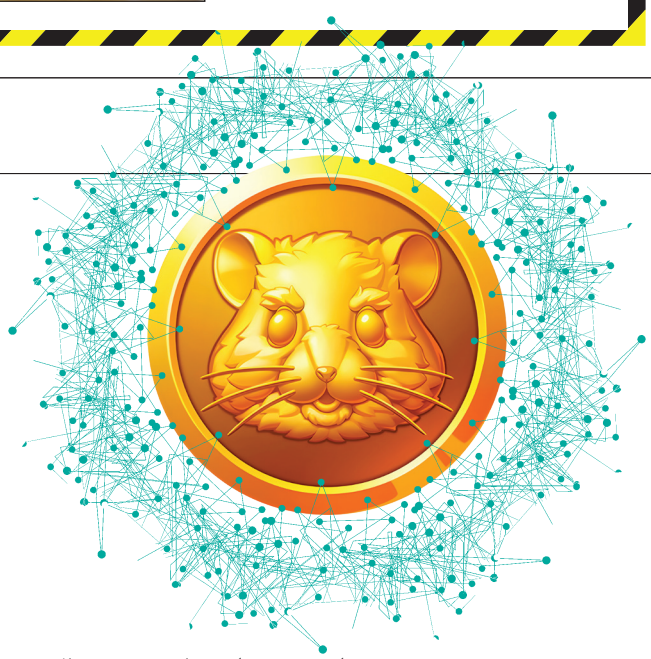
شکایت از کلاهبرداری ارز دیجیتال

برای شکایت از کلاهبرداری ارز دیجیتال ابتدا باید به دفاتر خدمات قضایی مراجعه و با طرح شکواییه، اقدام به ثبت آن کرد. دادسرا معمولا در این زمان تحقیقات را به پلیس فتا ارجاع داده و این نیرو با استفاده از زمینه‌های فنی خود، اقدام به جمع آوری ادله و مدارک خواهد کرد. اگر ارتباط در بستر فضای حقیقی باشد احتمال ردیابی کلاهبردار بیشتر است.

مجازات کلاهبرداری ارز دیجیتال

هر کس 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 ... تحصیل کند، مرتکب کلاهبرداری اینترنتی شده و علاوه بر رد مال به صاحب آن، به حبس از یک تا ۵ سال محکوم خواهد شد.



حقوقدان حوزه ارزهای دیجیتال در گفت‌وگو با «همشهری سرنخ» به بررسی ابعاد حقوقی بازی تازه در فضای مجازی پرداخته است

همستر محبوب کلاهبرداران

دنیای ارز دیجیتال با وجود همه مزیت‌هایی که برای کاربران و افزایش آزادی مالی آنان دارد، راه مناسبی هم در اختیار کلاهبرداران قرار داده تا بتوانند راحت‌تر از گذشته نقشه‌هایشان را عملی کرده و افراد ساده و ناآگاه را سرکیسه کنند. زینب ریاضت، وکیل دادگستری و عضو هیأت علمی دانشگاه تاکنون وکالت پرونده‌های زیادی با موضوع رمزارز و جرائم اقتصادی را برعهده داشته است. او در گفت‌وگویی به بررسی کلاهبرداری رمزارز شبکه‌ای پرداخته است.

فضای رمز ارز به‌خصوص رمزارزهای جدید و ناشناخته ممکن است مخاطرات و آسیب‌هایی به‌دنبال داشته باشد؟

زمانی که کاربران با استفاده از ارز دیجیتال روی یک برنامه ناشناس سرمایه‌گذاری می‌کنند، با توجه به اینکه بستر مالکیت پلت‌فرم نامشخص است و مالک هر کسی در هر جای دنیا می‌تواند باشد موضوع خطرناک به‌نظر می‌رسد. گاهی نیز ممکن است تا مقطعی هیچ هزینه‌ای از سوی کاربر صرف نشود اما در ادامه پس از اطمینان نسبی، فرد اموال خود را با برخی اقدامات بعدی مانند اجازه دسترسی به کیف پول از دست بدهد. بدین ترتیب باید گفت در دنیای مدرن امروز ظهور رمزارزها به گستردگی دامنه جرم کلاهبرداری کمک کرده است زیرا کلاهبرداران برای موفقیت و حفظ سودآوری از ناآگاهی قربانیان همواره استفاده کرده و روش‌های ارتکاب جرم را با مسائل جدید نوظهور سازگار می‌کنند و این نوآوری شناسایی برخی از کلاهبرداری‌ها و پیش‌بینی چگونگی کلاهبرداری را بسیار دشوار کرده است.

درباره رمزارز بیشتر توضیح دهید. مجرمان چطور در این فضا می‌توانند دست به کلاهبرداری بزنند؟

منظور از ارز مجازی گونه‌ای ابزار پرداخت و ابزار مبادله‌ای است که توسط برنامه رایانه‌ای خلق و کنترل می‌شود. اما ارز دیجیتال یک عبارت موسع از نظر حقوقی است و به ارزهایی که به‌صورت الکترونیکی ذخیره و منتقل می‌شوند گفته می‌شود. رمزارزهایی مانند بیت‌کوین تنها گونه‌ای ارز مجازی هستند و همه ارزهای مجازی رمز ارز نیستند اما بیت‌کوین به جهت گستردگی استفاده، نقطه آغاز یک نظم پولی نوین و یک مدل جایگزین برای سامانه پولی و مالی جهانی بوده است که موجب تغییر در ساختارهای اقتصادی دنیا شد.

تازه‌ترین اتفاق در این حوزه ماجرای ماین‌کردن ارز دیجیتال از طریق یک بازی به نام همبستر کامبت است که میلیون‌ها کاربر را جذب کرده است. این بازی چه آسیب‌هایی ممکن است در پی داشته باشد؟

همستر کامبت بستر مناسبی برای ارتکاب جرم فراهم کرده است. افرادی که در این بازی‌ها شرکت می‌کنند به طرق مختلف مانند هک اطلاعات از طریق لینک روبات همستر در بستر تلگرام ممکن است امنیت حساب کاربری خود را از دست بدهند این در حالی است که جرائم قابل پیش‌بینی در این بستر منحصر به هک اطلاعات نیست. حتی پس از لیست‌شدن یک ارز مشکوک و نامعتبر یا ارتباط با کیف پول کاربر هم نمی‌توان اطمینان داشت جرمی در کار نیست و همه‌چیز اطمینان‌بخش است.

در حال حاضر در سراسر جهان فقط 7 صرافی به شکل بسیار محدود ارز همستر را در کنار سایر رمزارزها لیست کرده‌اند و به‌نظر می‌رسد اعتبار این رمز ارز محل تردید جدی است.

حتی بر فرض اعتبار هم ارزهای مجازی توسط عموم دولت‌ها پشتیبانی نمی‌شوند و قاعده کلی ممنوعیت و یا نادیده‌انگاری است.

در چنین شرایطی چطور می‌شود به همستر کامبت اطمینان کرد؟

کارکرد قانونی و صحیح هر گونه رمز ارز نیازمند شناسایی و حمایت حاکمیت است که بستر آن وجود ندارد. تا جایی که حتی با توجه به اینکه معامله ارزهای دیجیتال براساس مقررات بانک مرکزی و هیأت وزیران در مبادلات داخلی رسمیت ندارد اما حتی توقیف و فروش آن به وسیله اجرای احکام نیز ممکن نیست. این البته در فرض دسترسی و شناسایی مرتکب است ولی متأسفانه در تمام دنیا با توجه به بستر رمز ارز مورد استفاده، چالش‌های شناسایی محل وقوع جرم و مجرم و همچنین قانون حاکم، اساسا ردیابی اموال و دسترسی به مرتکبان بسیار دشوار است و تاکنون پرونده بسیاری از کلاهبرداری‌های رمز ارز در دنیا به نتیجه مطلوب نرسیده است.

مهم‌ترین ترفندهایی که ممکن است کلاهبرداران سایبری با استفاده از آنها کاربران همستر کامبت را سرکیسه کنند چیست؟

موفقیت کلاهبرداری رمز ارز در ایران به جهت بسیاری از موانع و مشکلات اقتصادی و ارتباط با دنیا بیشتر از کشورهای دیگر است و در قالب رمز ارز تقلبی و فیک با وعده سود روزانه شگفت‌انگیز تا دسترسی غیرمجاز به کیف پول کاربران، جابه‌جایی غیرمجاز انواع دارایی‌های کاربران و یا به‌صورت طرح پانزی با زیرمجموعه‌گیری هرمی رخ می‌دهد تا اگر مثلا دوستی معرفی کنید ۲۰ درصد از سود روزانه او را نیز به‌دست آورید و حالا اگر دوست شما نفر دومی را هم دعوت کند، ۱۰ درصد از درآمد وی را هم کسب کنید و در نهایت بدین شکل دامنه جرم وسیع و کاربران نیز در آن سهیم می‌شوند.

آیا کلاهبرداری شبکه‌ای در قوانین کشور ما جرم‌انگاری شده و چه مجازات‌هایی برای افرادی که مرتکب کلاهبرداری به‌صورت شبکه‌ای می‌شوند درنظر گرفته شده است؟

در قانون تشدید مجازات مرتکبین ارتشا و اختلاس و کلاهبرداری، قوانینی به ارتکاب گروهی و شبکه‌ای جرائم موضوع این قانون اختصاص داده‌اند. به موجب ماده ۴ قانون تشدید، کسانی که با تشکیل یا رهبری شبکه چند نفری به کلاهبرداری مبادرت ورزند به استرداد اموال مذکور، جزای نقدی معادل مجموع آن اموال و انفصال دائم از خدمات دولتی و حبس از ۱۵ سال تا ابد محکوم می‌شوند و درصورتی که مصداق مفسد فی‌الارض باشند مجازات آنها، مجازات مفسد فی‌الارض خواهد بود. قانونگذار در ماده ۱۳۰ قانون مجازات اسلامی نیز مجازات سردستگی را تعیین کرده است و با توجه به ماده مذکور به‌رغم اینکه سال‌ها از زمان تصویب قانون تشدید می‌گذرد در مورد موضوع مذکور اختلاف جدی در آرای محاکم دادگستری و شعب دیوان عالی کشور مشاهده می‌شود.

درباره همستر کامبت ابهامات زیادی وجود دارد. این بازی در بستر فضای مجازی و شبکه‌های اجتماعی است. به‌نظر شما این بازی ممکن است در ادامه دچار چه آسیب‌هایی شود؟

هنوز چگونگی وقوع جرایم در بستر بازی‌های جدید مشخص نیست و اگرچه مواردی از کلاهبرداری به‌صورت تبلیغات در اینستاگرام یا تلگرام توسط پلیس فتا تاکنون گزارش شده اما ناظر به افرادی بوده که علی‌الظاهر در ایران ضمن فریب قربانیان از طریق مانور متقلبانه ادعای فروش کارت‌های بازی یا ارائه طریق روش‌های دریافت سکه‌های میلیونی را داشتند که اگر این اقدامات به‌صورت شبکه‌ای انجام شده باشد مصداق کلاهبرداری شبکه‌ای است و اما آنچه بسیار خطرناک به‌نظر می‌رسد سازماندهی تشکیلاتی طراحان این بازی به‌ویژه پس از اجازه دسترسی کاربران به بازی برای ارتباط با کیف پول الکترونیکی‌شان است که احتمالات جدی برای وقوع کلاهبرداری را تقویت می‌کند.

با وجود همه خطرات احتمالی چنین بازی‌هایی اما چرا همستر کامبت با این سرعت در کشورمان فراگیر شده است؟

پیشنهاد دعوت ۳ دوست به بازی با وعده اعطای سکه که منجر به گسترش چشمگیر کاربران بازی همستر شده است. این از مواردی است که در بسیاری از پرونده‌های کلاهبرداری‌های رمز ارز مشاهده می‌شود. درحالی که هیچ رمز ارزی را با تلفن همراه نمی‌توان ماین کرد؛ ادعای اینکه بدون دریافت هیچ پولی این بستر در بازی وجود دارد عجیب به‌نظر می‌رسد و دعوت دوستان نیز حداقل بستر دسترسی غیرمجاز به اطلاعات و فروش دیتا را فراهم می‌آورد.

در چنین شرایطی توصیه شما به‌عنوان یک حقوقدان به کاربران این بازی چیست؟

در دنیای رمز ارز مهم‌ترین کار ایمن‌سازی هویت آنلاین است و صرف‌نظر از اینکه هنوز تبعات اقدامات خطرآفرین بازی همستر مشخص نشده است حتی درصورت وقوع جرم نیز با توجه به بستر ارتکابی جرم در تلگرام امکان طرح شکایت و پیگیری مرتکبان بسیار دشوار و تقریباً بی‌نتیجه به‌نظر می‌رسد و اگرچه امکان تنظیم شکایت و پیگیری موضوع از طریق پلیس فتا و دادسرا وجود دارد و توصیه می‌شود اما با توجه به چالش‌های رسیدگی به پرونده‌های مشابه در دادسرای جرائم رایانه‌ای پیشنهاد می‌شود همه جوانب احتیاطی توسط شهروندان لحاظ شود تا موجب پشیمانی و خسارت برایشان نشود.