از **قانون آیین دادرسی جرائم نیروهای مسلح و دادرسی الکترونیکی مصوب ۸/۷/۱۳۹۳ کمیسیون قضائی و حقوقی مجلس شورای اسلامی**

بخش دهم ـ آیین دادرسی جرائم رایانه‌ای

ماده۶۶۴ـ 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 رایانه ای 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.

ماده۶۶۵ـ چنانچه جرم رایانه ای 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 می کند و دادگاه مربوط نیز رأی مقتضی را صادر می‌کند.

ماده۶۶۶ـ 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 رایانه ای اختصاص دهد.

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

ماده۶۶۷ـ ارائه دهندگان خدمات دسترسی موظفند داده های ترافیک را حداقل تا شش‌ماه پس از ایجاد حفظ نمایند و اطلاعات کاربران را حداقل تا شش‌ماه پس از خاتمه اشتراک نگهداری کنند.

تبصره۱ـ داده ترافیک، هرگونه داده ای است که سامانه های رایانه ای در زنجیره ارتباطات رایانه ای و مخابراتی تولید می‌کنند تا امکان ردیابی آنها از مبدأ تا مقصد وجود داشته باشد. این داده ها شامل اطلاعاتی از قبیل مبدأ، مسیر، تاریخ، زمان، مدت و حجم ارتباط و نوع خدمات مربوطه می شود.

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.

ماده۶۶۸ـ 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.

ماده۶۶۹ـ هرگاه حفظ داده های رایانه ای ذخیره‌شده برای تحقیق یا دادرسی لازم باشد، مقام‌قضائی می تواند 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 داده ها، ضابطان قضائی می توانند 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 داده های حفاظت شده را افشاء کنند یا اشخاصی که داده های مزبور به آنها مربوط می شود 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 پنج تا ده میلیون ریال یا هردو مجازات محکوم می‌شوند.

تبصره۱ـ حفظ داده ها 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.

ماده۶۷۰ـ مقام قضائی می تواند دستور ارائه داده های 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.

ماده۶۷۱ـ تفتیش و توقیف داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی به موجب دستور قضائی و در مواردی به عمل می آید که ظن قوی به کشف جرم یا شناسایی متهم یا ادله جرم وجود دارد.

ماده۶۷۲ـ تفتیش و توقیف داده ها یا سامانه های رایانه ای و مخابراتی در حضور متصرفان قانونی یا اشخاصی که به نحوی آنها را تحت کنترل قانونی دارند، نظیر متصدیان سامانه ها 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 داده های مورد نظر، نوع و تعداد سخت افزارها و نرم افزارها، نحوه دستیابی به داده های رمزنگاری یا حذف شده و زمان تقریبی انجام تفتیش و توقیف باشد که به اجرای صحیح آن کمک می کند.

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

الف ـ دسترسی به تمام یا بخشی از سامانه های رایانه ای یا مخابراتی

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

پ ـ دستیابی به داده های حذف یا رمزنگاری شده

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

ماده۶۷۶ـ در شرایط زیر سامانه های رایانه ای یا مخابراتی توقیف می‌شوند:

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

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

پ ـ متصرف قانونی سامانه رضایت داده باشد.

ت ـ تصویربرداری از داده ها 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 داده ها یا سامانه های رایانه ای 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.

ماده۶۸۰ـ در جایی که اصل داده ها توقیف می شود، ذی نفع حق دارد پس از پرداخت هزینه از آنها کپی دریافت کند، مشروط به اینکه ارائه داده های توقیف‌شده منافی با ضرورت کشف حقیقت نباشد و به روند تحقیقات لطمه ای وارد نسازد و داده ها مجرمانه نباشد.

ماده۶۸۱ـ در مواردی که اصل داده ها یا سامانه های رایانه ای یا مخابراتی توقیف می‌شود، قاضی موظف است با لحاظ نوع و میزان داده ها 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.

ماده۶۸۲ـ 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.

ماده۶۸۳ـ کنترل محتوای در حال انتقال ارتباطات غیرعمومی در سامانه های رایانه ای 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.

ماده۶۸۴ـ 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.

ماده۶۸۵ـ چنانچه داده های رایانه ای توسط طرف دعوی یا شخص ثالثی که از دعوی آگاهی ندارد، ایجاد یا پردازش یا ذخیره یا منتقل شود و سامانه رایانه ای یا مخابراتی مربوط به نحوی درست عمل کند که به صحت و تمامیت، اعتبار و انکارناپذیری داده ها خدشه وارد نشود، قابل استناد است.

ماده۶۸۶ـ کلیه مقررات مندرج در این بخش، علاوه بر جرائم رایانه ای شامل سایر جرائمی که ادله الکترونیکی در آنها مورد استناد قرار می گیرند نیز می شود.

ماده۶۸۷ـ 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.