گزارش خبر
NEWSREPORT

کد خبر: ۴۵۱۳۳۳
چهارشنبه ۸ اردیبهشت ۱۴۰۰ ۱۰:۱۳

دانستنی‌های حقوقی برای همه مردم

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

شبکه های 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 می گیرد، با این ابزارها ثبت و ضبط می شود. با این حساب و با وجود قوانین سختگیرانه مانند قانون جرایم رایانه ای، باید از تعداد جرایم کاسته می شود ولی اینطور نیست زیرا بسیاری از چیزهایی که ما می پنداریم سند اثبات جرم یا موضوعی هستند، از نظر قانون دارای اعتبار تلقی نمی‌شوند.

به گزارش خبرنگاران جامعه گزارش خبر، فرض کنید در شبکه های اجتماعی خارجی مانند تلگرام، توییتر، یا اینستاگرام، فردی به شما توهین کند، یا افترا بزند یا تصاویر خصوصی شما را تهیه وپخش کند و آبروی شما را ببرد. یا اصلا موضوع جرم نباشد، بلکه فرضا شما از شخصی طلبکار هستید و در یک اپلیکیشن خارجی مانند تلگرام از او می خواهد بدهی اش را بپردازد و این شخص جواب بدهد با وجودی که بدهکار هستم، نمی خواهم طلب تو را بپردازم.

آیا این اظهارات که در شبکه های اجتماعی یا از طریق ایمیل بیان شده و در قانون به آنها «داده پیام» می گویند، می تواند ثابت کند این فرد گناهکار، متهم، مجرم یا حتی بدهکار است؟ اینجاست که باید نگاهی به متن های مهم ضابطه گذاری قانونی در فضای مجازی بیندازیم.

اولین متن، قانون جرایم رایانه ای و دومین متن، آیین نامه جمع آوری و استنادپذیری ادله (دلایل) الکترونیک است. نکته اصلی اینجاست که در هر دو این متن ها، به سادگی نمی شود تشخیص داد چه داده پیامی دارای ارزش اثباتی در دادگاه است و چه داده پیامی نیست.

اولا باید در نظر داشت که بسیاری از قوانین معمول فعلی در این حوزه از جمله قانون جرایم رایانه ای و آیین نامه جمع آوری و استنادپذیری ادله الکترونیک، با تاکید بر «حفظ داده پیام از سوی سرویس دهندگان (ISPها-شرکتهای اینترنتی منتقل کننده داده پیام و صاحبان و مدیران شبکه های اجتماعی)» نوشته شده است ولی همانطور که می دانیم بیشترین استفاده شهروندان از سرویس های ایمیلی و شبکه های اجتماعی خارجی در بستر اینترنت استفاده می کنند که اصولا سرویس دهندگان آن در کشور نیستند و صنمی هم با سیستم قضایی ندارند که مرجع قضایی بتواند از آنها بخواهد داده پیام مورد استناد را در اختیارش بگذارند.

مثلا 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» تقریبا ناممکن است، چون هم مراجع قضایی عادت به مکاتبه با شرکتهای خارجی برای بررسی دلایل را ندارند و هم اصولا خط مشی این شرکت و سایر شرکتهای مشابه از جمله گوگل، واتس اپ، اینستاگرام، توییتر و نظایر آنها، اجازه افشای مسایلی که بین کاربران گذشته را نمی دهد. 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 نمی دهند.

قانونی که اجرای آن بسیار سخت است

هر چند در ماده ۱۱ آیین نامه جمع آوری و استنادپذیری ادله الکترونیکی آمده است: «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.» ولی در عرصه عمل، این حکم قانونی، تقریبا اجرا نشدنی است مگر درباره داده پیامهایی که فقط در نرم افزارها، سایتها و اپ های ایرانی جابجا شده است.

در این صورت است که چون معمولا دسترسی به داده پیام اصلی در اپ ها و سایتهای خارجی برای کسی مقدور نیست، مقام قضایی مطابق بند الف ماده ۱۸ آیین نامه مزبور، دستور تحویل یک نسخه چاپ شده از داده پیام را می دهد که معمولا شاکی یا پلیس این کار را با پرینت اسکرین شات از داده پیام در محیط اپ های خارجی انجام می دهد. ماده ۴۷ این آیین نامه هم تاکید دارد «نسخه های تهیه شده از داده های رایانه ای 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، تقریبا ممکن نیست! به بیان دیگر، شما اسکرین از پیام فردی را که در شبکه های اجتماعی برای شما فرستاده تهیه می کنید و پرینت گرفته و در اختیار قاضی یا پلیس قرار می دهید ولی طرف مقابل می تواند 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 نمی توان 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 شبکه های اجتماعی رد و بدل می شوند، از طریق قانونی و معمول قابل انتساب به اشخاص نیستند. یعنی نمی شود گفت دادگاه می پذیرد 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 اصلی ترین کار اثبات این داده پیامها بر عهده ضابطان تخصصی یعنی پلیس فضای تبادل اطلاعات در جرایم معمولی از قبیل کلاهبرداریهای الکترونیکی، 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 الکترونیکی و روانشناسی است، مرجع اصلی داده پیام صادر شده را شناسایی و سعی در اثبات انتساب داده پیام به متهمان می کنند. مانند آن که با روشهای فنی نفوذ به ابزار الکترونیکی طرف مقابل، قادر به شناسایی مکان فیزیکی اتصال به اینترنت فرد و شماره منحصر به فرد اتصال او (IP) می شوند یا با زیرپاکشی، تله گذاری و مانتیورینگ دقیق و تحلیل داده های پیام های 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 می گذارند.

در حقیقت، بدون ترفندهای پلیسی و فنون خاصی که به کار گرفته شده و در نهایت منجربه شناسایی و اخذ اقرار از متهم می شوند، 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 تکرارشوندگی 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 اولا فرد شناسایی شده باشد ثانیا انتساب این پیام را انکار نکند ثالثا 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 تقریبا 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 عموما چنین آرایی در مراحل بعدی اعتراض از جمله تجدیدنظر نقض می شوند چون لزوما 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 درهیچ 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 کاملا معلومی است و در آنها، دلایل الکترونیکی از مانند اسکرین شات نیست.