

## آیین نامه جمع آوری و استنادپذیری ادله الکترونیکی

شماره ۹۰۰۰/۲۸۱۹۹/۱۰۰ ۱۳۹۳/۵/۱۲

در اجرای ماده ۵۴ قانون جرایم رایانه ای 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- واژه ها و اصطلاحات بکار برده شده در این آیین نامه در معانی زیر بکار می رود:

الف - ارائه دهندگان خدمات دسترسی: اشخاصی هستند که امکان ارتباط کاربران را با شبکه های رایانه ای یا مخابراتی و ارتباطی داخلی یا بین المللی یا هر شبکه مستقل دیگر فراهم می آورند از قبیل تأمین کنندگان، توزیع کنندگان، عرضه کنندگان خدمات دسترسی به شبکه های رایانه ای یا مخابراتی.

ب - ارائه دهندگان خدمات میزبانی: اشخاصی هستند که امکان دسترسی کاربران به فضای ایجاد شده توسط سامانه های رایانه ای، مخابراتی و ارتباطی تحت تصرف یا کنترل خود را به کاربران واگذار می کنند تا رأساً یا توسط کاربر متقاضی، داده های رایانه ای را جهت نگهداری، انتشار، توزیع یا ارائه در شبکه های داخلی یا بین المللی یا هر منظور دیگر ذخیره یا پردازش کنند.

ج - ارائه داده های الکترونیکی: عبارت است از در اختیار قرار دادن تمام یا بخشی از داده های حفظ یا نگهداری شده توسط ارائه دهندگان خدمات دسترسی یا میزبانی یا اشخاصی که داده ها را تحت تصرف یا کنترل دارند.

د - جمع آوری ادله الکترونیکی: فرآیندی است که طی آن ادله الکترونیکی به تنهایی یا به همراه سامانه های رایانه ای یا مخابراتی یا حامل های داده، نگهداری، حفظ فوری، تفتیش و توقیف و شنود می شوند.

ه - 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 روش های استاندارد در مراحل شناسایی، کشف، جمع آوری، مستندسازی، تجزیه و تحلیل و ارائه آنها به مرجع مربوط به اجرا درآورده و ثبت می کنند؛ به نحوی که امکان ردیابی آنها از مبدأ تا مقصد وجود داشته باشد.

و - شنود: عبارت است از هر گونه دستیابی به محتوای در حال انتقال ارتباطات غیرعمومی در سامانه های رایانه ای یا مخابراتی یا امواج الکترومغناطیسی با استفاده از سامانه ها و تجهیزات سخت افزاری و نرم افزاری مربوط.

ز- مجری حفاظت: شخصی است که به نحوی داده های رایانه ای ذخیره شده را تحت تصرف یا کنترل دارد و مطابق ماده ۳۴ قانون و سایر قوانین و مقررات جهت حفاظت آنها تعیین می شود.

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 غیردولتی، 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 رایانه ای مصوب ۱۳۸۸/۳/۵ می باشد.

تبصره - سایر اصطلاحات به شرح تعریف ارائه شده در قوانین دیگر می باشد.

## فصل دوم: جمع آوری ادله الکترونیکی

الف: نگهداری داده ها

ماده ۲- ارائه دهندگان خدمات دسترسی و میزبانی موظفند از سامانه هایی استفاده نمایند که قابلیت نگهداری داده های ترافیک و اطلاعات کاربران را مطابق مواد ۳۲ و ۳۳ قانون داشته باشد.

ماده ۳- ارائه دهندگان خدمات دسترسی موظفند سامانه های خود را به نحوی تنظیم کنند که کلیه ارتباطات رایانه ای را که از طریق آنها انجام می شود ثبت کنند و کلیه داده های ترافیک مربوط به خود و کاربران مربوط را تا شش ماه پس از ایجاد نگهداری کنند.

تبصره - عرضه کنندگان خدمات دسترسی حضوری اینترنت (کافی نت ها) 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 منعقد شده درج شود.

ماده ۵- ارائه دهندگان 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- ارائه دهندگان خدمات میزبانی موظفند سامانه های رایانه ای خود را به نحوی تنظیم کنند که هر گونه 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 می کنند، ارائه دهنده خدمات میزبانی محسوب نمی شوند.

ماده ۶- ارائه دهندگان خدمات دسترسی و میزبانی و مجریان حفاظت موظفند امنیت داده های ترافیکی و محتوای نگهداری و حفاظت شده را مطابق با ضوابط و دستورالعمل هایی که به تصویب رئیس قوه قضاییه می رسد، تأمین نمایند.

اده ۷- داده های محتوا و ترافیک و اطلاعات کاربران باید مطابق مقررات این آیین نامه به نحوی نگهداری، حفاظت، توقیف و ارائه شود که صحت و تمامیت، محرمانگی، اعتبار و انکارناپذیری آنها محفوظ بماند.

ماده ۸- در مواردی که برابر قانون نگهداری و حفاظت داده ها الزامی است، نگهداری و حفاظت باید به گونه ای انجام شود که مدیریت جستجو و گزارش دهی آنها امکان پذیر باشد.

ماده ۹- وزارت ارتباطات و فناوری اطلاعات هماهنگی های لازم برای تنظیم زمان سامانه های جمع آوری داده های محتوا، ترافیک و اطلاعات کاربران را مطابق با ساعت رسمی کشور به عمل می آورد.

ماده ۱۰- مرکز آمار و فناوری اطلاعات با همکاری وزارت ارتباطات و فناوری اطلاعات سالانه رویه های فنی نحوه نگهداری، حفاظت، توقیف و ارائه داده ها و اطلاعات کاربران و همچنین راهنماهای عملی حفظ امنیت و استنادپذیری داده ها را تصویب و به ارائه دهندگان خدمات دسترسی و میزبانی و بهره برداران ابلاغ می نماید.

ب: حفاظت از ادله رایانه ای

ماده ۱۱- مقام قضایی در جریان تحقیق و فرآیند رسیدگی می تواند دستور حفاظت هر نوع داده رایانه ای ذخیره شده را از جمله داده های رمزنگاری شده، حذف، پنهان، فشرده یا پنهان نگاری شده و یا داده هایی که نوع و نام آنها موقتاً تغییر یافته و یا داده هایی که برای بررسی آنها نیاز به سخت افزار مخصوصی می باشد، صادر نماید.

تبصره ۱- ضابطان قضایی فقط در موارد مندرج در ماده ۳۴ قانون می توانند رأساً دستور حفاظت داده های 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 اظهارنظر نماید. مجری حفاظت تا تعیین تکلیف از ناحیه قاضی موظف به حفاظت از اطلاعات می باشد.

ماده ۱۲- دستور حفاظت باید به طور صریح و دقیق مشتمل بر نوع داده ها، 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 می شود.

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 داده های حفاظت شده در دو نسخه تنظیم و یک نسخه از آن را به مرجع صادرکننده دستور ارسال کند و نسخه دیگر را نزد خود نگه دارد.

ماده ۱۵- دستور حفاظت باید فوری و با روش مطمئن به مجری حفاظت ابلاغ شود. این دستور همچنین به اشخاص ذینفع نیز ابلاغ می شود؛ مگر آن که ابلاغ به آنها مخل رسیدگی باشد که در این صورت تشخیص زمان ابلاغ حسب مورد با مقام قضایی می باشد.

تبصره - روش مطمئن روشی است که با توجه به نوع داده ها و طول مدت زمان حفاظت، امکان بهره برداری از داده های حفاظت شده را در مراحل بعدی دادرسی ممکن سازد.

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

ج: ارائه ادله رایانه ای

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

ماده ۱۸- ارائه داده ها باید به نحوی باشد که محرمانگی، تمامیت، صحت و انکارناپذیری داده ها رعایت شده و حتی الامکان بدون ایجاد مانع برای فعالیت سامانه و با روش متعارف و کم هزینه به یکی از شیوه های ذیل باشد:

الف - تحویل یک نسخه چاپ شده از داده.

ب - تحویل یک نسخه رایانه ای از داده.

ج - ایجاد دسترسی به داده.

د - انتقال تجهیزات رایانه ای و مخابراتی.

ماده ۱۹- هنگام ارائه داده ها صورت جلسه ای در سه نسخه تنظیم و حداقل موارد ذیل در آن ذکر و به امضای ارائه دهنده و تحویل گیرنده می رسد:

الف - شماره و تاریخ دستور قضایی ارائه داده ها

ب - مشخصات ارائه دهنده

ج - مشخصات تحویل گیرنده

د - زمان و مکان ارائه

ه - نوع و حجم داده ها

و- اطلاعات مربوط به نحوه حفظ یا نگهداری داده ها

ز- روش های امنیتی بکاررفته در زمان ارائه

ح- مشخصات سخت افزاری و نرم افزاری تجهیزات.

ط- شیوه ارائه و مشخصات داده.

تبصره ۱- در هنگام انتقال تجهیزات، احتیاط لازم برای حفظ آنها به عمل می آید.

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 ذیربط، 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 هر گونه 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 ایجاب 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 بسترسازی و ایجاد زیرساخت های 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 روش های 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 داده ها یا سامانه ها 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 داده ها به روش چاپ یا کپی یا تصویربرداری داده ها انجام می شود، اصل داده ها در صورتی توقیف و غیرقابل دسترس می شود که در دستور قضایی تصریح شده باشد.

ماده ۳۴- ضابطان صرفاً مجاز به تفتیش و توقیف داده ها و سامانه هایی هستند که به طور صریح در دستور قضایی ذکر گردیده و چنانچه حین اجرای دستور، داده های مرتبط با جرم ارتكابی در سایر سامانه های رایانه ای یا مخابراتی تحت کنترل یا تصرف متهم

کشف شود، در صورت بیم امحان نسبت به حفظ فوری داده ها اقدام و مراتب را حداکثر ظرف ۲۴ ساعت کتباً به مقام قضایی مربوط گزارش می دهند.

ماده ۳۵- تفتیش داده ها یا سامانه ها 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 می پذیرد.

ماده ۳۶- ضابطان و اشخاصی که حسب قانون مأمور جمع آوری، تفتیش، نگهداری، حفظ و انتقال داده ها و سامانه های رایانه ای یا مخابراتی می شوند 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، امحا یا جابجایی داده های مورد نظر در سامانه های رایانه ای باشد.

ب - تفتیش صرفاً در محدوده دستور قضایی و داده های مرتبط با جرم موضوع دستور، انجام می پذیرد.

ج - کلیه فرایندهای انجام شده بر روی داده های مورد تفتیش یا توقیف باید با استفاده از روش های قابل تشخیص، ثبت و محافظت شود.

ماده ۳۸- توقیف با رعایت تناسب، نوع، اهمیت و نقش داده یا سامانه رایانه ای یا مخابراتی به روش های زیر انجام می شود:

الف - در توقیف داده ها از طریق چاپ داده ها، غیرقابل دسترس کردن داده ها به روش هایی از قبیل تغییر گذر واژه یا رمزنگاری و ضبط حامل های داده.

ب - در توقیف سامانه های رایانه ای یا مخابراتی از طریق تغییر گذر واژه، 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 شیوه هایی از قبیل ذخیره در حامل های داده، ذخیره در سامانه با گذاشتن گذرواژه، تهیه نسخه پشتیبان، تصویربرداری، تهیه رونوشت و چاپ انجام شود.

ماده ۳۹- دستور توقیف سامانه شامل سایر سخت افزارها یا حامل های داده متصل به آن نمی شود، مگر آن که در دستور قضایی تصریح گردد. در صورت نیاز به حفظ فوری سخت افزارها یا حامل های داده، ضابطان یا سایر مأموران در حدود وظایف قانونی می توانند نسبت به حفظ فوری آن مطابق ماده ۳۴ قانون و رعایت مقررات این آیین نامه اقدام نمایند.

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

ماده ۴۱- به منظور حفظ وضعیت اصلی ادله رایانه ای و جلوگیری از هرگونه تغییر، تحریف یا آسیب آن، مرجع قضایی مدت زمان نگهداری و مراقبت از آنها را تا مدت ۵ روز تعیین می کند.

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

ماده ۴۲- اجرای دستور توقیف باید طی صورت جلسه ای با قید دقیق جزییات 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 اولیه ای از سامانه رایانه ای یا مخابراتی و اجزای آن و کلیه اتصالات کابلی بین اجزای مختلف سخت افزارها و حامل های داده متصل به آن که علامت گذاری و ثبت می شوند 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 جمع آوری ادله و توقیف سامانه های رایانه ای و مخابراتی توسط دادستانی کل کشور با همکاری نیروی انتظامی تهیه و به تصویب دادستان کل کشور می رسد. این دستورالعمل باید دربردارنده چگونگی حفظ صحنه جرم و جمع آوری ادله از سامانه در حال اجرا، خاموش و روشن کردن سامانه، بسته بندی و انتقال اطلاعات و نیز نمونه درخواست های مرتبط با این موارد باشد.

ماده ۴۶- در مورد جمع آوری ادله الکترونیکی از جمله نگهداری، حفظ فوری، تفتیش و توقیف و شنود چنانچه موضوع مربوط به افراد و اماکن وابسته به قوه قضاییه و سازمان های تابعه مراکز مرتبط با قوه قضاییه باشد، با دستور مقام قضایی توسط مرکز حفاظت و اطلاعات قوه قضاییه انجام خواهد شد.

ماده ۴۷- نسخه های تهیه شده از داده های رایانه ای قابل استناد به صورت متن، صوت یا تصویر در حکم اصل داده می باشند.

ماده ۴۸- این آیین نامه توسط وزارت دادگستری با همکاری وزارت ارتباطات و فناوری اطلاعات تهیه و در ۴۸ ماده و ۱۱ تبصره در تاریخ ۱۳۹۳/۵/۱۲ به تصویب رئیس قوه قضاییه رسید.