گزارش یک

امیرحسین صفدری*

جلوتر بودن کلاهبرداران از قانون در سایت‌های متفرقه!

برخی کلاهبرداری‌های مجازی آنقدر پیچیده شده که قانون جرائم رایانه‌ای هم آنها را پیش‌بینی نمی‌کرد

در سال‌های اخیر جرائم تازه‌ای به حوزه کلاهبرداری اینترنتی اضافه شده است. قوانینی که در این حوزه تدوین می‌شوند باید قدرت به‌روز شدن داشته باشند، هرچند قانونگذار در جرائم رایانه‌ای دید کلی دارد و تصمیم‌گیری نهایی با قاضی است.

کلاهبرداری به زبان خیلی ساده فریب دادن افراد به روش‌های مختلف و گرفتن مال یا هر چیز دیگری از آنهاست. کلاهبرداری چه در فضای مجازی، چه در فضای حقیقی جامعه جرم محسوب می‌شود و مجازات سنگینی برای کلاهبرداران به همراه دارد. کلاهبرداری‌ها معمولاً بر پایه عدم‌آگاهی و طمع افراد اتفاق می‌افتد و کلاهبرداران از همین مسئله به خوبی بهره می‌برند و در نهایت با گرفتن پول، سرمایه و اعتماد افراد از آنها سوءاستفاده‌های غیرقابل جبرانی می‌کنند.

باافزایش روزافزون کاربران فضای مجازی متأسفانه این روزها در جامعه شاهد این هستیم که آمار کلاهبرداری‌ها در فضای مجازی افزایش چشمگیری داشته است و کلاهبرداران سودجو از طریق روش‌های مختلف و زیرکانه مردم را فریب می‌دهند و آنها را قربانی کلاهبرداری می‌کنند.

کلاهبرداری به بهانه برنده شدن در قرعه‌کشی‌ها

رایج‌ترین روش کلاهبرداری که از زمان‌های خیلی دور هم وجود داشته و امروزه هم در فضای مجازی افزایش زیادی پیدا کرده است، کلاهبرداری به بهانه برنده شدن در بانک، قرعه‌کشی برنامه‌های رادیویی و تلویزیونی، کمک هزینه سفر به کربلا، مشهد و خرید وسایل است، به عنوان مثال افراد سودجو معمولاً وقتی با شما تماس می‌گیرند از شما می‌خواهند اطلاعات کارت بانکی خود را جهت دریافت جایزه خود بدهید یا پای دستگاه عابر بانک بروید یا از حساب خود موجودی دریافت کنید یا تاریخ انقضای کارت بانکی خود را بگویید یا رمزی را که برای شما ارسال شده است به آنها بدهید یا رمز دوم خود را بدهید یا مشخصات هویتی خود را بگویید یا cvv2 کارت بانکی خود را اعلام کنید.

چنانچه هر شخصی بخواهد برای شما پولی واریز کند که این پول اعم از جایزه باشد یا پاداش یا هر پول دیگری، شما فقط شماره کارت یا شماره حساب خود را باید بدهید.

کلاهبرداری از طریق ساخت صفحات جعلی افراد

روش رایج دیگر که در فضای مجازی این روزها افزایش چشمگیری داشته سوءاستفاده از هویت اشخاص است. این کار از طریق اپلیکیشن‌های موجود اعم از اینستاگرام، تلگرام، واتس‌آپ و دیوار انجام می‌شود. در این نوع از کلاهبرداری‌ها فرد سودجو یک صفحه جعلی با نام، عکس و هویت یک شخص دیگر می‌سازد و از این طریق فرد سودجو خود را جای شخص دیگری جا می‌زند و اصولاً به اسم آن فرد از دیگران درخواست پول می‌کند یا سوءاستفاده‌های دیگری انجام می‌دهد که باعث متضرر شدن آن شخص می‌شود.

قانونگذار ما مطابق ماده ۱۶ قانون جرائم رایانه‌ای به صراحت تمام به این افراد سودجو می‌گوید: هرکس به وسیله سیستم‌های رایانه‌ای یا مخابراتی، فیلم یا صوت یا تصویر دیگری را تغییر دهد یا تحریف کند و آن را منتشر یا با علم به تغییر یا تحریف منتشر کند، به نحوی که عرفاً موجب هتک حیثیت او شود، به حبس از ۹۱ روز تا دو سال یا جزای نقدی از ۵ تا ۴۰ میلیون ریال یا هر دو مجازات محکوم خواهد شد.

کلاهبرداری اینترنتی به بهانه خرید اکانت بازی‌های آنلاین

از آنجا که برخی از جوانان و نوجوانان درگیر بازی‌های آنلاین هستند، گاهی اوقات دست به خرید و فروش اکانت بازی‌های آنلاین می‌زنند و چون اطلاعات کافی ندارند، متأسفانه قربانی کلاهبرداری اینترنتی از این طریق می‌شوند.

شیوه این نوع از کلاهبرداری‌ها به این شکل است که افراد سودجو با ترفندهای زیرکانه خود از جوانان و نوجوانان مبالغ هنگفتی جهت فروش اکانت بازی درخواست می‌کنند. پس از واریز مبلغ مورد نظر ارتباط‌شان را با مالباخته قطع می‌کنند و به همین راحتی شما قربانی کلاهبرداری اینترنتی شده‌اید.

این روزها خرید و فروش اکانت بازی‌های رایانه‌ای در فضای مجازی به یک کار معمولی و ساده تبدیل شده است، به طوری که برخی کاربران با رساندن بازی به مراحل بالا اقدام به فروش اکانت بازی خود می‌کنند اما افراد سودجو با سوءاستفاده از این موضوع دست به کلاهبرداری می‌زنند و پس از دریافت وجه از تحویل دادن اکانت بازی خودداری می‌کنند.

نوجوانان و جوانانی که درگیر بازی‌های آنلاین هستند و قصد خرید یا فروش اکانت خود را دارند اولاً تا جایی که امکان دارد از خرید و فروش اکانت بازی خود و دیگران خودداری کنند. اگر هم زمانی خواستید اقدام به خرید و فروش کنید، هروقتی که پول را به حساب فروشنده واریز کردید و رمز عبور اکانت را گرفتید، سریعاً تمامی مشخصات را تغییر دهید، چراکه ممکن است این افراد سودجو آن اکانت را همزمان به چندین نفر فروخته باشند و از این طریق شما دیگر هیچ کاری نمی‌توانید انجام دهید و قربانی کلاهبرداری شده‌اید.

متأسفانه این روزها اعتیاد به بازی‌های اینترنتی و بازی‌های آنلاین سبب شده است مشکلات زیادی برای افراد در خانواده و جامعه رخ دهد. در خصوص دانلود این نوع از بازی‌ها حتماً به سایت‌های معتبر یا اپلیکیشن‌های معتبر رجوع کنید.

افراد سودجو و کلاهبردار با انتشار نسخه‌های جعلی بازی‌های آنلاین و اینترنتی حاوی محتوای ویروس و بدافزار که اغلب هم رایگان است، قصد آسیب رساندن به سامانه‌های رایانه‌ای و گوشی‌های شما را دارند. از همین طریق ممکن است موبایل شما یا سیستم رایانه‌ای شما را هک کنند و اطلاعات شما را به سرقت ببرند، پس به شدت مراقب باشید تا قربانی کلاهبرداری و سرقت اینترنتی نشوید

کلاهبرداری اینترنتی از طریق نصب نرم‌افزارهای مختلف

از آنجا که برخی نرم‌افزارها و اپلیکیشن‌ها در کشور ما بنا به دلایلی فیلتر هستند، افراد برای اینکه بتوانند از این نرم‌افزارها استفاده کنند باید از فیلترشکن یا همان vpn استفاده کنند.

برخی کلاهبرداری‌های اینترنتی از طریق نصب کردن همین فیلترشکن‌ها صورت می‌گیرد. این افراد سودجو از این طریق می‌توانند به راحتی و به سرعت به اطلاعات شخصی و خصوصی شما دسترسی پیدا و از این طریق به شما آسیب‌های جبران‌ناپذیری را وارد کنند.

آمارها نشان می‌دهد نوجوانان زیادی از طریق نصب همین فیلترشکن‌ها مورد سوءاستفاده قرار می‌گیرند چراکه این نوجوانان نسبت به معتبر بودن یا نامعتبر بودن آن فیلترشکن آگاهی کافی و لازم را ندارند و ممکن است فیلترشکنی را نصب کنند که معتبر نباشد.

کلاهبرداران حرفه‌ای با ارسال پیامک و لینک‌های آلوده یا هنگام نصب و اجرای آن فیلترشکن یا نرم‌افزار از کاربر می‌خواهند برخی دسترسی‌ها را به آنها بدهد تا برنامه اجرا شود. کاربر هم که می‌خواهد از آن نرم‌افزار استفاده کند، به ناچار قبول می‌کند و این اجازه را می‌دهد و از همین طریق به راحتی قربانی کلاهبرداری اینترنتی می‌شود.

کلاهبرداری از پژوهشگران به بهانه کار علمی پژوهشی

در این روش از کلاهبرداری، افراد سودجو از دانشجویان و پژوهشگران به بهانه ترجمه ارزان‌قیمت مقالات، مقاله‌نویسی، پایان‌نامه‌نویسی، پذیرش تضمینی از مجلات علمی پژوهشی یا پذیرش از مجلات ISI کلاهبرداری می‌کنند.

کلاهبرداران ابتدا مبلغی به عنوان بیعانه می‌گیرند و در فضای مجازی قول و قرار انجام امور را می‌دهند. مثلاً قرار می‌شود کار در شبکه‌های اجتماعی پیگیری و تحویل شود. در نهایت هیچ‌گونه خدماتی هم ارائه نمی‌شود و از این طریق آنها را در برخی موارد قربانی کلاهبرداری می‌کنند، در برخی از موارد هم با ارائه مقالات جعلی و کاملاً کپی‌شده از دیگر نویسندگان باعث می‌شوند اعتبار علمی آن دانشجو یا پژوهشگر هم از بین برود. در این خصوص قانون جرائم رایانه‌ای دیدگاه خاصی ندارد و همان قوانین کلی حاکم است و علم قاضی است که پرونده را جهت می‌دهد.

کلاهبرداری به بهانه خرید و فروش حواله‌های خودرو

این روزها بحث خرید و فروش حواله‌های خودرو به شدت داغ شده است و افراد زیادی دست به خرید و فروش این حواله‌ها می‌زنند که همین امر هم باعث شده است عده‌ای از افراد سودجو دست به کلاهبرداری بزنند. در این روش از کلاهبرداری افرادی که به دروغ خود را برنده حواله خودرو معرفی می‌کنند، ابتدا اعلام می‌کنند حواله خودروی مورد نظر را زیر قیمت بازار به فروش می‌رسانند. در گام بعدی شما را ترغیب می‌کنند که مبلغی را به عنوان بیعانه برای آنها واریز کنید و پس از واریز پول دیگر پاسخگوی شما نیستند و به همین سادگی و راحتی شما قربانی کلاهبرداری شده‌اید.

کلاهبرداری از این روش خیلی زیرکانه انجام می‌شود و در همان جایی که شما فکر نمی‌کنید قربانی کلاهبرداری شوید، فریب می‌خورید و قربانی می‌شوید. بهتر است برای خرید حواله‌های خودرو به نمایندگی‌های معتبر مراجعه کنید و از مراجعه کردن به سایت‌های متفرقه و فاقد مجوز یا شبکه‌های اجتماعی یا افرادی که نمی‌شناسید جداً خودداری کنید و هرگز مبلغی جهت بیعانه برای آنها واریز نکنید.

کلاهبرداری از صاحبان مشاغل با رسیدهای جعلی

در حال حاضر نرم‌افزارهای مختلفی جهت استفاده در مشاغل مختلف طراحی شده است که کارکردهای متفاوتی دارد. نرم‌افزار جدیدی که تحت عنوان رسیدساز طراحی شده است کاسبان را قربانی کلاهبرداری می‌کند، به این صورت که این نرم‌افزار تقلبی و جعلی اقدام به ساخت رسید بانکی جعلی می‌کند که عیناً شبیه رسیدهای واقعی است، در صورتی که آن رسید کاملاً جعلی است. بهتر است وقتی فردی که به شما بدهکار است به شما مراجعه کرد و رسید واریزی را به شما نشان داد، ابتدا به موجودی حساب خود نگاه کنید.

در صورتی که وجهی پرداخت شده بود به آن رسید اعتماد کنید و فریب این حرف‌ها را که ممکن است سامانه پیامکی بانک مشکل دارد و پیامک نیامده است، نخورید چراکه اگر تعارف کنید، ممکن است قربانی کلاهبرداری شوید.

کلاهبرداری به بهانه مشاهده ابلاغیه الکترونیکی دادگستری

یکی دیگر از کلاهبرداری‌های رایج در فضای مجازی که این روزها به شدت هم افزایش پیدا کرده کلاهبرداری به بهانه مشاهده ابلاغیه الکترونیکی است. مجرمان سایبری با ارسال پیامک و با جعل تارنماهایی مشابه تارنمای ثبت‌نام الکترونیک قوه قضائیه از کاربران فضای مجازی کلاهبرداری می‌کنند. این پیامک‌ها حاوی مطالبی همانند مشاهده ابلاغیه، حکم جلب شما صادره و علیه شما شکوائیه ثبت شده، است. کاربران فضای مجازی به دلیل مشاهده چنین متنی دچار استرس می‌شوند و متأسفانه از سر کنجکاوی روی لینک مورد نظر کلیک می‌کنند.

در این مرحله مجرمان خطرناک شما را به یک درگاه اینترنتی پرداخت وجه متصل می‌کنند و شما با وارد کردن اطلاعات حساب خود قربانی کلاهبرداری اینترنتی می‌شوید.

قانونگذار ماده ۱۳ قانون جرائم رایانه‌ای را به جرم کلاهبرداری اینترنتی اختصاص داده و چنین آورده است: هرکس به طور غیرمجاز از سامانه‌های رایانه‌ای یا مخابراتی با ارتکاب اعمالی از قبیل وارد کردن، تغییر، محو، ایجاد یا متوقف کردن داده‌ها یا مختل کردن سامانه، وجه یا مال یا منفعت یا خدمات یا امتیازات مالی برای خود یا دیگری تحصیل کند، علاوه بر رد مال به صاحب آن به حبس از یک تا پنج سال یا جزای نقدی از ۲۰ میلیون ریال تا ۱۰۰ میلیون ریال یا هر دو مجازات محکوم خواهد شد. نکته مهم در خصوص مواجهه با پیامک‌های جعلی اینچنینی این است که شما باید بدانید پیامک‌های دریافتی از جانب قوه قضائیه با سرشماره «adliran» است و هرگز با شماره شخصی ارسال نمی‌شود. پیامک‌های ارسالی توسط قوه قضائیه فاقد لینک الکترونیکی است و شما برای مشاهده ابلاغیه خود در سامانه «ثنا» هیچ پولی نباید پرداخت کنید.

*نویسنده و پژوهشگر علم حقوق

گزارش ۲

علیرضا سزاوار

چالش قانون با جرائم سایبری

جرائم فضای مجازی در بخش کلاهبرداری‌های رایانه‌ای با شگردهای گوناگون در حال گسترش است

استفاده از فیلترشکن‌ها بستری را فراهم می‌کند تا مجرمان از این فضا بیشتر استفاده کنند و راحت‌تر بتوانند اقدامات کلاهبرداری خودشان را انجام دهند. شناسایی متهم از طریق فیلترشکن‌ها کار بسیار سختی است، چون دسترسی به IP یک مقدار مشکل می‌شود، البته سامانه‌ای در پلیس «فتا» ناجا به نام سامانه شمس وجود دارد که VPN را رصد و متهم را شناسایی می‌کند.

رشد سریع و بسیار زیاد جرائم سایبری در کشور در حالی است که قانونگذار برای مقابله با این پدیده در سال ۸۸ قانون جرائم رایانه‌ای و متعاقب آن قانون دادرسی الکترونیکی را سال ۹۳ به تصویب رسانده است.

در گسترش جرائم فضای مجازی دلایل متعددی مثل افزایش روزافزون کاربران فضای مجازی، پایین بودن آگاهی کاربران و بی‌توجهی بسیاری از آنان به رعایت نکات امنیتی، بیکاری، سهولت ارتکاب جرم و پنهان ماندن مجرمان، مشکلات فرهنگی و اخلاقی کاربران نقش دارند اما قطعاً نقش قانون و اجرای آن بیش از همه عوامل یاد شده در مقابله با این پدیده، مؤثر است.

استناد قانون به مدارک الکترونیکی

مدارک الکترونیکی طبق مفاد قانون تجارت الکترونیک و موادی از قانون آیین دادرسی کیفری به رسمیت شناخته شده است. ماده ۶ قانون تجارت الکترونیک مقرر داشته است: «هرگاه وجود یک نوشته از نظر قانون لازم باشد، «داده پیام» در حکم نوشته است.»

همینطور ماده ۷ آن قانون بیان می‌کند: «هرگاه قانون، وجود امضا را لازم بداند، امضای الکترونیکی مکفی است»، البته با شرایط خاصی که در آن قانون در نظر گرفته شده است، به عنوان مثال امضای الکترونیکی باید شرایط خاصی داشته باشد که سند الکترونیکی که با آن امضا شده است، حکم سند رسمی را پیدا کند.

ماده ۶۸۵ قانون آیین دادرسی کیفری در فصل مربوط به آیین دادرسی جرائم رایانه‌ای نیز بیان کرده است: چنانچه داده‌های رایانه‌ای توسط طرف دعوی یا شخص ثالثی که از دعوی آگاهی ندارد، ایجاد یا پردازش یا ذخیره یا منتقل شود و سامانه رایانه‌ای یا مخابراتی مربوط به نحوی درست عمل کند که به صحت و تمامیت، اعتبار و انکارناپذیری داده‌ها خدشه وارد نشود، قابل استناد است.» بنابراین از نظر قانونی مشکلی برای استناد به این ادله الکترونیکی وجود ندارد، البته آیین‌نامه‌هایی در این زمینه پیش‌بینی شده است که هنوز برخی آیین‌نامه‌های مربوط به تصویب نرسیده‌اند.

متنوع شدن جرائم در فضای مجازی این سؤال را مطرح می‌کند که قانون جرائم رایانه‌ای و قانون دادرسی الکترونیکی، آن گونه که باید جامع و بازدارنده هستند؟ برخی کارشناسان معتقدند قانون در حوزه جرائم رایانه‌ای دچار خلأ است، برخی هم معتقدند مشکل به ضعف در اجرا و نظارت بر حسن اجرای قانون برمی‌گردد.

قوانین باید قدرت به‌روز شدن داشته باشند

معاون شرکت مخابرات ایران و کارشناس فضای مجازی در این خصوص به قدس آنلاین گفت: جرائم رایانه‌ای مقوله تازه‌ای است که اصولاً تشخیص همه جرائم و تعیین نوع مجازات برای همه آنها از سوی بیشتر کشورهای دنیا به درستی دیده نشده است. باید توجه داشته باشیم که مثلاً در دو سال اخیر چقدر جرائم تازه‌ای در این حوزه اضافه شده است، به همین دلیل شاید لازم باشد قوانینی که در این حوزه تدوین می‌شوند، قدرت به‌روز شدن داشته باشند.

داود زارعیان افزود: قانون جرائم رایانه‌ای در دهه ۸۰ تصویب شده، البته این قانون یک قانون نسبتاً جامعی است و خیلی از مسائل این حوزه مثل محرمانه بودن اطلاعات، جاسوسی، سرقت اطلاعات، هک اطلاعات، نشر اکاذیب، حریم خصوصی افراد و جرائم سازمان‌یافته اقتصادی و اجتماعی جعل داده‌ها را دربرمی‌گیرد، اما اصولاً قوانینی که در حوزه فناوری نوین اطلاعاتی تدوین می‌شوند، هر سال مورد بازنگری قرار می‌گیرند، چراکه جرائم تازه‌ای بر جرائم قبلی اضافه می‌شوند، مثلاً اگر قانون جرائم یارانه‌ای در سال ۹۶ تصویب شده باشد، در همین سه سال می‌بینیم جرائم جدیدی مثل بیت کوین اضافه‌شده، در حالی که قانونگذار در این مورد یا موارد مشابه دیگر سکوت کرده است.

وی از ضرورت اصلاح قوانین جرائم رایانه‌ای در هر سال سخن گفت و افزود: حداقل باید به قانون مربوط الحاقیه بزنیم.

بازنگری در حوزه فنی و حقوقی

زارعیان با اشاره به اینکه در حوزه جرائم رایانه‌ای علاوه بر موضوع یادشده با دو مسئله دیگر مواجه هستیم، تصریح کرد: یکی اینکه کشف و شناسایی برخی جرائم رایانه‌ای به سادگی ممکن نیست، چون افراد از راه‌های مختلف از جمله جابه‌جایی‌های زیاد و با آی‌پی‌های مختلف این کار را انجام می‌دهند و بعد هم ممکن است فردی که مجرم اصلی است، پیدا نشود. مشکل دوم این است که همه افرادی که از نظر مادی یا معنوی در این حوزه مورد تجاوز قرار می‌گیرند، اطلاع ندارند چگونه باید مشکل خود را پیگیری کنند، بنابراین یک بخشی از جرائم اتفاق می‌افتد و به همین شکل از آن عبور می‌شود، به همین دلیل شاید لازم باشد هر ساله هم در حوزه فنی و هم در حوزه حقوقی بازنگری‌هایی داشته باشیم.

وی در خصوص این پرسش که آیا در اجرای قانون جرائم رایانه‌ای و نظارت بر حسن اجرای آن مشکلات خاصی وجود دارد، گفت: اصولاً در قوانین جدید تا مدت‌ها شاهد این گونه مسائل و مشکلات هستیم. همان‌طور که اشاره شد، ممکن است قانون برای برخی از جرائم، جرم‌انگاری نکرده باشد یا مجازات‌های لازم برای آن دیده نشده باشد، ضمن اینکه ممکن است برخی از وکلای دادگستری هم درک مناسبی از این جرائم نداشته باشند و نتوانند به خوبی از موکلان خود دفاع کنند، به هر حال الان در اجرای این قوانین مشکلاتی داریم، البته روند اجرای قوانین رو به بهبود است.

وی در همین زمینه می‌افزاید: در یک دهه اخیر تحولات خوبی در حوزه نیروی انتظامی و بخش‌های دیگر فناوری نوین اطلاعات ایجاد شده که شناسایی مجرمان فضای مجازی را ساده‌تر کرده و طبیعی است رسیدگی به جرائم این بخش هم سریع‌تر و بهتر انجام می‌شود.

مجازات سنگین برای مجرمان

این کارشناس حوزه فضای مجازی اگرچه معتقد است قانون جرائم رایانه‌ای در بسیاری از موارد بازدارندگی لازم را دارد اما معتقد است: این قانون در بعضی موارد مجازات‌های سنگین حتی حبس تا ۱۵ سال را برای مجرمان پیش‌بینی کرده است، با این وجود به نظر می‌رسد با توجه به شرایط و به منظور اثرگذاری بیشتر، همچنان باید به سمت مجازات‌های جدی‌تر نقدی حرکت کنیم، چون برخی مجازات‌های نقدی پیش‌بینی‌شده در قانون جرائم رایانه‌ای پایین است، مثلاً در جایی که مجازات حبس به مدت دو سال پیش‌بینی شده، جریمه نقدی این مدت را تا ۵ میلیون تومان دیده است که به نظر می‌رسد خیلی بازدارنده نیست.

فرصتی برای بازنگری قانون جرائم رایانه‌ای نیست

سرپرست سابق دادسرای ویژه جرائم رایانه‌ای و فناوری ارتباطات هم در این خصوص به قدس آنلاین گفت: سال ۸۰ وقتی لایحه جرائم رایانه‌ای در دستور کار مجلس قرار گرفت، حدود ۸۰ ماده داشت اما با ۵۶ ماده به تصویب رسید، یعنی این قانون همان موقع پاسخگوی نیازها و جرائمی که رخ می‌داد، نبود، این در حالی است که هر روز که می‌گذرد جرائم رایانه‌ای پیچیده‌تر و شکل و نوع آن عوض می‌شود. الان هم که جای خود دارد. به هر حال قانون یاد شده، قطعاً پاسخگوی نیازهای امروز نیست.

رضا جعفری در همین زمینه افزود: برخی مسئولان، مقداری نسبت به مباحث جرائم رایانه‌ای بی‌تفاوت هستند، چون هدفی که ما از تشکیل دادسرای ویژه مبارزه با جرائم رایانه‌ای و فناوری ارتباطات داشتیم، هدف خوبی بود، کارهایی هم انجام شد اما قدری مورد کم‌لطفی قرار گرفت، یعنی چندان به این مجموعه اهمیت داده نشد، در نتیجه دادسرای جرائم رایانه‌ای به خوبی جا نیفتاد. در واقع دادسرای جرائم رایانه‌ای در کشور وجود دارد اما جایگاه واقعی خودش را هنوز پیدا نکرده است و نمی‌تواند آن‌طور که باید به صورت تخصصی و ویژه کار کند تا جایی که الان همه دادسراهای موجود در کشور صلاحیت رسیدگی به جرائم رایانه‌ای را دارند، این در حالی است که پلیس فتا که پس از دادسرای جرائم یارانه‌ای یا همزمان با آن فعالیتش را شروع کرد به خوبی جا افتاد، چون متولیانش اهمیت آن را فهمیدند و اهتمام لازم را به خرج دادند تا به خوبی در ایفای نقش خود جا افتاد.

دادسرای جرائم رایانه‌ای در کشور وجود دارد اما جایگاه واقعی خودش را هنوز پیدا نکرده است و نمی‌تواند آن‌طور که باید به صورت تخصصی و ویژه کار کند تا جایی که الان همه دادسراهای موجود در کشور صلاحیت رسیدگی به جرائم رایانه‌ای را دارند

اطلاع‌رسانی در این زمینه ضعیف است

سرپرست سابق دادسرای ویژه جرائم رایانه‌ای با تأکید بر اینکه قانون جرائم رایانه‌ای نیاز به یک بازنگری اساسی دارد، تصریح می‌کند: نه تنها قانون جرائم رایانه‌ای دچار ضعف و خلأهای قانونی است بلکه در اجرا نیز مشکلاتی دارد. در واقع خود این قانون مشکلات مختلفی دارد، به‌ویژه اینکه به‌روز نیست، در حوزه اجرای آن هم به نحوی دچار مشکل هستیم، صلاحیت رسیدگی به جرائم رایانه‌ای نیز به همه دادسراها داده شده است. به هر حال این قانون یک بازنگری اساسی می‌خواهد اما به نظر می‌رسد دست‌اندرکاران فعلاً برای این مقوله فرصت ندارند.

وی در پاسخ به این پرسش که آیا مجازات‌های پیش‌بینی‌شده در قانون یادشده بازدارندگی لازم را دارند، می‌گوید: خیلی از مجازات‌هایی که در قانون پیش‌بینی می‌شوند، بازدارندگی ندارند، چه از لحاظ کیفی و چه از نظر کمی. بحث قانون جرائم رایانه‌ای هم به همین صورت است. قطعاً این قانون بازدارندگی لازم را ندارد، اگر داشت که این همه کلاهبرداری‌های اینترنتی انجام نمی‌شد، البته مقداری مردم ما هم نسبت به این جرائم آگاه نیستند و اطلاع‌رسانی در این زمینه ضعیف است.

جرم با فناوری همگام می‌شود

یک حقوقدان و کارشناس مسائل حقوق رسانه هم در این زمینه نظر متفاوتی دارد و بر این باور است قوانین در این حوزه به اندازه کافی وجود دارد و علت وقوع زیاد جرائم در این حوزه را امکان گسترده پنهانکاری می‌داند.

کامبیز نوروزی در این خصوص به خبرگزاری برنا گفت: رفتارهای ناهنجار نیز به همین علت در فضای مجازی بیشتر وجود دارد. وقتی شخص با مشخصات جعلی و نامشخص می‌تواند وارد این فضا شود، قطعاً راحت‌تر می‌تواند مرتکب جرم و حرکات خشونت‌آمیز شود.

این وکیل پایه یک دادگستری افزود: جرم همراه با زندگی و فناوری متحول می‌شود. فضای مجازی قابلیت‌های زیادی دارد و این مسئله سبب شده است وقوع جرائم نیز پیچیده‌تر شود. امروزه شاهد هستیم ابزاری همچون بیت‌کوین نیز به‌وجود آمده که حتی ردیابی پول را نیز سخت کرده است. این حقوقدان بر این باور است که قوانین به قدر کافی وجود دارد. این طبیعت حوزه وب است که مسدود کردن تخلف در آن را سخت می‌کند، به شکلی که شاهد هستیم حتی حساب توئیتر شخصیت‌های برجسته ایالات متحده نیز هک شد و تمامی تشکیلات توئیتر نیز هنوز نتوانسته این مشکل را حل کند.

به عقیده وی، این سختی و پیچیدگی طبیعی وب است که کار برای مقابله با وقوع جرم در فضای مجازی را سخت کرده است. از سوی دیگر شاهد هستیم در دنیای واقعی جامعه ما محدودیت‌هایی اعمال می‌شود که بازتولید آن در فضای مجازی به شکل بدتری رقم می‌خورد.

گفتنی است قوانینی که سال‌ها قبل در خصوص جرائم رایانه‌ای تصویب شده‌اند، پاسخگوی نیازهای واقعی این فضا نیستند، حتی برخی قضات هم در گفت‌وگو با رسانه‌ها عنوان کرده‌اند که قانون جرائم رایانه‌ای که در سال ۱۳۸۸ تصویب شده هم در حال حاضر نقایص و نقاط ضعف فراوان دارد، یعنی برخی رفتارهای مجرمانه با اهمیت را که در فضای مجازی اتفاق می‌افتد، پوشش نمی‌دهد یا ضمانت اجرای ضعیف برای آن پیش‌بینی شده است.