

دانستنی‌های حقوقی برای همه مردم

چه زمانی «اسکرین شات» پیام‌های شبکه‌های اجتماعی در دادگاه سند محسوب می‌شود؟

شبکه‌های اجتماعی و ابزارهای ارتباطی نوین و به خصوص تلفن همراه شرایطی را فراهم کرده است که گویی همه در محضر عالم هستیم و هر گونه اقدامی هر چند در خفا صورت می‌گیرد، با این ابزارها ثبت و ضبط می‌شود. با این حساب و با وجود قوانین سختگیرانه مانند قانون جرایم رایانه‌ای، باید از تعداد جرایم کاسته می‌شود ولی اینطور نیست زیرا بسیاری از چیزهایی که ما می‌پنداریم سند اثبات جرم یا موضوعی هستند، از نظر قانون دارای اعتبار تلقی نمی‌شوند.

به گزارش خبرنگاران جامعه گزارش خبر، فرض کنید در شبکه‌های اجتماعی خارجی مانند تلگرام، توئیتر، یا اینستاگرام، فردی به شما توهین کند، یا افترا بزند یا تصاویر خصوصی شما را تهیه و پخش کند و آبروی شما را ببرد. یا اصلاً موضوع جرم نباشد، بلکه فرضاً شما از شخصی طلبکار هستید و در یک اپلیکیشن خارجی مانند تلگرام از او می‌خواهد بدهی اش را بپردازد و این شخص جواب بدهد با وجودی که بدهکار هستید، نمی‌خواهم طلب تو را بپردازم.

آیا این اظهارات که در شبکه‌های اجتماعی یا از طریق ایمیل بیان شده و در قانون به آنها «داده پیام» می‌گویند، می‌تواند ثابت کند این فرد گناهکار، متهم، مجرم یا حتی بدهکار است؟ اینجاست که باید نگاهی به متن‌های مهم ضابطه‌گذاری قانونی در فضای مجازی بیندازیم.

اولین متن، قانون جرایم رایانه‌ای و دومین متن، آیین‌نامه جمع‌آوری و استنادپذیری ادله (دلایل) الکترونیک است. نکته اصلی اینجاست که در هر دو این متن‌ها، به سادگی نمی‌شود تشخیص داد چه داده پیامی دارای ارزش اثباتی در دادگاه است و چه داده پیامی نیست.

اولاً باید در نظر داشت که بسیاری از قوانین معمول فعلی در این حوزه از جمله قانون جرایم رایانه‌ای و آیین‌نامه جمع‌آوری و استنادپذیری ادله الکترونیک، با تأکید بر «حفظ داده پیام از سوی سرویس‌دهندگان (ISP)ها-شرکتهای اینترنتی منتقل‌کننده داده پیام و صاحبان و مدیران شبکه‌های اجتماعی» نوشته شده است ولی همانطور که می‌دانیم بیشترین استفاده شهروندان از سرویس‌های ایمیلی و شبکه‌های اجتماعی خارجی در بستر اینترنت استفاده می‌کنند که اصولاً سرویس‌دهندگان آن در کشور نیستند و صمنی هم با سیستم قضایی ندارند که مرجع قضایی بتواند از آنها بخواهد داده پیام مورد استناد را در اختیارش بگذارند.

مثلاً اگر کسی به شما در اپلیکیشن تلگرام فحاشی و توهین کرد و پس از شکایت شما، اعلام کرد چنین چیزی را نگفته، منتسب کردن «داده پیام» توهین آمیز به او از طریق گواهی شرکت صاحب اپلیکیشن تلگرام یا سرویس «جی.میل» تقریباً ناممکن است، چون هم مراجع قضایی عادت به مکاتبه با شرکتهای خارجی برای بررسی دلایل را ندارند و هم اصولاً خط مشی این شرکت و سایر شرکتهای مشابه از جمله گوگل، واتس‌آپ، اینستاگرام، توئیتر و نظایر آنها، اجازه افشای مسائلی که بین کاربران گذشته را نمی‌دهد. یعنی اگر هم از آنها استعلام شود خواهند گفت به دلیل اعلام محرمانگی انتقال داده پیامها در خط مشی و مرامنامه خود، به این استعلام پاسخ نمی‌دهند.

قانونی که اجرای آن بسیار سخت است

هر چند در ماده ۱۱ آیین‌نامه جمع‌آوری و استنادپذیری ادله الکترونیک آمده است: «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 پنهان‌نگاری 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.» ولی در عرصه عمل، این حکم قانونی، تقریباً اجرا نشدنی است مگر درباره داده پیامهایی که فقط در نرم‌افزارها، سایتها و اپ‌های ایرانی جایجا شده است.

در این صورت است که چون معمولاً دسترسی به داده پیام اصلی در اپ‌ها و سایتها خارجی برای کسی مقدور نیست، مقام قضایی مطابق بند الف ماده ۱۸ آیین‌نامه مزبور، دستور تحویل یک نسخه چاپ شده از داده پیام را می‌دهد که معمولاً شاکای یا پلیس این کار را با پرینت اسکرین شات از داده پیام در محیط اپ‌های خارجی انجام می‌دهد. ماده ۴۷ این آیین‌نامه هم تأکید دارد «نسخه‌های تهیه شده از داده‌های رایانه‌ای قابل استناد به صورت متن، صوت یا تصویر در حکم اصل داده» است ولی نکته اصلی اینجاست که انتساب این داده پیامها به فردی که طرف شکایت یا دعوا قرار گرفته است اگر با انکار او همراه باشد، تقریباً ممکن نیست! به بیان دیگر، شما اسکرین از پیام فردی را که در شبکه‌های اجتماعی برای شما فرستاده تهیه می‌کنید و پرینت گرفته و در اختیار قاضی یا پلیس قرار می‌دهید ولی طرف مقابل می‌تواند به سادگی بگوید من این را ننوشتم! یا: این پیام از جانب من صادر نشده است! در این صورت، با وجودی که بتوان با اغماض گفت این پیام دارای اثر حقوقی داده شده است ولی نمی‌توان گفت فلان فرد خاص، این پیام را داده است!

ترفندهای پلیسی برای اثبات انتساب داده پیام

واقعیت این است که بسیاری از داده پیامهایی که در شبکه‌های اجتماعی رد و بدل می‌شوند، از طریق قانونی و معمول قابل انتساب به اشخاص نیستند. یعنی نمی‌شود گفت دادگاه می‌پذیرد فلانی این پیام را صادر کرده است و اگر شخصی که داده پیام منسوب به اوست، انکار کند، (اقرار نکند) اثبات انتساب داده پیام مجرمانه یا دارای مسئولیت حقوقی (مانند پیام اقرار به بدهکاری) به او بسیار مشکل است.

اینجاست که باید گفت اصلی‌ترین کار اثبات این داده پیامها بر عهده ضابطان تخصصی یعنی پلیس فضای تبادل اطلاعات در جرایم معمولی از قبیل کلاهبرداریهای الکترونیک، توهین و بردن حیثیت (افترا) و همچنین مراکز جنگ الکترونیک (جنگال) نهادهای امنیتی در جرایم خاصی مانند جرایم علیه امنیت عمومی و جرایم سازمان یافته از قبیل قاچاق گسترده مواد مخدر، انسان، اسلحه و نظایر آن است.

این مراکز تخصصی با ترفندهای خاصی که تلفیقی از روشهای الکترونیک و روانشناسی است، مرجع اصلی داده پیام صادر شده را شناسایی و سعی در اثبات انتساب داده پیام به متهمان می‌کنند. مانند آن که با روشهای فنی نفوذ به ابزار الکترونیک طرف مقابل، قادر به شناسایی مکان فیزیکی اتصال به اینترنت فرد و شماره منحصر به فرد اتصال او (IP) می‌شوند یا با زیرپاکشی، تله‌گذاری و مانیتورینگ دقیق و تحلیل داده‌های پیام‌های وی و شناسایی الگوهای ارائه و انتشار پیامها، قادر به شناسایی مرجع اصلی انتشار داده پیامها شده و در نهایت پس از دسترسی به او، با ارائه اسناد غیرقابل انکار و در بازجویی فنی، اقرار و اعتراف متهم را دریافت کرده و در اختیار مقام قضایی برای صدور رای می‌گذارند.

در حقیقت، بدون ترفندهای پلیسی و فنون خاصی که به کار گرفته شده و در نهایت منجر به شناسایی و اخذ اقرار از متهم می‌شوند، داده پیامهای

موجود به تنهایی، ارزش اثبات کردن چیزی را ندارند، پس در این صورت، باید پرونده به اندازه ای از اهمیت یا فراوانی و تکرار شونده‌گی برسد که نیروهای تخصصی، تشخیص دهند ارزش صرف وقت را دارد.

اینجاست که باید گفت اسکرین شات و پرینت پیامهای شبکه های اجتماعی در صورتی قابلیت استناد به طرف مقابل را دارد که اولاً فرد شناسایی شده باشد ثانیاً انتساب این پیام را انکار نکند ثالثاً به صدور چنین پیامی اقرار کند. در غیر این صورت اگر فردی شناسایی نشود ولی اقدامات الکترونیک مجرمانه ای انجام دهد، یا پس از شناسایی، اقرار به جرم نکند تقریباً هیچ کاری برای انتساب داده پیام مجرمانه به او نمی شود کرد. هر چند در برخی پرونده ها دیده شده است که نظریات کارشناسی کارشناس ضابط قضایی با وجود انکار متهم، توانسته است برای قاضی پرونده این اقناع وجدانی را به وجود بیاورد که دلایل کافی برای مجرم دانستن متهم وجود دارد و با همین دلایل، اقدام به صدور رای محکومیت کرده که عموماً چنین آراییی در مراحل بعدی اعتراض از جمله تجدیدنظر نقض می شوند چون لزوماً دلایل کارشناسی ارائه شده از سوی ضابط پرونده و فقدان اقرار متهم (و ای بسا انکار مصرانه او در تمام مراحل رسیدگی) برای سه نفر قاضی رسیدگی کننده در مرحله تجدیدنظر این اطمینان را به وجود نمی آورد که متهم، مجرم است.

قوانین پشتیبانی کننده از اسکرین شات

ذکر این نکته ضروری است که قانونگذار ما تنها در یک جا، گرفتن اسکرین شات از داده پیام را دارای ارزش اثباتی و همردیف دلیل آورده است. در ماده ۱۲ قانون تجارت الکترونیک درباره این موضوع آمده است: «اسناد و ادله اثبات دعوی ممکن است به صورت داده پیام بوده و در هیچ محکمه یا اداره دولتی نمی‌توان براساس قواعد ادله موجود، ارزش اثباتی «داده پیام» را صرفاً به دلیل شکل و قالب آن رد کرد.» باید توجه داشت که گسترده این ماده تنها در حوزه تجارت الکترونیک است و دادگاه ها نمی توانند دلایل دارای ارزش اثباتی در این قانون را در امور کیفری هم مورد استناد قرار دهند زیرا باید قانون به نفع متهم تفسیر شود و طبیعی است سوای جعلی بودن بسیاری از اسکرین شاتهای ارائه شده به محاکم کیفری یا دادسراها، دلایل قانونی که در قوانین کیفری برای اثبات جرم به کار رفته است، مشخص و محدود به مواردی کاملاً معلومی است و در آنها، دلایل الکترونیکی از مانند اسکرین شات نیست.