحت تصرف یا کنترل دارند صادر کند. در شرایط فوری، نظیر خطر آسیب دیدن یا تغییر یا از بین رفتن داده‌ها، ضابطان قضائی می‌توانند دستور حفاظت را صادر کنند و مراتب را حداکثر تا بیست و چهار 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 نود و یک روز تا شش‌ماه یا جزای نقدی از **ده تا بیست میلیون ریال**[1] یا هردو مجازات محکوم می‌شوند.

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

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

ماده٦٧٠ـ مقام قضائی می‌تواند دستور ارائه داده‌های حفاظت شده مذکور در مواد (۶۶۷)، (۶۶۸) و (۶۶۹) این قانون را به اشخاص یاد شده بدهد تا در اختیار ضابطان قرار گیرد. خودداری از اجرای این دستور و همچنین عدم نگهداری وعدم مواظبت از این داده‌ها موجب مجازات مقرر در ماده (۶۶۹) این قانون می‌شود.

ماده٦٧١ـ 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 دارد.[2]

---

[1] اصلاحی به موجب تصویبنامه ۱۳۹۹/۱۱/۸ هیات وزیران درخصوص «تعدیل میزان مبالغ مجازات نقدی جرایم و تخلفات مندرج در قوانین و مقررات مختلف» موضوع ابلاغیه شماره ۱۵۷۳۹۷۳/ت۵۷۷۵۲ه – ۱۳۹۹/۱۲/۲۵

[2] اصل بیست و پنجم قانون اساسی: بازرسی و نرساندن نامه ها، ضبط و فاش کردن مکالمات تلفنی، افشای مخابرات تلگرافی و تلکس، سانسور، عدم مخابره و نرساندن آنها، استراق سمع و هر گونه تجسس ممنوع است مگر به حکم قانون.

ماده ۵۷۰ قانون مجازات اسلامی (اصلاحی ۱۳۸۱/۱۰/۱۱)- هر یک از مقامات ومامورین وابسته به نهادها و دستگاههای حکومتی که برخلاف قانون ، آزادی شخصی افراد ملت راسلب کند یا آنان رااز حقوق مقرر در قانون اساسی جمهوری اسلامی ایران محروم نماید علاوه بر انفصال از خدمت و محرومیت یک تاپنج سال از مشاغل حکومتی به حبس از دو ماه تا سه سال محکوم خواهدشد .

ماده ۵۸۰ قانون مجازات اسلامی- هر یک از مستخدمین وماموربن قضائی یا غیرقضائی یا کسی که خدمت دولتی به او ارجاع شده باشد بدون ترتیب قانونی به منزل کسی بدون اجازه و رضای صاحب منزل داخل شود به حبس از یک ماه تا یک سال محکوم خواهد شد مگر اینکه ثابت نماید به امر یکی از روسای خود که صلاحیت حکم را داشته است مکره به اطاعت امر او بوده ، اقدام کرده است که در این صورت مجازات مزبور در حق آمر اجراء خواهد شد و اگر مرتکب یا سبب وقوع جرم دیگری نیز باشد مجازات آن را نیز خواهد دید و چنانچه این عمل در شب واقع شود مرتکب یا آمر به حداکثر مجازات مقرر محکوم خواهدشد .

ماده۶۷۲ـ 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 می‌شود. درصورت عدم حضور یا امتناع از حضور آنان چنانچه تفتیش یا توقیف ضرورت داشته باشدیا فوریت امر اقتضاء کند، قاضی با ذکر دلایل دستور تفتیش و توقیف بدون حضور اشخاص مذکور را صادر می‌کند.

ماده۶۷۳ـ دستور تفتیش و توقیف باید شامل اطلاعاتی از جمله اجرای 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 نرم افزارها، نحوه دستیابی به داده‌های رمزنگاری یا حذف شده و زمان تقریبی انجام تفتیش و توقیف باشد که به اجرای صحیح آن کمک می‌کند.

ماده۶۷۴ـ تفتیش داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی شامل اقدامات ذیل می‌شود:

الف ـ دسترسی به تمام یا بخشی از سامانه‌های رایانه‌ای یا مخابراتی

ب ـ دسترسی به حاملهای داده از قبیل دیسکت ها یا لوحهای فشرده یا کارتهای حافظه

پ ـ دستیابی به داده‌های حذف یا رمزنگاری شده

ماده۶۷۵ـ در توقیف داده‌ها، با رعایت تناسب، نوع، اهمیت و نقش آنها در ارتکاب جرم، به روشهایی از قبیل چاپ داده‌ها، تصویربرداری از تمام یا بخشی از داده‌ها، غیرقابل دسترس کردن داده‌ها با روشهایی از قبیل تغییرگذرواژه یا رمزنگاری و ضبط حاملهای داده عمل می‌شود.

ماده۶۷۶ـ در شرایط زیر سامانه‌های رایانه‌ای یا مخابراتی توقیف می‌شوند:

الف ـ داده‌های ذخیره شده به سهولت در دسترس نباشد یا حجم زیادی داشته باشد.

ب ـ تفتیش و تجزیه و تحلیل داده‌ها بدون سامانه سخت افزاری امکان پذیر نباشد.

پ ـ متصرف قانونی سامانه رضایت داده باشد.

ت ـ تصویربرداری از داده‌ها به لحاظ فنی امکان پذیر نباشد.

ث ـ تفتیش در محل باعث آسیب داده‌ها شود.

ماده۶۷۷ـ توقیف سامانه‌های رایانه‌ای یا مخابراتی متناسب با نوع و اهمیت و نقش آنها در ارتکاب جرم با روشهایی از قبیل تغییر گذرواژه به منظور عدم دسترسی به سامانه، مهر و موم (پلمب) سامانه در محل استقرار و ضبط سامانه صورت می‌گیرد.

ماده۶۷۸ـ چنانچه در حین اجرای دستور تفتیش و توقیف، تفتیش داده‌های مرتبط با جرم ارتکابی در سایر سامانه‌های رایانه‌ای یا مخابراتی که تحت کنترل یا تصرف متهم قرار دارند ضروری باشد، ضابطان با دستور مقام قضائی دامنه تفتیش و توقیف را به‌سامانه‌های دیگر گسترش می‌دهند و داده‌های مورد نظر را تفتیش یا توقیف می‌کنند.

ماده۶۷۹ـ توقیف داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی که موجب ایراد لطمه جانی یا خسارات مالی شدید به اشخاص یا اخلال در ارائه خدمات عمومی شود، ممنوع است مگر اینکه توقیف برای اجرای موضوع اهم نظیر حفظ امنیت کشور ضرورت داشته باشد.

ماده ۶۸۰ـ در جایی که اصل داده‌ها توقیف می‌شود، ذی نفع حق دارد پس از پرداخت هزینه از آنها کپی دریافت کند، مشروط به اینکه ارائه داده‌های توقیف‌شده منافی با ضرورت کشف حقیقت نباشد و به روند تحقیقات لطمه‌ای وارد نسازد و داده‌ها مجرمانه نباشد.

ماده ۶۸۱ـ 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 نرم افزارهای مورد نظر و نقش آنها درجرم ارتکابی، در مهلت متناسب و متعارف برای آنها تعیین تکلیف کند.

ماده ۶۸۲ـ متضرر می‌تواند در مورد عملیات و اقدامات مأموران در توقیف داده‌ها و سامانه‌های رایانه‌ای و مخابراتی، اعتراض کتبی خود را همراه با دلایل ظرف ده روز به مرجع قضائی دستوردهنده تسلیم نماید. به درخواست یادشده خارج از نوبت رسیدگی می‌شود و قرار صادره قابل اعتراض است.

ماده ۶۸۳ـ کنترل محتوای در حال انتقال ارتباطات غیرعمومی در سامانه‌های رایانه‌ای یا مخابراتی مطابق مقررات راجع به کنترل ارتباطات مخابراتی مقرر در آیین دادرسی کیفری است.

تبصره ـ دسترسی به محتوای ارتباطات غیرعمومی ذخیره شده، نظیر پیام‌نگار (ایمیل) یا پیامک در حکم کنترل و مستلزم رعایت مقررات مربوط است.

ماده ۶۸۴ـ آیین‌نامه اجرائی نحوه نگهداری و مراقبت از ادله الکترونیکی جمع‌آوری‌شده ظرف شش‌ماه از تاریخ لازم‌الاجراء شدن این قانون توسط وزیر دادگستری با همکاری وزارت ارتباطات و فناوری اطلاعات تهیه می‌شود و به تصویب رئیس قوه قضائیه می‌رسد.

ماده ۶۸۵ـ چنانچه داده‌های رایانه‌ای توسط طرف دعوی یا شخص ثالثی که از دعوی آگاهی ندارد، ایجاد یا پردازش یا ذخیره یا منتقل شود و سامانه رایانه‌ای یا مخابراتی مربوط به نحوی درست عمل کند که به صحت و تمامیت، اعتبار و انکارناپذیری داده‌ها خدشه وارد نشود، قابل استناد است.

ماده ۶۸۶ـ کلیه مقررات مندرج در این بخش، علاوه بر جرائم رایانه‌ای شامل سایر جرائمی که ادله الکترونیکی در آنها مورد استناد قرار می‌گیرند نیز می‌شود.

ماده ۶۸۷ـ در مواردی که در این بخش برای رسیدگی به جرائم رایانه‌ای مقررات خاصی از جهت آیین‌دادرسی پیش‌بینی نشده است، تابع مقررات‌عمومی آیین دادرسی کیفری است.

آیین‌نامه جمع‌آوری و استنادپذیری ادله الکترونیکی

مصوب ۱۳۹۳/۵/۱۲

منتشره در روزنامه رسمی شماره ۲۰۲۱۸-۱۳۹۳/۵/۱۵

در اجرای ماده ۵۴ قانون جرایم رایانه‌ای مصوب ۵ /۳ /۱۳۸۸ مجلس شورای اسلامی[1] و بـنا به پیشنهاد وزیر دادگستری، آیین‌نامه جمع‌آوری و استنادپذیری ادله الکترونیکی به شرح مواد آتی است:

فصل اول: تعاریف

ماده۱ـ واژه‌ها و اصطلاحات بکار برده شده در این آیین‌نامه در معانی زیر بکار می‌رود:

الف ـ ارائه‌دهندگان خدمات دسترسی: اشخاصی هستند که امکان ارتباط کاربران را با شبکه‌های رایانه‌ای یا مخابراتی و ارتباطی داخلی یا بین‌المللی یا هر شبکه مستقل دیگر فراهم می‌آورند از قبیل تأمین‌کنندگان، توزیع‌کنندگان، عرضه‌کنندگان خدمات دسترسی به شبکه‌های رایانه‌ای یا مخابراتی.

ب ـ ارائه‌دهندگان خدمات میزبانی: اشخاصی هستند که امکان دسترسی کاربران به فضای ایجادشده توسط سامانه‌های رایانه‌ای، مخابراتی و ارتباطی تحت تصرف یا کنترل خود را به کاربران واگذار می‌کنند تا رأساً یا توسط کاربر متقاضی، داده‌های رایانه‌ای را جهت نگهداری، انتشار، توزیع یا ارائه در شبکه‌های داخلی یا بین‌المللی یا هر منظور دیگر ذخیره یا پردازش کنند.

ج ـ ارائه داده‌های الکترونیکی: عبارت است از در اختیار قرار دادن تمام یا بخشی از داده‌های حفظ یا نگهداری‌شده توسط ارائه‌دهندگان خدمات دسترسی یا میزبانی یا اشخاصی که داده‌ها را تحت تصرف یا کنترل دارند.

د ـ جمع‌آوری ادله الکترونیکی: فرآیندی است که طی آن ادله الکترونیکی به تنهایی یا به همراه سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده، نگهداری، حفظ فوری، تفتیش و توقیف و شنود می‌شوند.

هـ ـ زنجیره حفاظتی: مجموعه اقداماتی است که ضابط دادگستری و سایر اشخاص ذیصلاح به منظور حفظ صحت، تمامیت، اعتبار و انکارناپذیری ادله الکترونیکی با بکارگیری ابزارها و روشهای استاندارد در مراحل شناسایی، کشف، جمع‌آوری، مستندسازی، تجزیه و تحلیل و ارائه آنها به مرجع مربوط به اجراء درآورده و ثبت می‌کنند؛ به نحوی که امکان ردیابی آنها از مبدأ تا مقصد وجود داشته باشد.

و ـ شنود: عبارت است از هر گونه دستیابی به محتوای در حال انتقال ارتباطات غیرعمومی در سامانه‌های رایانه‌ای یا مخابراتی یا امواج الکترومغناطیسی با استفاده از سامانه‌ها و تجهیزات سخت‌افزاری و نرم‌افزاری مربوط.

زـ مجری حفاظت: شخصی است که به نحوی داده‌های رایانه‌ای ذخیره شده را تحت تصرف یا کنترل دارد و مطابق ماده ۳۴ قانون[1] و سایر قوانین و مقررات جهت حفاظت آنها تعیین می‌شود.

---

[1] ماده ۷۸۲ کتاب تعزیرات قانون مجازات اسلامی

ح ـ متصرف قانونی: در مورد اشخاص حقیقی، شخص مالک یا شخصی است که به نحوی داده یا سامانه را به صورت مشروع در اختیار دارد یا نماینده یا ولی یا سرپرست قانونی وی. در مورد اشخاص حقوقی دولتی یا عمومی غیردولتی، بالاترین مقام آنها یا نماینده قانونی آنها طبق مقررات مربوط و در مورد سایر اشخاص حقوقی، مدیر یا نماینده قانونی آنهاست.

ط ـ قانون: منظور از قانون در این آیین‌نامه، قانون جرایم رایانه‌ای مصوب ۵ /۳ /۱۳۸۸ می‌باشد.

تبصره ـ سایر اصطلاحات به شرح تعریف ارائه شده در قوانین دیگر می‌باشد.

فصل دوم: جمع‌آوری ادله الکترونیکی

الف: نگهداری داده‌ها

ماده۲ـ ارائه‌دهندگان خدمات دسترسی و میزبانی موظفند از سامانه‌هایی استفاده نمایند که قابلیت نگهداری داده‌های ترافیک و اطلاعات کاربران را مطابق مواد ۳۲ و ۳۳ قانون[۲] داشته باشد.

ماده۳ـ ارائه‌دهندگان خدمات دسترسی موظفند سامانه‌های خود را به نحوی تنظیم کنند که کلیه ارتباطات رایانه‌ای را که از طریق آنها انجام می‌شود ثبت کنند و کلیه داده‌های ترافیک مربوط به خود و کاربران مربوط را تا شش ماه پس از ایجاد نگهداری کنند.

تبصره ـ عرضه کنندگان خدمات دسترسی حضوری اینترنت (کافی‌نت‌ها)موظفند مشخصات هویتی، آدرس، ساعت شروع و خاتمه کار کاربر و نشانی اینترنتی (IP) تخصیصی را در دفتر روزانه ثبت نمایند.

ماده۴ـ ارائه‌دهندگان خدمت دسترسی موظفند اطلاعات کاربران را حداقل ۶ ماه پس از خاتمه اشتراک یا لغو قرارداد کاربر نگهداری کنند. هویت و نشانی کاربر باید در قرارداد منعقده درج شود.

ماده۵ ـ ارائه دهندگان خدمات میزبانی داخلی و نمایندگان داخلی ارائه‌دهندگان خدمات میزبانی خارجی 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. برگه اشتراک باید به نحوی تنظیم شود که هویت و نشانی آنان مشخص باشد.

تبصره۱ـ ارائه‌دهندگان خدمات میزبانی موظفند سامانه‌های رایانه‌ای خود را به نحوی تنظیم کنند که هرگونه تغییر اعم از اصلاح یا حذف محتوا و داده ترافیک حاصل از آن را ذخیره نماید.

تبصره۲ـ اشخاصی که نسبت به انباشت یا ذخیره موقت اطلاعات در راستای ارائه خدمات دسترسی اقدام می‌کنند، ارائه‌دهنده خدمات میزبانی محسوب نمی‌شوند.

---

[۱] ماده ۷۶۲ کتاب تعزیرات قانون مجازات اسلامی که به موجب ماده ۶۹۸ قانون آیین دادرسی کیفری مصوب ۱۳۹۲ نسخ شده است و در حال حاضر ماده ۶۶۹ آن قانون جایگزین آن شده است.

[۲] مواد ۷۶۰ و ۷۶۱ کتاب تعزیرات قانون مجازات اسلامی که به موجب ماده ۶۹۸ قانون آیین دادرسی کیفری مصوب ۱۳۹۲ نسخ شده است و در حال حاضر مواد ۶۶۷ و ۶۶۸ آن قانون جایگزین آن شده است.

ماده۶ ـ ارائه‌دهندگان خدمات دسترسی و میزبانی و مجریان حفاظت موظفند امنیت داده‌های ترافیکی و محتوای نگهداری و حفاظت شده را مطابق با ضوابط و دستورالعمل‌هایی که به تصویب رئیس قوه قضائیه می‌رسد، تأمین نمایند.

ماده۷ـ داده‌های محتوا و ترافیک و اطلاعات کاربران باید مطابق مقررات این آیین‌نامه به نحوی نگهداری، حفاظت، توقیف و ارائه شود که صحت و تمامیت، محرمانگی، اعتبار و انکارناپذیری آنها محفوظ بماند.

ماده۸ ـ در مواردی که برابر قانون نگهداری و حفاظت داده‌ها الزامی است، نگهداری و حفاظت باید به گونه‌ای انجام شود که مدیریت جستجو و گزارش‌دهی آنها امکان‌پذیر باشد.

ماده۹ـ وزارت ارتباطات و فن‌آوری اطلاعات هماهنگی‌های لازم برای تنظیم زمان سامانه‌های جمع‌آوری داده‌های محتوا، ترافیک و اطلاعات کاربران را مطابق با ساعت رسمی کشور به عمل می‌آورد.

ماده۱۰ـ مرکز آمار و فناوری اطلاعات با همکاری وزارت ارتباطات و فناوری اطلاعات سالانه رویه‌های فنی نحوه نگهداری، حفاظت، توقیف و ارائه داده‌ها و اطلاعات کاربران و همچنین راهنماهای عملی حفظ امنیت و استنادپذیری داده‌ها را تصویب و به ارائه‌دهندگان خدمات دسترسی و میزبانی و بهره‌برداران ابلاغ می‌نماید.

ب: حفاظت از ادله رایانه‌ای

ماده۱۱ـ مقام قضایی در جریان تحقیق و فرآیند رسیدگی می‌تواند دستور حفاظت هر نوع داده رایانه‌ای ذخیره شده را از جمله داده‌های رمزنگاری شده، حذف، پنهان، فشرده یا پنهان نگاری شده و یا داده‌هایی که نوع و نام آنها موقتاً تغییر یافته و یا داده‌هایی که برای بررسی آنها نیاز به سخت‌افزار مخصوصی می‌باشد، صادر نماید.

تبصره۱ـ ضابطان قضایی فقط در موارد مندرج در ماده ۳۴ قانون[1] می‌توانند رأساً دستور حفاظت داده‌های ذخیره شده را صادر کنند.

تبصره۲ـ قاضی مکلف است بلافاصله پس از اعلام ضابط قضایی نسبت به تأیید یا رد دستور حفاظت صادره توسط ضابط اظهارنظر نماید. مجری حفاظت تا تعیین تکلیف از ناحیه قاضی موظف به حفاظت از اطلاعات می‌باشد.

ماده۱۲ـ دستور حفاظت باید به طور صریح و دقیق مشتمل بر نوع داده‌ها، موضوع و مدت زمان با رعایت تبصره۲ ماده ۳۴ قانون،[2] باشد.

ماده۱۳ـ در موارد مقتضی، اجرای دستور حفاظت با نظارت ضابطان قضایی متخصص یا اشخاص خبره مورد وثوق به نمایندگی از طرف مرجع قضایی انجام می‌شود.

---

[1] ماده ۷۶۲ کتاب تعزیرات قانون مجازات اسلامی که به موجب ماده ۶۹۸ قانون آیین دادرسی کیفری مصوب ۱۳۹۲ نسخ شده است و در حال حاضر ماده ۶۶۹ آن قانون جایگزین آن شده است.

[2] ماده ۷۶۲ کتاب تعزیرات قانون مجازات اسلامی که به موجب ماده ۶۹۸ قانون آیین دادرسی کیفری مصوب ۱۳۹۲ نسخ شده است و در حال حاضر ماده ۶۶۹ آن قانون جایگزین آن شده است.

ماده۱۴ـ مجری حفاظت موظف است بلافاصله پس از ابلاغ، دستور حفاظت را اجراء و صورت‌جلسه‌ای را مشتمل بر زمان اجرای دستور، نحوه حفاظت، حجم و نوع داده‌های حفاظت‌شده در دو نسخه تنظیم و یک نسخه از آن را به مرجع صادرکننده دستور ارسال کند و نسخه دیگر را نزد خود نگه دارد.

ماده۱۵ـ دستور حفاظت باید فوری و با روش مطمئن به مجری حفاظت ابلاغ شود. این دستور همچنین به اشخاص ذینفع نیز ابلاغ می‌شود؛ مگر آن که ابلاغ به آنها مخلّ رسیدگی باشد که در این صورت تشخیص زمان ابلاغ حسب مورد با مقام قضایی می‌باشد.

تبصره ـ روش مطمئن روشی است که با توجه به نوع داده‌ها و طول مدت زمان حفاظت، امکان بهره‌برداری از داده‌های حفاظت شده را در مراحل بعدی دادرسی ممکن سازد.

ماده۱۶ـ حفاظت از داده‌ها باید به نحوی باشد که محرمانگی، تمامیت، صحت و انکارناپذیری داده‌ها رعایت شود.

ج: ارائه ادله رایانه‌ای

ماده۱۷ـ دستور ارائه توسط مقام قضایی صادر می‌شود و باید به طور صریح و شفاف و مشتمل بر شخص ارائه‌دهنده، موضوع و نوع داده‌ها، شیوه و زمان تحویل داده‌ها و مرجع تحویل‌گیرنده باشد.

ماده۱۸ـ ارائه داده‌ها باید به نحوی باشد که محرمانگی، تمامیت، صحت و انکارناپذیری داده‌ها رعایت شده و حتی‌الامکان بدون ایجاد مانع برای فعالیت سامانه و با روش متعارف و کم هزینه به یکی از شیوه‌های ذیل باشد:

الف ـ تحویل یک نسخه چاپ شده از داده.

ب ـ تحویل یک نسخه رایانه‌ای از داده.

ج ـ ایجاد دسترسی به داده.

د ـ انتقال تجهیزات رایانه‌ای و مخابراتی.

ماده۱۹ـ هنگام ارائه داده‌ها صورت‌جلسه‌ای در سه نسخه تنظیم و حداقل موارد ذیل در آن ذکر و به امضای ارائه دهنده و تحویل گیرنده می‌رسد:

الف ـ شماره و تاریخ دستور قضایی ارائه داده‌ها

ب ـ مشخصات ارائه دهنده

ج ـ مشخصات تحویل گیرنده

د ـ زمان و مکان ارائه

هـ ـ نوع و حجم داده‌ها

وـ اطلاعات مربوط به نحوه حفظ یا نگهداری داده‌ها

ز ـ روشهای امنیتی بکاررفته در زمان ارائه

ح ـ مشخصات سخت‌افزاری و نرم‌افزاری تجهیزات

ط ـ شیوه ارائه و مشخصات داده.

تبصره۱ـ در هنگام انتقال تجهیزات، احتیاط لازم برای حفظ آنها بعمل می‌آید.

تبصره۲ـ یک نسخه از صورت‌جلسه به مرجع قضایی ارسال می‌شود و نسخه‌ای در اختیار ارائه دهنده و نسخه دیگر در اختیار تحویل گیرنده قرار می‌گیرد.

ماده۲۰ـ از زمان ارائه داده‌ها به ضابطان قضایی یا دیگر اشخاص ذیربط، مسئولیت حفظ داده‌های مذکور با شخص یا اشخاص تحویل گیرنده خواهد بود.

ماده۲۱ـ ارائه داده‌هایی که افشاء یا دسترسی به آنها مطابق قوانین خاص دارای محدودیت یا توأم با تشریفات می‌باشد، تابع مقررات مربوط است.

ماده۲۲ـ دستور ارائه داده، مجوز افشای آن نمی‌باشد و پس از دستور ارائه هرگونه دسترسی به مفاد داده مستلزم صدور دستور قضایی است.

ماده۲۳ـ اشخاصی که مسئول اجرای هریک از دستورات قضایی اعم از نگهداری، حفاظت، ارائه، تفتیش و توقیف سامانه و داده یا شنود آن می‌باشند یا دستور به آنها ابلاغ می‌شود یا به نوعی مرتبط با دستورات یاد شده هستند، حق افشای مفاد دستور و یا داده‌ها و اطلاعات مربوط را ندارند.

د: تفتیش و توقیف ادله رایانه‌ای

ماده۲۴ـ ضابطان قضایی باید کلیه اطلاعاتی که ضرورت تفتیش و توقیف را ایجاب می‌نماید در درخواست خود اعلام نمایند. همچنین، موارد زیر را حسب مورد در درخواست تفتیش یا توقیف ذکر نمایند:

الف ـ دلایل ضرورت تفتیش و توقیف

ب ـ حتی‌الامکان نوع و میزان داده‌ها و سخت‌افزارها

ج ـ محل تفتیش یا توقیف

د ـ دلایل لازم برای تصویربرداری و بررسی در خارج از محل

هـ ـ زمان تقریبی لازم برای تفتیش و توقیف.

ماده۲۵ـ در دستور تفتیش یا توقیف داده یا سامانه باید محل تفتیش یا توقیف تعیین و حتی‌الامکان در محل استقرار سامانه انجام پذیرد.

ماده۲۶ـ مدت توقیف و فرصت اجرای تفتیش باید در دستور قضایی تصریح و کمترین فرصت ممکن منظور شود. در صورت نیاز به زمان بیشتر، به درخواست مجری تفتیش یا توقیف و ذکر علت آن، این مدت قابل تمدید می‌باشد.

ماده۲۷ـ تفتیش و توقیف در مواردی که مستلزم ورود به منازل و اماکن خصوصی باشد، مطابق مقررات مندرج در آیین دادرسی کیفری خواهد بود.

ماده۲۸ـ در مواردی که تفتیش یا توقیف طبق دستور قضایی بدون حضور متصرف قانونی یا شخصی که داده یا سامانه را تحت اختیار دارد، انجام پذیرد، مراتب پس از انجام فوراً به ذینفع ابلاغ خواهد شد.

ماده۲۹ـ چنانچه پس از اجرای دستور توقیف و یا در زمان اجرای دستور توقیف داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی بیم لطمه جانی یا خسارت مالی شدید به اشخاص یا اخلال در ارائه خدمات عمومی برود مراتب از مرجع قضایی صادرکننده دستور توقیف کسب تکلیف شده و در صورت تشخیص قاضی حسب مفاد ماده ۴۴ قانون[۱] عمل می‌گردد.

ماده۳۰ـ قوه قضاییه تمهیدات لازم از جمله بسترسازی و ایجاد زیرساختهای ارتباط رایانه‌ای و الکترونیکی و همچنین راه‌اندازی سامانه‌ها و درگاههای مبتنی بر فناوری اطلاعات را جهت تسهیل در عملیاتی کردن فرایندها و روشهای موضوع این آیین‌نامه فراهم می‌آورد.

ماده۳۱ـ اشخاصی که داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی را تحت کنترل و یا تصرف دارند، موظف به همکاری در اجرای دستور تفتیش و توقیف می‌باشند. در صورتی که به واسطه عدم همکاری یا عدم دسترسی به این اشخاص، تفتیش یا توقیف امکان‌پذیر نباشد، نحوه دسترسی به داده‌ها یا سامانه‌ها از قبیل ورود به محل، رفع موانع استفاده از سخت‌افزار و نرم‌افزار، رمزگشایی و امثال آن با دستور مقام قضایی تعیین خواهد شد.

ماده۳۲ـ رضایت متصرف قانونی سامانه موضوع بند ج ماده ۴۱ قانون،[۲] باید کتبی و با امضای وی باشد.

ماده۳۳ـ در مواردی که توقیف داده‌ها به روش چاپ یا کپی یا تصویربرداری داده‌ها انجام می‌شود، اصل داده‌ها در صورتی توقیف و غیرقابل دسترس می‌شود که در دستور قضایی تصریح شده باشد.

ماده۳۴ـ ضابطان صرفاً مجاز به تفتیش و توقیف داده‌ها و سامانه‌هایی هستند که به طور صریح در دستور قضایی ذکر گردیده و چنانچه حین اجرای دستور، داده‌های مرتبط با جرم ارتکابی در سایر سامانه‌های رایانه‌ای یا مخابراتی تحت کنترل یا تصرف متهم کشف شود، در صورت بیم امحاء نسبت به حفظ فوری داده‌ها اقدام و مراتب را حداکثر ظرف ۲۴ ساعت کتباً به مقام قضایی مربوط گزارش می‌دهند.

ماده۳۵ـ تفتیش داده‌ها یا سامانه‌ها در محل استقرار یا از طریق شبکه یا در آزمایشگاه یا در محل مناسب با دستور و تشخیص مقام قضایی با رعایت صحت، تمامیت، محرمانگی، و انکارناپذیری ادله انجام می‌پذیرد.

ماده۳۶ـ ضابطان و اشخاصی که حسب قانون مأمور جمع‌آوری، تفتیش، نگهداری، حفظ و انتقال داده‌ها و سامانه‌های رایانه‌ای یا مخابراتی می‌شوند باید علاوه بر داشتن شرایط لازم از قبیل تخصص و توانایی فنی و آموزش کافی، تجهیزات و وسایل لازم را در اختیار داشته باشند.

ماده۳۷ـ هنگام تفتیش رعایت موارد زیر ضروری است:

الف ـ شیوه اقدام نباید موجب تغییر، امحاء یا جابجایی داده‌های موردنظر در سامانه‌های رایانه‌ای باشد.

---

[۱] ماده ۷۷۲ کتاب تعزیرات قانون مجازات اسلامی که به موجب ماده ۶۹۸ قانون آیین دادرسی کیفری مصوب ۱۳۹۲ نسخ شده است و در حال حاضر ماده ۶۷۹ آن قانون جایگزین آن شده است.

[۲] ماده ۷۶۹ کتاب تعزیرات قانون مجازات اسلامی که به موجب ماده ۶۹۸ قانون آیین دادرسی کیفری مصوب ۱۳۹۲ نسخ شده است و در حال حاضر بند «پ» ماده ۶۷۶ آن قانون جایگزین آن شده است.

ب ـ تفتیش صرفاً در محدوده دستور قضایی و داده‌های مرتبط با جرم موضوع دستور، انجام می‌پذیرد.

ج ـ کلیه فرایندهای انجام شده بر روی داده‌های مورد تفتیش یا توقیف باید با استفاده از روش‌های قابل تشخیص، ثبت و محافظت شود.

ماده۳۸ـ توقیف با رعایت تناسب، نوع، اهمیت و نقش داده یا سامانه رایانه‌ای یا مخابراتی به روش‌های زیر انجام می‌شود:

الف ـ در توقیف داده‌ها از طریق چاپ داده‌ها، غیرقابل دسترس کردن داده‌ها به روش‌هایی از قبیل تغییر گذر واژه یا رمزنگاری و ضبط حامل‌های داده.

ب ـ در توقیف سامانه‌های رایانه‌ای یا مخابراتی از طریق تغییر گذرواژه، پلمپ سامانه در محل استقرار یا ضبط سامانه.

تبصره ـ توقیف باید حتی‌الامکان بدون ایجاد مانع برای فعالیت سامانه و به روش ساده و کم هزینه به شیوه‌هایی از قبیل ذخیره در حامل‌های داده، ذخیره در سامانه با گذاشتن گذرواژه، تهیه نسخه پشتیبان، تصویربرداری، تهیه رونوشت و چاپ انجام شود.

ماده۳۹ـ دستور توقیف سامانه شامل سایر سخت‌افزارها یا حامل‌های داده متصل به آن نمی‌شود، مگر آن که در دستور قضایی تصریح گردد. در صورت نیاز به حفظ فوری سخت‌افزارها یا حامل‌های داده، ضابطان یا سایر مأموران در حدود وظایف قانونی می‌توانند نسبت به حفظ فوری آن مطابق ماده ۳۴ قانون[1] و رعایت مقررات این آیین‌نامه اقدام نمایند.

ماده۴۰ـ در صورت پلمپ سامانه چنانچه نیاز به گماردن حافظ باشد با دستور مقام قضایی اقدام می‌شود.

ماده۴۱ـ به منظور حفظ وضعیت اصلی ادله رایانه‌ای و جلوگیری از هرگونه تغییر، تحریف یا آسیب آن، مرجع قضایی مدت زمان نگهداری و مراقبت از آنها را تا مدت ۵ روز تعیین می‌کند.

تبصره ـ چنانچه برای نگهداری و مراقبت مدت بیشتری مورد نیاز باشد، مدت مذکور به صورت مستدل توسط مقام قضایی تمدید می‌شود.

ماده۴۲ـ اجرای دستور توقیف باید طی صورت‌جلسه‌ای با قید دقیق جزئیات و مشخصات داده یا سامانه، محل، تاریخ و زمان دقیق، مشخصات حاضران و مجری دستور، مشخصات حافظ در صورت وجود، شماره و تاریخ دستور قضایی مبنی بر توقیف، شیوه توقیف و مشخصات مالک یا متصرف داده یا سامانه و موارد ضروری دیگر تنظیم و ضمن اعلام به مقام قضایی رسیدگی‌کننده، در سابقه ضبط گردد.

ماده۴۳ـ ضابطان قضایی و سایر مأموران در حدود وظایف قانونی در شروع تفتیش و توقیف باید صورت وضعیت اولیه‌ای از سامانه رایانه‌ای یا مخابراتی و اجزای آن و کلیه اتصالات کابلی بین اجزای مختلف سخت‌افزارها و حامل‌های داده متصل به آن که علامت‌گذاری و ثبت می‌شوند را تنظیم و به امضای

---

[1] ماده ۷۶۲ کتاب تعزیرات قانون مجازات اسلامی که به موجب ماده ۶۹۸ قانون آیین دادرسی کیفری مصوب ۱۳۹۲ نسخ شده است و در حال حاضر ماده ۶۶۹ آن قانون جایگزین آن شده است.

تفتیش‌کننده یا توقیف‌کننده و متصرف قانونی که سامانه تحت کنترل اوست یا قائم‌مقام قانونی وی برسانند. برای ضبط دقیق مشخصات ابزار و اجزای آن تصویربرداری بلامانع است.

ماده۴۴ـ مرجع قضایی صالح، ضمن صدور رأی باید نسبت به داده یا سامانه توقیف شده تعیین تکلیف نماید.

فصل سوم: امور متفرقه

ماده۴۵ـ دستورالعمل حقوقی و فنی جمع‌آوری ادله و توقیف سامانه‌های رایانه‌ای و مخابراتی توسط دادستانی کل کشور با همکاری نیروی انتظامی تهیه و به تصویب دادستان کل کشور می‌رسد. این دستورالعمل باید دربردارنده چگونگی حفظ صحنه جرم و جمع‌آوری ادله از سامانه در حال اجراء ، خاموش و روشن کردن سامانه، بسته‌بندی و انتقال اطلاعات و نیز نمونه درخواست‌های مرتبط با این موارد باشد.

ماده۴۶ـ در مورد جمع‌آوری ادله الکترونیکی از جمله نگهداری، حفظ فوری، تفتیش و توقیف و شنود چنانچه موضوع مربوط به افراد و اماکن وابسته به قوه قضائیه و سازمان‌های تابعه مراکز مرتبط با قوه قضاییه باشد، با دستور مقام قضایی توسط مرکز حفاظت و اطلاعات قوه قضاییه انجام خواهد شد.

ماده۴۷ـ نسخه‌های تهیه شده از داده‌های رایانه‌ای قابل استناد به صورت متن، صوت یا تصویر در حکم اصل داده می‌باشند.

ماده۴۸ـ این آیین‌نامه توسط وزارت دادگستری با همکاری وزارت ارتباطات و فناوری اطلاعات تهیه و در ۴۸ ماده و ۱۱ تبصره در تاریخ ۱۲ /۵ /۱۳۹۳ به تصویب رئیس قوه قضائیه رسید.

رئیس قوه قضائیه ـ صادق آملی لاریجانی