

آیین نامه جمع آوری و استنادپذیری ادله الکترونیکی

آیین نامه جمع آوری و استنادپذیری ادله الکترونیکی

در اجرای ماده ۵۴ قانون جرایم رایانه‌ای مصوب ۱۳۸۸/۳/۵ مجلس شورای اسلامی و بنا به پیشنهاد وزیر دادگستری، آیین نامه جمع آوری و استنادپذیری ادله الکترونیکی به شرح مواد آتی است:

فصل اول: تعاریف

ماده ۱ واژه‌ها و اصطلاحات بکار برده شده در این آیین نامه در معانی زیر بکار می‌رود:

الف- ارائه دهندگان 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 تأمین کنندگان، توزیع کنندگان، عرضه کنندگان خدمات دسترسی به شبکه‌های رایانه‌ای یا مخابراتی.

ب- ارائه دهندگان خدمات میزبانی: اشخاصی هستند که امکان دسترسی کاربران به فضای ایجاد شده توسط سامانه‌های رایانه‌ای، مخابراتی و ارتباطی تحت تصرف یا کنترل خود را به کاربران واگذار می‌کنند تا راساً 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 ارائه داده‌های الکترونیکی: عبارت است از در اختیار قراردادن تمام یا بخشی از داده‌های حفظ یا نگهداری شده توسط ارائه دهندگان خدمات دسترسی یا میزبانی یا اشخاصی که داده‌ها را تحت تصرف یا کنترل دارند.

د - جمع آوری ادله الکترونیکی: فرایندی 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.

ه - زنجیره حفاظتی: مجموعه اقداماتی است که ضابط دادگستری و سایر اشخاص ذیصلاح به منظور حفظ صحت، تمامیت، اعتبار و انکار ناپذیری ادله الکترونیکی با بکارگیری ابزارها و روشهای استاندارد در مراحل شناسایی، کشف، جمع آوری، مستند سازی، تجزیه و تحلیل و ارائه آنها به مرجع مربوط به اجرا در آورده و ثبت می‌کنند؛ به نحوی که امکان ردیابی آنها از مبدا تا مقصد وجود داشته باشد.

و - شنود: عبارت است از هرگونه دستیابی به محتوای در حال انتقال ارتباطات غیر عمومی در سامانه‌های رایانه‌ای یا مخابراتی یا امواج الکترومغناطیسی با استفاده از سامانه‌ها و تجهیزات سخت‌افزاری و نرم‌افزاری مربوط.

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

ح 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 غیر دولتی، بالاترین مقام آنها یا نماینده قانونی آنها طبق مقررات مربوط و در مورد سایر اشخاص حقوقی، مدیر یا نماینده قانونی آنهاست.

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

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

فصل دوم: جمع آوری ادله الکترونیکی

الف: نگهداری داده‌ها

ماده ۲ ارائه دهندگان خدمات دسترسی و میزبانی موظفند از سامانه‌هایی استفاده نمایند که قابلیت نگهداری داده‌های ترافیک و اطلاعات کاربران را مطابق مواد ۳۲ و ۳۳ قانون داشته باشد.

ماده ۳ 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: عرضه کنندگان خدمات دسترسی حضوری اینترنت (کافی نت‌ها) موظفند مشخصات هویتی، آدرس، ساعت شروع و خاتمه کار کاربر و نشانی اینترنتی (IP) تخصیصی را در دفتر روزانه ثبت نمایند.

ماده ۴ ارائه دهندگان خدمات 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 منعقدہ درج شود.

ماده ۵ ارائه‌دهندگان خدمات میزبانی داخلی و نمایندگان داخلی ارائه دهندگان 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.

تبصره ۱: 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.

تبصره ۲: اشخاصی که نسبت به انباشت یا ذخیره موقت اطلاعات در راستای ارائه خدمات دسترسی اقدام می‌کنند، ارائه دهنده خدمات میزبانی محسوب نمی‌شوند.

ماده ۶ ارائه دهندگان 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 رییس قوه قضاییه می‌رسد، تأمین نمایند.

ماده ۷ 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 انکار ناپذیری آنها محفوظ بماند.

ماده ۸ در مواردی که برابر قانون نگهداری و حفاظت داده‌ها الزامی است، نگهداری و حفاظت باید به گونه‌ای انجام شود که مدیریت جستجو و گزارش دهی آنها امکان‌پذیر باشد.

ماده ۹ وزارت ارتباطات و فن آوری اطلاعات هماهنگی‌های لازم برای تنظیم زمان سامانه‌های جمع‌آوری داده‌های محتوا، ترافیک و اطلاعات کاربران را مطابق با ساعت رسمی کشور به عمل می‌آورد.

ماده ۱۰ 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 استناد پذیری داده‌ها را تصویب و به ارائه دهندگان خدمات دسترسی و میزبانی و بهره برداران ابلاغ می‌نماید.

ب: حفاظت از ادله رایانه‌ای

ماده ۱۱ مقام قضایی در جریان تحقیق و فرایند 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 سخت افزار مخصوصی می‌باشد، صادر نماید.

تبصره ۱: ضابطان قضایی فقط در موارد مندرج در ماده ۳۴ قانون می‌توانند راساً دستور حفاظت داده‌های ذخیره شده را صادر کنند.

تبصره ۲: قاضی مکلف است بلافاصله پس از اعلام ضابط قضایی نسبت به تأیید یا رد دستور حفاظت صادره توسط ضابط اظهار نظر نماید. مجری حفاظت تا تعیین تکلیف از ناحیه قاضی موظف به حفاظت از اطلاعات می‌باشد.

ماده ۱۲ دستور حفاظت باید به طور صریح و دقیق مشتمل بر نوع داده‌ها، موضوع و مدت زمان با رعایت تبصره ۲ ماده ۳۴ قانون، باشد.

ماده ۱۳ در موارد مقتضی، اجرای دستور حفاظت با نظارت ضابطان قضایی متخصص یا اشخاص خبره مورد وثوق به نمایندگی از طرف مرجع قضایی انجام می‌شود.

ماده ۱۴ مجری حفاظت موظف است بلافاصله پس از ابلاغ، دستور حفاظت را اجرا و صورت جلسه ای را مشتمل بر زمان اجرای دستور، نحوه حفاظت، حجم و نوع داده‌های حفاظت شده در دو نسخه تنظیم و یک نسخه از آن را به مرجع صادر کننده دستور ارسال کند و نسخه دیگر را نزد خود نگه دارد.

ماده ۱۵ دستور حفاظت باید فوری و باروش مطمئن به مجری حفاظت ابلاغ شود. این دستور همچنین به اشخاص ذینفع نیز ابلاغ می‌شود؛ مگر آن که ابلاغ به آنها محل رسیدگی باشد که در این صورت تشخیص زمان ابلاغ حسب مورد با مقام قضایی می‌باشد. تبصره: روش مطمئن روشی است که با توجه به نوع داده‌ها و طول مدت زمان حفاظت، امکان بهره برداری از داده‌های حفاظت شده را در مراحل بعدی دادرسی ممکن سازد.

ماده ۱۶ حفاظت از داده‌ها باید به نحوی باشد که محرمانگی، تمامیت، صحت و انکارناپذیری داده‌ها رعایت شود.

ج: ارائه ادله رایانه‌ای

ماده ۱۷ دستور ارائه توسط مقام قضایی صادر می‌شود و باید به طور صریح و شفاف و مشتمل بر شخص ارائه دهنده، موضوع و نوع داده‌ها، شیوه و زمان تحویل داده‌ها و مرجع تحویل گیرنده باشد.

ماده ۱۸ ارائه داده‌ها باید به نحوی باشد که محرمانگی، تمامیت، صحت و انکارناپذیری داده‌ها رعایت شده و حتی الامکان بدون ایجاد مانع برای فعالیت سامانه و باروش متعارف و کم هزینه به یکی از شیوه‌های ذیل باشد:

الف- تحویل یک نسخه چاپ شده از داده.

ب- تحویل یک نسخه رایانه‌ای از داده.

ج- ایجاد دسترسی به داده.

د- انتقال تجهیزات رایانه‌ای و مخابراتی.

ماده ۱۹ هنگام ارائه داده‌ها صورت جلسه ای در سه نسخه تنظیم و حداقل موارد ذیل در آن ذکر و به امضای ارائه دهنده و تحویل گیرنده می‌رسد:

الف- شماره و تاریخ دستور قضایی ارائه داده‌ها

ب - مشخصات ارائه دهنده

ج - مشخصات تحویل گیرنده

د- زمان و مکان ارائه

ه نوع و حجم داده‌ها

و - اطلاعات مربوط به نحوه حفظ یا نگهداری داده‌ها

ز - روشهای امنیتی بکاررفته در زمان ارائه

ح - مشخصات سخت‌افزاری و نرم‌افزاری تجهیزات

ط - شیوه ارائه و مشخصات داده.

تبصره ۱: در هنگام انتقال تجهیزات، احتیاط لازم برای حفظ آنها بعمل می‌آید.

تبصره ۲: یک نسخه از صورت جلسه به مرجع قضایی ارسال می شود و نسخه ای در اختیار ارائه دهنده و نسخه دیگر در اختیار تحویل گیرنده قرار می گیرد.

ماده ۲۰ از زمان ارائه داده ها به ضابطان قضایی یا دیگر اشخاص ذربط، مسئولیت حفظ داده های مذکور با شخص یا اشخاص تحویل گیرنده خواهد بود.

ماده ۲۱ ارائه داده هایی که افشا یا دسترسی به آنها مطابق قوانین خاص دارای محدودیت یا توأم با تشریفات می باشد، تابع مقررات مربوط است.

ماده ۲۲ دستور ارائه داده، مجوز افشای آن نمی باشد و پس از دستور ارائه هرگونه دسترسی به مفاد داده مستلزم صدور دستور قضایی است.

ماده ۲۳ اشخاصی که مسئول اجرای هر یک از دستورات قضایی اعم از نگهداری، حفاظت، ارائه، تفتیش و توقیف سامانه و داده یا شنود آن می باشند یا دستور به آنها ابلاغ می شود یا به نوعی مرتبط با دستورات یاد شده هستند، حق افشای مفاد دستور و یا داده ها و اطلاعات مربوط را ندارند.

د: تفتیش و توقیف ادله رایانه ای

ماده ۲۴ ضابطان قضایی باید کلیه اطلاعاتی که ضرورت تفتیش و توقیف را ایجاد می نماید در درخواست خود اعلام نمایند. همچنین، موارد زیر را حسب مورد در درخواست تفتیش یا توقیف ذکر نمایند:

الف- دلایل ضرورت تفتیش و توقیف

ب - حتی الامکان نوع و میزان داده ها و سخت افزارها

ج - محل تفتیش یا توقیف

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

ه - زمان تقریبی لازم برای تفتیش و توقیف.

ماده ۲۵ در دستور تفتیش یا توقیف داده یا سامانه باید محل تفتیش یا توقیف تعیین و حتی الامکان در محل استقرار سامانه انجام پذیرد.

ماده ۲۶ 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 می باشد.

ماده ۲۷ تفتیش و توقیف در مواردی که مستلزم ورود به منازل و اماکن خصوصی باشد، مطابق مقررات مندرج در آیین دادرسی کیفری خواهد بود.

ماده ۲۸ 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.

ماده ۲۹ چنانچه پس از اجرای دستور توقیف و یا در زمان اجرای دستور توقیف داده ها یا سامانه های رایانه ای 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 عمل می گردد.

ماده ۳۰ قوه قضاییه تمهیدات لازم از جمله بستر سازی و ایجاد زیر ساختهای ارتباط رایانه ای و الکترونیکی و همچنین راه اندازی سامانه ها و درگاه های مبتنی بر فناوری اطلاعات را جهت تسهیل در عملیاتی کردن فرایندها و روشهای موضوع این آیین نامه فراهم می آورد.

ماده ۳۱ اشخاصی که داده ها یا سامانه های رایانه ای یا مخابراتی را تحت کنترل و یا تصرف دارند، موظف به همکاری در اجرای دستور تفتیش و توقیف می باشند. در صورتی که به واسطه عدم همکاری یا عدم دسترسی به این اشخاص، تفتیش یا توقیف امکان پذیر نباشد،

نحوه دسترسی به داده‌ها یا سامانه‌ها از قبیل ورود به محل، رفع موانع استفاده از سخت افزار و نرم افزار، رمزگشایی و امثال آن با دستور مقام قضایی تعیین خواهد شد.

ماده ۳۲ رضایت متصرف قانونی سامانه موضوع بند ج ماده ۴۱ قانون، باید کتبی و با امضای وی باشد.

ماده ۳۳ 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.

ماده ۳۴ 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 ارتكابی در سایر سامانه‌های رایانه‌ای یا مخابراتی تحت کنترل یا تصرف متهم کشف شود، در صورت بیم احما نسبت به حفظ فوری داده‌ها اقدام و مراتب را حداکثر ظرف ۲۴ ساعت کتباً به مقام قضایی مربوط گزارش می‌دهند.

ماده ۳۵ 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.

ماده ۳۶ 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.

ماده ۳۷ هنگام تفتیش رعایت موارد زیر ضروری است:

الف شیوه اقدام نباید موجب تغییر، احما یا جابجایی داده‌های مورد نظر در سامانه‌های رایانه‌ای باشد.

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

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

ماده ۳۸ توقیف با رعایت تناسب، نوع، اهمیت و نقش داده یا سامانه رایانه‌ای یا مخابراتی به روش‌های زیر انجام می‌شود:

الف در توقیف داده‌ها از طریق چاپ داده‌ها، غیر قابل دسترس کردن داده‌ها به روش‌هایی از قبیل تغییر گذرواژه یا رمزنگاری و ضبط حامل‌های داده.

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

تبصره: توقیف باید حتی الامکان 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.

ماده ۳۹ 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 و رعایت مقررات این آیین‌نامه اقدام نمایند.

ماده ۴۰ در صورت پلمپ سامانه چنانچه نیاز به گماردن حافظ باشد با دستور مقام قضایی اقدام می‌شود.

ماده ۴۱ 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: چنانچه برای نگهداری و مراقبت مدت بیشتری مورد نیاز باشد، مدت مذکور به صورت مستدل توسط مقام قضایی تمدید می‌شود.

ماده ۴۲ 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 رسیدگی کننده، در سابقه ضبط گردد.

ماده ۴۳ 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 علامت گذاری و ثبت می‌شوند را تنظیم و به امضای تفتیش کننده یا توقیف کننده و متصرف قانونی که سامانه تحت کنترل اوست یا قائم مقام قانونی وی برسانند. برای ضبط دقیق مشخصات ابزار و اجزای آن تصویربرداری بلامانع است.

ماده ۴۴ مرجع قضایی صالح، ضمن صدور رأی باید نسبت به داده یا سامانه توقیف شده تعیین تکلیف نماید.

فصل سوم: امور متفرقه

ماده ۴۵ 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 اجرا، خاموش و روشن کردن سامانه، بسته‌بندی و انتقال اطلاعات و نیز نمونه درخواست‌های مرتبط با این موارد باشد.

ماده ۴۶ 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 قضاییه و سازمان‌های تابعه مراکز مرتبط با قوه قضاییه باشد، با دستور مقام قضایی توسط مرکز حفاظت و اطلاعات قوه قضاییه انجام خواهد شد.

ماده ۴۷ نسخه‌های تهیه شده از داده‌های رایانه‌ای قابل استناد به صورت متن، صوت یا تصویر در حکم اصل داده می‌باشند.

ماده ۴۸ این آیین نامه توسط وزارت دادگستری با همکاری وزارت ارتباطات و فناوری اطلاعات تهیه و در ۴۸ ماده و ۱۱ تبصره به تصویب رئیس قوه قضائیه رسید.

صادق آملی لاریجانی رییس قوه قضاییه