از شناسایی کلاهبردار تا بازگشت پول

وقتی پول مردم با یک کلیک ناپدید می‌شود

«جوان» در گفت‌وگو با اساتید علم حقوق، مسئولیت بانک‌ها، پلتفرم‌های اینترنتی و شرکت‌های پرداخت در برابر قربانیان کلاهبرداری را بررسی کرده است

■ نیره ساری

این روزها می‌شود تمام دارایی یک فرد، نه با یک سرقت فیزیکی و نه با ورود سارقی به خانه، بلکه با چند لمس ساده روی صفحه تلفن همراه از دست برود. پیامکی که ظاهری رسمی دارد، لینکی که شبیه درگاه پرداخت بانکی طراحی شده یا آگهی فروشی که در نگاه اول هیچ نشانی از فریب‌کاری ندارد، می‌تواند نقطه آغاز ماجرایی باشد که در چند دقیقه، حساب بانکی یک شهروند را خالی کند. قربانی می‌ماند و حسابی که موجودی آن به صفر رسیده، شماره‌ای که دیگر پاسخگو نیست و پرسشی که گاهی ماه‌ها و حتی سال‌ها بی‌جواب باقی می‌ماند. پول من را چه کسی باید برگرداند؟

■■■

گسترش بانکداری الکترونیک، خریدوفروش اینترنتی و خدمات پرداخت آنلاین، زندگی روزمره مردم را آسان‌تر کرده است. امروز برای خرید یک کالا، پرداخت قبض، انتقال وجه یا انجام بسیاری از امور مالی، نیازی به مراجعه حضوری به بانک نیست، اما همین سهولت، در کنار فرصت‌های تازه اقتصادی، میدان گسترده‌تری نیز برای فعالیت مجرمان سایبری فراهم کرده است. کلاهبرداری اینترنتی دیگر محدود به چند شگرد ناشناخته نیست؛ از درگاه‌های جعلی و پیامک‌های فیشینگ گرفته تا آگهی‌های ساختگی، حساب‌های اجاره‌ای و فریب شهروندان در شبکه‌های اجتماعی، هر روز شکل‌های تازه‌ای از دستبرد به دارایی مردم را رقم می‌زند. در چنین شرایطی، مسئله فقط شناسایی و مجازات کلاهبردار نیست. پرسش مهم‌تر این است در زنجیره‌ای که از ارتکاب جرم تا انتقال پول و گاه ناپدیدشدن رد آن امتداد پیدا می‌کند، هر یک از بازیگران چه مسئولیتی دارند؟ آیا شهروندی که قربانی یک عملیات فریب‌کارانه شده، باید تمام تبعات مالی آن را به دوش بکشد؟ بانک‌ها تا چه اندازه در قبال امنیت حساب مشتریان خود مسئولند؟ پلتفرم‌هایی که بستر انتشار آگهی و ارتباط خریدار و فروشنده را فراهم می‌کنند، در برابر فعالیت کاربران متخلف چه تکلیفی دارند؟

در نگاه نخست، ممکن است پاسخ ساده به نظر برسد. مجرم باید شناسایی و مجازات شود و خسارت قربانی نیز از او دریافت شود، اما واقعیت پرونده‌های کلاهبرداری اینترنتی به این سادگی نیست. گاهی وجه سرقت‌شده در فاصله‌ای کوتاه میان چند حساب بانکی جابه‌جا می‌شود، گاهی از حساب‌های اجاره‌ای برای پنهان کردن مسیر انتقال پول استفاده می‌شود و گاهی نیز قربانی پس از اطلاع از برداشت غیرمجاز، با این واقعیت مواجه می‌شود که بخش مهمی از دارایی‌اش دیگر در حساب اولیه وجود ندارد.

در این میان، نقش شبکه بانکی و پرداخت اهمیت ویژه‌ای پیدا می‌کند. بانک‌ها و ارائه‌دهندگان خدمات پرداخت، زیرساخت انجام تراکنش‌های مالی را در اختیار شهروندان قرار می‌دهند و طبیعی است که امنیت این زیرساخت‌ها به یکی از مهم‌ترین انتظارات مشتریان تبدیل شود. البته صرف وقوع کلاهبرداری، به معنای مسئولیت خودکار بانک نیست. باید بررسی شود که آیا در فرایند ارائه خدمت، احراز هویت، حفاظت از اطلاعات یا اجرای تراکنش‌ها قصور و تخلفی رخ داده است یا خیر و آیا میان این قصور احتمالی و خسارت واردشده رابطه سببیت وجود دارد!

از سوی دیگر، نمی‌توان در همه پرونده‌ها نقش رفتار مشتری را نادیده گرفت. برای مثال، شرایط حقوقی فردی که بدون اطلاع از حسابش برداشت شده با کسی که اطلاعات بانکی خود را در اختیار کلاهبردار قرار داده یا رمز یک‌بارمصرف را به درخواست او ارسال کرده، لزوماً یکسان نیست. با این حال، حتی در چنین مواردی نیز بررسی دقیق چگونگی وقوع جرم و وظایف قانونی سایر بازیگران ضروری است. مسئولیت حقوقی را نمی‌توان صرفاً با یک قضاوت کلی درباره بی‌احتیاطی قربانی تعیین کرد.

وجه دیگر ماجرا به پلتفرم‌های اینترنتی و بسترهای خریدوفروش آنلاین مربوط می‌شود. بسیاری از معاملات روزمره مردم در فضایی انجام می‌شود که فروشنده و خریدار یکدیگر را نمی‌شناسند و اعتماد آنها تا حد زیادی به اعتبار بستر ارتباطی وابسته است. انتشار یک آگهی جعلی، استفاده از هویت غیرواقعی یا فعالیت حساب‌هایی که با هدف فریب کاربران ایجاد شده‌اند، می‌تواند شهروندان را در معرض خسارت قرار دهد. در اینجا پرسش مهمی مطرح می‌شود مبنی بر اینکه آیا پلتفرم صرفاً فضایی برای ارتباط کاربران فراهم می‌کند و هیچ مسئولیتی در قبال اتفاقات رخ‌داده ندارد یا اینکه متناسب با نوع خدمات، امکانات نظارتی و تکالیف قانونی خود باید برای شناسایی و محدودکردن فعالیت‌های متقلبانه اقدام کند؟

البته تعیین مسئولیت پلتفرم نیز نیازمند بررسی شرایط هر پرونده است. نمی‌توان هر تخلف کاربر را به‌طور خودکار به پای میزبان آن بستر نوشت؛ همانطور که نمی‌توان با استناد به واسطه‌بودن، تمام مسئولیت‌های احتمالی را از دوش ارائه‌دهنده خدمت برداشت. حدود تعهدات پلتفرم، میزان اطلاع آن از تخلف، امکان پیشگیری یا توقف فعالیت مجرمانه و واکنش آن پس از گزارش کاربران، از جمله موضوعاتی است که باید در ارزیابی حقوقی مورد توجه قرار گیرد.

از سوی دیگر، یکی از مهم‌ترین دغدغه‌های قربانیان کلاهبرداری اینترنتی، فاصله میان شناسایی مجرم و بازگشت دارایی از دست‌رفته است. برای فردی که پس‌انداز چندساله یا سرمایه کسب‌وکارش را از دست داده، محکومیت کیفری متهم به‌تنهایی پایان ماجرا نیست. او به دنبال بازگشت پولی است که ممکن است در چند مرحله منتقل شده و سرنوشت آن نامعلوم باشد.

به همین دلیل، سرعت واکنش پس از اعلام وقوع جرم، امکان شناسایی مسیر انتقال وجوه و اتخاذ تصمیم‌های قانونی برای توقیف اموال و حساب‌های مرتبط، اهمیت فراوانی دارد. هرچه فاصله میان وقوع جرم و اقدام مؤثر بیشتر شود، احتمال پیچیده‌ترشدن مسیر بازیابی وجوه نیز افزایش می‌یابد.

آنچه امروز بیش از هر زمان دیگری اهمیت دارد، نگاه زنجیره‌ای به امنیت مالی در فضای مجازی است. امنیت دارایی مردم صرفاً با شناسایی و مجازات کلاهبرداران تأمین نمی‌شود، بلکه به مجموعه‌ای از تکالیف پیشگیرانه، نظارت مؤثر، پاسخگویی نهادهای ارائه‌دهنده خدمات و سازوکارهای کارآمد برای جبران خسارت نیاز دارد.

در پرونده پیشرو، برای بررسی ابعاد این مسئله با یک قاضی متخصص در حوزه جرائم سایبری و دو وکیل باتجربه در زمینه جرائم رایانه‌ای و مسئولیت حقوقی پلتفرم‌ها گفت‌وگو کرده‌ایم. این گفت‌وگوها از سه زاویه متفاوت به یک پرسش مشترک می‌پردازند: وقتی پول مردم با یک کلیک ناپدید می‌شود، قانون چه راهی پیش پای قربانی می‌گذارد و سهم هر یک از بازیگران اقتصاد دیجیتال در جبران خسارت و پیشگیری از تکرار این اتفاق چیست؟

پاسخ به این پرسش، فقط دغدغه کسانی نیست که امروز قربانی کلاهبرداری اینترنتی شده‌اند؛ مسئله تمام شهروندانی است که هر روز با اطمینان به زیرساخت‌های بانکی و پلتفرم‌های دیجیتال، بخشی از زندگی اقتصادی خود را به فضای مجازی سپرده‌اند.



«کلاهبرداری اینترنتی صرفاً مسئله‌ای کیفری نیست، بلکه با حقوق بانکی، مسئولیت مدنی، تجارت الکترونیکی و حمایت از مصرف‌کننده نیز ارتباط مستقیم دارد. من معتقدم پاسخ مؤثر به این جرائم، مستلزم مجموعه‌ای از اقدامات هماهنگ است؛ از جمله پیشگیری از وقوع جرم، ارتقای امنیت خدمات مالی، شناسایی و مجازات مرتکبان، تعیین مسئولیت اشخاص دخیل و فراهم کردن امکان بازیابی سریع وجوه. اعتماد عمومی به اقتصاد دیجیتال زمانی تقویت می‌شود که شهروندان بدانند قانون، علاوه بر مجازات مجرم، برای حمایت از حقوق مالی آنان نیز راهکار مؤثر دارد

دکتر صادق تبریزی، قاضی دادگستری و عضو هیئت علمی دانشگاه:

قرائنی مثل نحوه افتتاح حساب و الگوی تراکنش در رسیدگی قضایی اهمیت دارد



دکتر صادق تبریزی، قاضی دادگستری و عضو هیئت علمی دانشگاه ضمن بررسی مهم‌ترین چالش‌های رسیدگی به کلاهبرداری‌های اینترنتی معتقد است: در رسیدگی قضایی، قرائنی مانند نحوه افتتاح و استفاده از حساب، پیام‌های مبادله شده، دریافت کارمزد، تعداد و الگوی تراکنش‌ها، ارتباط با سایر متهمان و نحوه انتقال بعدی وجوه اهمیت پیدا می‌کنند. متن گفت‌وگو با وی به شرح زیر است.

■■■

گاهی گفته می‌شود کسی که روی لینک جعلی کلیک کرده یا رمز بانکی خود را در اختیار دیگران گذاشته، خودش مقصر است. آیا بی‌احتیاطی قربانی می‌تواند مسئولیت کیفری کلاهبردار را از بین ببرد؟

در رسیدگی قضایی باید میان دو موضوع کاملاً متفاوت تفکیک قائل شد. نخست، مسئولیت کیفری مرتکب جرم و دوم، تأثیر احتمالی رفتار زیان دیده در وقوع خسارت. اصل بر این است که بی‌احتیاطی قربانی به خودی خود موجب زوال مسئولیت کیفری مرتکب نمی‌شود. اگر شخصی با توسل به وسایل متقلبانه دیگری را فریب دهد و مال او را تصاحب کند، نمی‌تواند صرفاً با این استدلال که قربانی باید دقت بیشتری می‌کرد از مسئولیت کیفری رهایی یابد.

برای مثال، فرض کنید فردی با طراحی صفحه‌ای شبیه درگاه رسمی پرداخت، اطلاعات بانکی شهروندی را به دست آورده و از حساب او برداشت می‌کند. اینکه قربانی به نشانی اینترنتی توجه کافی نکرده باشد، به تنهایی رفتار مجرمانه شخصی را که اطلاعات را تحصیل کرده و از آن سوءاستفاده کرده است، مشروع نمی‌کند.

البته در دادگاه، تشخیص عنوان مجرمانه اهمیت دارد. هر جرمی که با استفاده از اینترنت انجام شود، الزاماً کلاهبرداری رایانه‌ای نیست. در کلاهبرداری رایانه‌ای موضوع ماده ۱۳ قانون جرائم رایانه‌ای، نحوه استفاده غیرمجاز از سامانه و داده‌ها اهمیت اساسی دارد، درحالی‌که در کلاهبرداری سنتی، رفتار متقلبانه و فریب انسان نقش محوری دارد.

بنابراین، قاضی باید رفتار مرتکب، شیوه تحصیل مال و ارکان قانونی جرم را بررسی کند. در کنار آن، رفتار قربانی نیز ممکن است در دعوای جبران خسارت و بررسی رابطه سببیت مؤثر باشد. به بیان ساده، فریب خوردن یک شهروند نباید با مجازبودن فریب دادن او اشتباه گرفته شود.

چرا در برخی پرونده‌ها با وجود شناسایی کلاهبردار و صدور حکم محکومیت، مالباخته همچنان به پول خود نمی‌رسد؟

باید توجه داشت، صدور حکم محکومیت کیفری و وصول مال دو مرحله متفاوت هستند. ممکن است وقوع جرم اثبات و مرتکب محکوم شود، اما مالی برای استرداد یا اجرای حکم در دسترس نباشد.

در جرائم اینترنتی، یکی از مشکلات مهم، سرعت جابه‌جایی وجوه است. پول ممکن است در مدت کوتاهی از حساب اولیه به چند حساب دیگر منتقل شود، به دارایی‌های متفاوت تبدیل شود یا در اختیار اشخاصی قرار گیرد که شناسایی نقش آنان مستلزم تحقیقات جداگانه است. در چنین وضعیتی، حتی اگر هویت مرتکب اصلی شناسایی شود، بازگرداندن وجه همیشه ساده نیست.

البته نظام حقوقی فاقد ابزار حمایتی نیست. برای نمونه، مواد ۱۰۷ تا ۱۰۹ قانون آیین دادرسی کیفری، امکان درخواست تأمین خواسته و توقیف اموال با رعایت شرایط قانونی را پیش بینی کرده‌اند. در کلاهبرداری رایانه‌ای نیز قانونگذار، علاوه بر مجازات مرتکب، رد مال به صاحب آن را مقرر کرده است.

اما مشکل اینجاست که وجود ابزار قانونی با امکان استفاده مؤثر و به موقع از آن یکسان نیست. اگر در زمان شناسایی و توقیف اموال تأخیر ایجاد شود، ممکن است اجرای حکم با دشواری جدی روبه‌رو شود. نکته دیگر این است که رد مال، جبران سایر خسارت‌های احتمالی و وصول محکوم به، هرکدام شرایط و تشریفات قانونی خاص خود را دارند. بنابراین، نباید تصور کرد که صدور حکم حبس برای مرتکب، خودبه خود موجب بازگشت پول قربانی می‌شود.

حمایت مؤثر از مالباخته زمانی محقق می‌شود که اقدامات لازم برای شناسایی و حفظ اموال از همان مراحل ابتدایی تحقیقات مورد توجه قرار گیرد.

حساب‌های اجاره‌ای چه نقشی در کلاهبرداری‌های اینترنتی دارند؟ آیا هر صاحب حسابی که پول کلاهبرداری به حساب او واریز شده، شریک جرم محسوب می‌شود؟

خیر. صرف واریز وجه ناشی از جرم به حساب یک شخص، برای احراز مشارکت یا معاونت او در کلاهبرداری کافی نیست. در حقوق کیفری، مسئولیت اشخاص اصولاً شخصی است و برای انتساب جرم باید عناصر قانونی، مادی و روانی آن احراز شود. به همین دلیل، قاضی نمی‌تواند تنها بر اساس اینکه حساب بانکی متعلق به یک شخص بوده، او را شریک کلاهبرداری معرفی کند.

ممکن است صاحب حساب خود قربانی فریب شده باشد؛ برای مثال، شخصی با وعده استخدام یا پرداخت کارمزد، او را به واگذاری اطلاعات حساب ترغیب کرده باشد، بدون اینکه صاحب حساب از هدف مجرمانه آگاهی داشته باشد.

در وضعیت دیگر، ممکن است فرد با آگاهی از اینکه حساب او برای دریافت وجوه نامشروع استفاده می‌شود، امکانات بانکی خود را در اختیار مرتکبان قرار دهد. در چنین فرضی، با توجه به نوع رفتار، میزان آگاهی، قصد شخص و ارتباط او با جرم اصلی، امکان بررسی مسئولیت کیفری وجود دارد. همچنین ممکن است رفتار صاحب حساب واجد عنوان مجرمانه مستقلی باشد که باید بر اساس شرایط همان جرم بررسی شود.

در رسیدگی قضایی، قرائنی مانند نحوه افتتاح و استفاده از حساب، پیام‌های مبادله شده، دریافت کارمزد، تعداد و الگوی تراکنش‌ها، ارتباط با سایر متهمان و نحوه انتقال بعدی وجوه اهمیت پیدا می‌کنند. اما هیچ‌یک از این قرائن نباید جایگزین اثبات ارکان جرم شود. مرز میان فرد فریب خورده و همدست آگاه، آگاهی و رفتار قابل انتساب اوست نه صرف مالکیت حساب بانکی.

اثبات کلاهبرداری اینترنتی چه تفاوتی با جرائم سنتی دارد؟ قاضی چگونه از اصالت پیام‌ها، تصاویر و سایر ادله الکترونیکی اطمینان پیدا می‌کند؟

تفاوت مهم این پرونده‌ها در ماهیت ادله و شیوه ارزیابی آنهاست. در جرائم سنتی ممکن است بخش مهمی از ادله، اسناد کاغذی یا آثار فیزیکی باشد اما در جرائم اینترنتی، داده‌های الکترونیکی نقش بسیار مهمی دارند. پیامهای ردوبدل شده، اطلاعات حساب‌های کاربری، سوابق تراکنش‌ها، نشانی‌های اینترنتی، داده‌های ثبت شده در سامانه‌ها و گزارش‌های کارشناسی می‌توانند در کشف حقیقت مؤثر باشند. با این حال، صرف ارائه یک تصویر از صفحه تلفن‌همراه یا یک پیام چاپ‌شده، لزوماً به معنای اثبات قطعی انتساب آن به متهم نیست. امکان جعل، دستکاری، حذف بخشی از مکالمه یا استفاده اشخاص مختلف از یک حساب کاربری باید مورد توجه قرار گیرد.

برای مثال، ممکن است شاکی تصویری از مکالمه‌ای ارائه کند که در آن شخصی وعده تحویل کالا داده و سپس وجهی دریافت کرده است. دادگاه باید بررسی کند که آیا حساب کاربری واقعاً متعلق به متهم بوده، آیا محتوای ارائه شده اصالت دارد و آیا ارتباطی میان مکالمه و انتقال وجه وجود دارد یا خیر.

در این پرونده‌ها، گزارش کارشناسی تخصصی و بررسی داده‌ها از منابع معتبر اهمیت فراوانی دارد. همچنین نحوه جمع‌آوری، نگهداری و ارائه ادله باید به گونه‌ای باشد که امکان ارزیابی اصالت و تمامیت آنها فراهم شود. قانون جرائم رایانه‌ای نیز مقرراتی درباره ادله الکترونیکی و نحوه نگهداری و ارائه آنها پیش‌بینی کرده است.

البته قاضی نباید ارزیابی نهایی ادله را به طور کامل به کارشناس واگذار کند. کارشناس درباره موضوعات تخصصی اظهارنظر می‌کند اما احراز وقوع جرم و انتساب آن به متهم، در نهایت وظیفه مرجع قضایی است. مهم‌ترین ضرورت در این حوزه، ارتقای مستمر دانش فنی قضات، ضابطان و کارشناسان است.

چرا گاهی دستور مسدودسازی حساب‌های مرتبط با کلاهبرداری دیر صادر یا اجرا می‌شود؟ آیا قوانین فعلی پاسخگوی سرعت انتقال پول هستند؟

در جرائم مالی اینترنتی، سرعت یکی از عوامل تعیین کننده در موفقیت اقدامات قضایی است. ممکن است فاصله میان واریز وجه به حساب اولیه و انتقال آن به حساب‌های بعدی بسیار کوتاه باشد.

از سوی دیگر، مسدودسازی حساب بانکی اقدامی است که می‌تواند بر حقوق مالی اشخاص اثر مستقیم بگذارد. بنابراین، نمی‌توان صرف ادعای یک فرد را برای مسدودسازی نامحدود حساب اشخاص کافی دانست. مرجع قضایی باید میان ضرورت اقدام فوری و لزوم رعایت حقوق اشخاص تعادل برقرار کند.

یکی از چالش‌های عملی، شناسایی دقیق حساب‌های مرتبط با جرم است. ممکن است وجه به حساب شخصی منتقل شده باشد که خود از منشأ مجرمانه آن بی‌اطلاع است. در چنین وضعیتی، بررسی نقش صاحب حساب و تعیین حدود اقدام قضایی اهمیت دارد.

مشکل دیگر، تعدد نهادهای دخیل در فرایند پیگیری است. بانک‌ها، شرکت‌های پرداخت، ضابطان تخصصی و مراجع قضایی هرکدام وظایف و اختیارات متفاوتی دارند و هرگونه تأخیر در تبادل اطلاعات می‌تواند فرصت انتقال بیشتر وجوه را فراهم کند.

راهکار اصلی، ایجاد فرایندهای هماهنگ‌تر و سریع‌تر در چارچوب قانون است، به گونه‌ای که اطلاعات ضروری با سرعت در اختیار مرجع صالح قرار گیرد و در موارد واجد شرایط، دستور قانونی به‌موقع صادر و اجرا شود. همچنین باید امکان بررسی و رفع محدودیت‌های غیرضروری برای اشخاصی که ارتباط مجرمانه آنان احراز نشده است، وجود داشته باشد. اقدام قضایی مؤثر، اقدامی است که هم سریع باشد و هم قانونی.

آیا مجازات‌های فعلی برای مقابله با کلاهبرداری اینترنتی بازدارندگی کافی دارند؟ آیا برخورد با شبکه‌های سازمان یافته باید شدیدتر شود؟

ارزیابی بازدارندگی مجازات‌ها صرفاً با بررسی میزان حبس یا جزای نقدی امکانپذیر نیست. در سیاست کیفری، عواملی مانند احتمال کشف جرم، سرعت رسیدگی، قطع دسترسی مرتکب به عواید مجرمانه و امکان جبران خسارت قربانی نیز اهمیت فراوانی دارند.

ممکن است قانون برای رفتاری مجازات نسبتاً شدیدی تعیین کرده باشد، اما اگر مرتکب تصور کند احتمال شناسایی او اندک است یا می‌تواند منافع حاصل از جرم را حفظ کند، افزایش مجازات به‌تنهایی اثر مطلوبی نخواهد داشت.

در پرونده‌های مرتبط با شبکه‌های مجرمانه نیز باید میان نقش اشخاص تفکیک شود. طراح و سازمان دهنده فعالیت مجرمانه، شخصی که آگاهانه زیرساخت مالی را فراهم می‌کند و فردی که بدون اطلاع کافی مورد سوءاستفاده قرار گرفته است، لزوماً مسئولیت کیفری یکسانی ندارند. اصل فردی کردن مسئولیت کیفری اقتضا می‌کند نقش، قصد و رفتار هر متهم جداگانه بررسی شود. در عین حال، هرجا شرایط قانونی عناوین مربوط به فعالیت سازمان‌یافته یا سایر عوامل مؤثر در تعیین مجازات وجود داشته باشد، مرجع قضایی باید مقررات مربوط را اعمال کند.

سیاست کیفری مؤثر باید چند هدف را همزمان دنبال کند. از جمله شناسایی سریع مرتکبان اصلی، جلوگیری از تداوم فعالیت شبکه‌های مجرمانه، محروم کردن مرتکبان از عواید جرم و فراهم کردن امکان بازگشت اموال به قربانیان. تقویت ظرفیت تخصصی پلیس و مراجع قضایی، همکاری قانونی و مؤثر با شبکه بانکی و ارتقای آگاهی عمومی می‌تواند به اندازه اصلاح مجازات‌ها اهمیت داشته باشد.

بنابراین، پاسخ به کلاهبرداری اینترنتی نباید صرفاً افزایش مجازات باشد. مجازات زمانی می‌تواند نقش بازدارنده مؤثرتری ایفا کند که با کشف به موقع جرم، رسیدگی دقیق و جلوگیری از انتفاع اقتصادی مرتکب همراه شود.

به طور خلاصه رسیدگی به کلاهبرداری‌های اینترنتی، آزمونی برای توان نظام قضایی در مواجهه با جرائمی است که سرعت ارتکاب و پیچیدگی فنی آنها روزبه‌روز افزایش می‌یابد. در این پرونده‌ها، رعایت حقوق متهم، حمایت از قربانی، اعتبارسنجی ادله الکترونیکی و جلوگیری از انتقال عواید جرم باید در کنار یکدیگر مورد توجه قرار گیرند. در نهایت، عدالت کیفری زمانی برای شهروندان ملموس‌تر خواهد بود که علاوه بر شناسایی و مجازات مرتکب، امکان مؤثر و قانونی برای بازگرداندن اموال و جبران خسارت آنان نیز فراهم شود.



دکتر فاطمه قناد، وکیل پایه یک دادگستری و دانشیار دانشگاه علم و فرهنگ:

حساب بانکی اجاره‌ای حلقه‌مهم در زنجیره ارتکاب جرائم مالی و سایبری است

دکتر فاطمه قناد، وکیل پایه یک دادگستری و دانشیار دانشگاه علم و فرهنگ در گفت‌وگو با «جوان» حساب بانکی اجاره‌ای را یکی از حلقه‌های مهم در زنجیره ارتکاب جرائم مالی و سایبری دانسته و می‌گوید: اجاره دادن حساب، به تنهایی و بدون احراز عناصر قانونی و روانی، الزاماً معاونت در کلاهبرداری یا پولشویی نیست. نحوه دریافت وجه، تکرار تراکنش‌ها، دریافت کارمزد، ارتباط با مرتکب و رفتار صاحب حساب پس از دریافت وجوه، می‌توانند در ارزیابی علم و عمد او مؤثر باشند. متن گفت‌وگو با وی به شرح زیر است:

■■■

در پرونده‌های کلاهبرداری اینترنتی، چرا شناسایی مجرم همیشه به بازگشت پول مالباخته منجر نمی‌شود؟ آیا قوانین فعلی ابزار کافی برای حمایت از قربانیان و جبران خسارت آنها را فراهم کرده‌اند؟

باید میان شناسایی مرتکب و بازگشت مال به بزه‌دیده تفکیک قائل شد. این دو از نظر حقوقی و عملی الزاماً ملازمه‌ای با یکدیگر ندارند. ممکن است هویت فردی که در عملیات کلاهبرداری نقش داشته شناسایی شود، اما وجه حاصل از جرم پیش‌تر از حساب اولیه خارج شده، میان چند حساب بانکی گردش کرده یا به دارایی دیگری تبدیل شده باشد. در واقع، در بسیاری از این پرونده‌ها با زنجیره‌ای از اشخاص و حساب‌ها مواجهیم که مرتکب اصلی، صاحب حساب دریافت‌کننده وجه و انتقال‌دهنده آن ممکن است اشخاص متفاوتی باشند.

از نظر قانونی، ابزارهایی برای حمایت از بزه‌دیده وجود دارد. ماده ۷۴۱ قانون مجازات اسلامی، در کلاهبرداری رایانه‌ای، علاوه بر مجازات مرتکب، رد مال به صاحب آن را نیز پیش‌بینی کرده است. ماده ۲۱۴ قانون مجازات اسلامی نیز بر تکلیف مجرم به بازگرداندن مال تحصیل‌شده و جبران خسارات تأکید دارد. بنابراین، نمی‌توان گفت نظام حقوقی در این زمینه فاقد مبنای قانونی است. بااینحال، وجود حکم به رد مال با امکان عملی اجرای آن تفاوت دارد. مسئله اصلی در بسیاری از پرونده‌ها، نه فقدان حکم قانونی بلکه دشواری ردیابی وجوه، شناسایی تمام حلقه‌های انتقال و توقیف به‌موقع دارایی‌هاست. به اعتقاد من، موفقیت سیاست جنایی در این حوزه را نباید صرفاً با تعداد مرتکبان شناسایی‌شده یا محکومان سنجید، بلکه امکان واقعی بازگرداندن مال به بزه‌دیده نیز باید بخشی از معیار ارزیابی کارآمدی نظام عدالت کیفری باشد.

حساب‌های بانکی اجاره‌ای به یکی از ابزارهای اصلی کلاهبرداران سایبری تبدیل شده‌اند. از نظر کیفری، صاحب حسابی که آگاهانه حساب خود را در اختیار دیگران قرار می‌دهد، چه مسئولیتی دارد؟

حساب بانکی اجاره‌ای را باید یکی از حلقه‌های مهم در زنجیره ارتکاب جرائم مالی و سایبری دانست. مرتکب اصلی با استفاده از حساب اشخاص دیگر می‌کوشد میان هویت واقعی خود و جریان انتقال وجوه حاصل از جرم فاصله ایجاد کند.

بااینحال، صرف اینکه حساب بانکی به نام شخصی باشد که وجه حاصل از کلاهبرداری به آن واریز شده، برای انتساب مسئولیت کیفری کافی نیست. اصل شخصی بودن مسئولیت کیفری اقتضا می‌کند نقش و میزان آگاهی صاحب حساب به‌طور مستقل بررسی شود. بر اساس ماده ۱۲۶ قانون مجازات اسلامی، اگر صاحب حساب با علم به هدف مجرمانه، حساب خود را در اختیار مرتکب قرار دهد و با این اقدام وقوع جرم را تسهیل کند، حسب شرایط قانونی، امکان تحقق معاونت در جرم وجود دارد. چنانچه در عملیات اجرایی جرم نیز مشارکت داشته باشد، ماده ۱۲۵ درباره شرکت در جرم قابل بررسی است. همچنین اگر آگاهانه در انتقال، تبدیل یا پنهان‌سازی عواید حاصل از جرم نقش داشته باشد، ممکن است رفتار او با مقررات ماده ۲ قانون مبارزه با پولشویی انطباق پیدا کند. البته این عناوین را نباید با یکدیگر خلط کرد. اجاره دادن حساب، به‌تنهایی و بدون احراز عناصر قانونی و روانی، الزاماً معاونت در کلاهبرداری یا پولشویی نیست. نحوه دریافت وجه، تکرار تراکنش‌ها، دریافت کارمزد، ارتباط با مرتکب و رفتار صاحب حساب پس از دریافت وجوه، می‌توانند در ارزیابی علم و عمد او مؤثر باشند.

در بسیاری از پرونده‌های کلاهبرداری اینترنتی، قربانیان برای اثبات جرم با مشکلات جدی مواجه‌اند. مهم‌ترین موانع اثبات این جرائم در مراجع قضایی چیست؟

مهم‌ترین دشواری در اثبات این جرائم، فاصله میان کشف ردپای فنی و انتساب حقوقی رفتار به شخص معین است. ممکن است پلیس بتواند شماره تلفن، نشانی اینترنتی، حساب بانکی، پیام‌ها یا سوابق تراکنش‌ها را شناسایی کند، اما هیچ‌یک از این داده‌ها به‌تنهایی لزوماً اثبات نمی‌کند که شخص معینی با علم و اراده مرتکب جرم شده است. برای مثال، مالکیت یک سیمکارت یا حساب بانکی الزاماً به معنای استفاده شخصی از آن در زمان ارتکاب جرم نیست. استفاده از هویت جعلی، حساب‌های متعدد، واسطه‌های مالی و انتقال سریع وجوه نیز بازسازی زنجیره وقوع جرم را دشوار می‌کند. در این زمینه، مواد ۱۲ و ۱۳ قانون تجارت الکترونیکی اهمیت دارند؛ زیرا داده‌پیام را به دلیل شکل و قالب الکترونیکی آن از عداد دلایل خارج نمی‌کنند و ارزش اثباتی آن را با توجه به عوامل اطمینان‌بخش، از جمله اصالت و تمامیت، مورد ارزیابی قرار می‌دهند. همچنین بر اساس ماده ۲۱۱ قانون مجازات اسلامی، گزارش ضابطان، نظریه کارشناسی و اطلاعات حاصل از تحقیقات، در صورت برخورداری از شرایط قانونی، می‌توانند از مستندات علم قاضی باشند.

بنابراین، مسئله صرفاً جمع‌آوری داده دیجیتال نیست؛ بلکه باید اصالت، تمامیت، ارتباط داده با موضوع اتهام و قابلیت انتساب آن به متهم احراز شود. نباید میان کشف یک نشانه فنی و اثبات قضایی جرم خلط کرد.

آیا قوانین کیفری فعلی با شیوه‌های جدید کلاهبرداری در فضای مجازی تناسب دارند؟ به‌ویژه در مواردی که مجرمان با هویت جعلی، شماره‌های ناشناس و حساب‌های متعدد فعالیت می‌کنند، چه خلأهایی وجود دارد؟

پاسخ به این پرسش مستلزم تفکیک میان خلأ قانونی و دشواری اجرای قانون است. صرف ظهور شیوه‌های جدید کلاهبرداری به معنای ناکافی بودن عناوین مجرمانه موجود نیست.

ماده ۷۴۱ قانون مجازات اسلامی، کلاهبرداری رایانه‌ای را در مواردی که مرتکب از طریق اعمالی مانند وارد کردن، تغییر، محو یا ایجاد داده‌ها یا مختل کردن سامانه، به‌طور غیرمجاز مال یا منفعت مالی تحصیل می‌کند، جرم‌انگاری کرده است. در مقابل، اگر شخص با استفاده از اینترنت، اما از طریق فریب مستقیم انسان و توسل به وسایل متقلبانه، مال دیگری را تحصیل کند، ممکن است رفتار او مشمول ماده یک قانون تشدید مجازات مرتکبین ارتشا، اختلاس و کلاهبرداری باشد.

نظریه مشورتی شماره ۱۸۲/۱۴۰۵/۷ مورخ ۱۴۰۵/۴/۲۴ اداره کل حقوقی قوه قضائیه نیز بر ضرورت تفکیک این دو وضعیت تأکید دارد. بنابراین، صرف استفاده از بستر اینترنت برای تحقق عنوان کلاهبرداری رایانه‌ای کافی نیست و باید شیوه ارتکاب و عناصر قانونی جرم بررسی شود.

البته در عمل با چالش‌هایی مانند دشواری احراز هویت واقعی مرتکبان، پراکندگی اطلاعات میان بانک‌ها و ارائه‌دهندگان خدمات ارتباطی، استفاده از حساب‌های واسطه و دسترسی دشوار به داده‌های سکوهای خارجی مواجهیم. به اعتقاد من، بخشی از این مشکلات بیش از آنکه ناشی از فقدان عنوان مجرمانه باشد، به ضعف هماهنگی نهادی و ناکافی بودن سازوکارهای عملیاتی کشف و تعقیب مربوط است. ازاین‌رو، پیش از پیشنهاد جرم‌انگاری‌های جدید باید ظرفیت قوانین موجود و موانع اجرای آنها به‌دقت ارزیابی شود.

اگر قربانی کلاهبرداری اینترنتی در ساعات اولیه پس از انتقال وجه به پلیس یا مراجع قضایی مراجعه کند، چه ظرفیت قانونی برای توقف انتقال پول و مسدودسازی حساب مقصد وجود دارد؟ آیا روند فعلی به‌اندازه کافی سریع و مؤثر است؟

در اینجا زمان یک عامل تعیین‌کننده است. در بسیاری از پرونده‌ها، فاصله میان انتقال وجه و نخستین اقدام مؤثر برای شناسایی و توقیف آن می‌تواند سرنوشت امکان بازگشت پول را مشخص کند. قانون آیین دادرسی کیفری ظرفیت‌هایی برای حمایت مالی از بزه‌دیده پیش‌بینی کرده است. مواد ۱۰۷ تا ۱۰۹ این قانون به تأمین خواسته اختصاص دارند. بر اساس ماده ۱۰۷، شاکی می‌تواند تأمین ضرر و زیان خود را از بازپرس درخواست کند و در صورت وجود ادله قابل قبول، قرار تأمین خواسته صادر شود. اهمیت ماده ۱۰۹ نیز در این است که اگر تأخیر در اجرای قرار موجب تضییع خواسته شود، ابتدا قرار اجرا و سپس ابلاغ خواهد شد.

همچنین ماده ۱۵۱ قانون آیین دادرسی کیفری امکان کنترل حساب‌های بانکی را در موارد ضروری، برای کشف جرم یا دستیابی به ادله وقوع جرم و با تأیید رئیس حوزه قضایی، پیشبینی کرده است. البته باید توجه داشت، کنترل حساب بانکی با توقیف موجودی آن یکسان نیست و هر اقدام باید مستند به اختیار قانونی مربوط باشد. از نظر عملی، قربانیان می‌توانند از طریق مرکز فوریت‌های سایبری پلیس فتا به شماره ۰۹۶۳۸۰، گزارش اولیه را در سریع‌ترین زمان ممکن ثبت کنند. نباید منتظر تکمیل تمام مراحل شکایت بمانند، زیرا ممکن است وجوه در این فاصله به حساب‌های متعدد منتقل شود. به نظر من، مسئله اصلی در این حوزه، ضرورت ایجاد سازوکاری هماهنگ میان پلیس فتا، بانک‌ها و مراجع قضایی است تا گزارش اولیه قربانی، شناسایی تراکنش مشکوک و اقدامات قانونی برای حفظ وجوه با کمترین تأخیر انجام شود. البته مسدودسازی حساب به معنای بازگشت قطعی وجه نیست؛ اما هرچه مداخله در مراحل اولیه صورت گیرد، امکان جلوگیری از خروج و پنهان‌سازی عواید جرم افزایش می‌یابد. در نهایت، کارآمدی سیاست جنایی در برابر کلاهبرداری اینترنتی صرفاً با تعداد پرونده‌های کشف‌شده یا محکومان سنجیده نمی‌شود، بلکه میزان توانایی نظام عدالت کیفری در جلوگیری از گردش عواید جرم و بازگرداندن مال به بزه‌دیدگان نیز باید در ارزیابی آن مورد توجه قرار گیرد.



دکتر محمد کاظم زارع، وکیل پایه یک دادگستری و مدرس حقوق کیفری:

به‌محض اطلاع از برداشت غیرمجاز، موضوع را به بانک گزارش کنید

دکتر محمدکاظم زارع، وکیل پایه یک دادگستری و مدرس و مؤلف حقوق کیفری، در گفت‌وگو با «جوان» به قربانیان توصیه کرد: به‌محض اطلاع از برداشت غیرمجاز، موضوع را به بانک گزارش کنند، مستندات تراکنش‌ها و پیام‌ها را حفظ کنند و از طریق پلیس فتا و مراجع قضایی پیگیری کنند. متن گفت‌وگو با وی به شرح زیر است:

■■■

در مواردی که فرد بدون اطلاع و رضایت صاحب حساب، قربانی برداشت غیرمجاز اینترنتی می‌شود، مرز مسئولیت بانک و مشتری کجاست؟ آیا بانک می‌تواند صرفاً با این استدلال که تراکنش با رمز یک‌بارمصرف یا اطلاعات صحیح کارت انجام شده، خود را از مسئولیت مبرا کند؟

به نظر من، نخستین نکته این است که باید میان صحت فنی تراکنش و رضایت واقعی صاحب حساب تفاوت قائل شویم. اینکه یک انتقال وجه با رمز یک‌بارمصرف و اطلاعات صحیح کارت انجام شده، الزاماً به معنای رضایت صاحب حساب یا قانونی‌بودن برداشت نیست.

برای مثال، ممکن است شخصی از طریق یک پیامک جعلی به صفحه‌ای هدایت شود که کاملاً شبیه درگاه رسمی پرداخت است. او اطلاعات خود را وارد می‌کند و کلاهبردار از همان اطلاعات برای برداشت وجه استفاده می‌کند. در چنین وضعیتی، بانک نمی‌تواند صرفاً با این استدلال که رمز صحیح بوده، بحث مسئولیت خود را پایان‌یافته بداند.

البته من معتقدم نباید از این موضوع نتیجه گرفت که بانک ضامن تمام کلاهبرداری‌های اینترنتی است. مسئولیت بانک زمانی قابل طرح است که مبنای قانونی یا قراردادی آن وجود داشته باشد. باید بررسی شود آیا بانک الزامات امنیتی را رعایت کرده، سامانه آن نقص مؤثری داشته، تعهد مشخصی را نقض کرده یا پس از اطلاع از برداشت غیرمجاز، برخلاف وظایف قانونی خود عمل کرده است. در نتیجه، اگر بانک در خصوص سنجش هویت کاربر، امنیت اطلاعات کاربر و حساب بانکی و همچنین ارسال رمز بدون رعایت پروتکل‌های امنیتی دارای عمد یا تقصیر باشد، به‌عنوان یک شخص حقوقی می‌تواند مطابق ماده ۱۴۳ قانون مجازات اسلامی و همچنین قانون مسئولیت مدنی دارای مسئولیت کیفری و مدنی (یا صرفاً مدنی در موارد عدم حصول شرایط مسئولیت کیفری) باشد.

از منظر حقوقی، برای احراز مسئولیت مدنی، اصولاً باید خسارت، رفتار قابل انتساب و رابطه سببیت میان آنها بررسی شود. ماده یک قانون مسئولیت مدنی از مبانی مهم این تحلیل است.

در اینجا لازم است تفاوتی میان کلاهبرداری رایانه‌ای و کلاهبرداری سنتی نیز مطرح کنم. ماده ۷۴۱ قانون مجازات اسلامی، بخش تعزیرات، ناظر بر تحصیل متقلبانه مال یا منفعت از طریق اعمال رایانه‌ای مقرر در قانون است، درحالی‌که ماده یک قانون تشدید مجازات مرتکبان ارتشا، اختلاس و کلاهبرداری، بر فریب اشخاص و وسایل متقلبانه تکیه دارد. بنابراین، هر کلاهبرداری که در فضای اینترنت اتفاق می‌افتد، لزوماً کلاهبرداری رایانه‌ای محسوب نمی‌شود.

همچنین مسئولیت کیفری بانک به‌عنوان شخص حقوقی، با مسئولیت مدنی آن متفاوت است و صرف وقوع جرم در بستر خدمات بانکی، برای تحقق شرایط ماده ۱۴۳ قانون مجازات اسلامی کافی نیست.

به اعتقاد من، نه می‌توان بانک را در تمام موارد مسئول شناخت و نه می‌توان رمز صحیح را دلیل قطعی بی‌مسئولیتی آن دانست. هر پرونده باید بر اساس مستندات فنی و حقوقی خودش بررسی شود.

گاهی قربانی خودش اطلاعات کارت بانکی یا رمز یک‌بارمصرف را در یک درگاه جعلی وارد می‌کند. از منظر حقوقی، آیا این رفتار به معنای پذیرش مسئولیت کامل از سوی مشتری است یا همچنان می‌توان در صورت اثبات ضعف زیرساخت‌های امنیتی یا قصور بانک، مسئولیت مشترکی برای بانک در نظر گرفت؟

من معتقدم فریب‌خوردن را نباید با پذیرش آگاهانه مسئولیت تمام خسارت یکسان دانست. بسیاری از درگاه‌های جعلی به‌قدری حرفه‌ای طراحی می‌شوند که تشخیص آنها حتی برای کاربران آشنا با اینترنت نیز دشوار است.

فرض کنید شهروندی پیامکی درباره پرداخت هزینه یک خدمت عمومی دریافت می‌کند. پیام ظاهری رسمی دارد و او را به صفحه‌ای هدایت می‌کند که از نظر طراحی شبیه درگاه بانکی است. آیا صرف واردکردن اطلاعات بانکی به این معناست که قربانی باید تمام خسارت را تحمل کند؟ به نظر من، چنین نتیجه‌ای بدون بررسی شرایط وقوع حادثه قابل دفاع نیست.

البته شهروندان نیز باید مراقبت متعارف از اطلاعات بانکی خود داشته باشند. اگر فردی با وجود هشدارهای روشن، رمز محرمانه خود را در اختیار اشخاص ناشناس قرار دهد، این رفتار ممکن است در ارزیابی تقصیر و رابطه سببیت مؤثر باشد و از باب مسئولیت خود زیان‌دیده، ضمان را منتفی بداند، اما بی‌احتیاطی مشتری به‌تنهایی ثابت نمی‌کند که بانک یا شرکت پرداخت تمام تعهدات خود را انجام داده و در مواردی به مسئولیت اشتراکی بانک و مشتری روی می‌آوریم، به‌خصوص در جایی که علاوه بر مقصر بودن مشتری، بانک نیز در تشخیص هویت کاربر و رعایت پروتکل‌های امنیتی دارای تقصیر بوده است.

برای مثال، اگر همزمان با فریب مشتری، نقص امنیتی مؤثری در سامانه پرداخت وجود داشته باشد یا یک تعهد قانونی مشخص نقض شده باشد، بیش از یک عامل مسئول است. البته تعیین سهم مسئولیت اشخاص، تابع شرایط پرونده و قواعد قانونی مربوط است که به‌طور خلاصه می‌توان طبق نظریه کارشناس رسمی و براساس تأثیر یا درصد عملکرد، میزان مسئولیت را تعیین کرد.

در این موارد، کارشناسی فنی اهمیت فراوانی دارد. باید مشخص شود اطلاعات چگونه تحصیل شده، تراکنش از چه مسیری انجام گرفته، چه هشدارهایی وجود داشته و رفتار هر شخص چه تأثیری در وقوع خسارت داشته است.

نکته مهم دیگر آن است که تقصیر احتمالی قربانی، مسئولیت کیفری مرتکب را از بین نمی‌برد. کسی که با اقدامات مجرمانه مال دیگری را تصاحب کرده، نمی‌تواند صرفاً با استناد به اعتماد یا کم‌دقتی قربانی، از مسئولیت فرار کند.

به نظر من، پرسش اصلی نباید فقط این باشد که چه کسی رمز را وارد کرده، بلکه باید بررسی کنیم چه عواملی موجب خروج غیرمجاز پول شده‌اند.

اگر فردی از طریق یک پلتفرم خریدوفروش اینترنتی با فروشنده‌ای جعلی مواجه شود و پس از واریز وجه متضرر شود، آیا پلتفرم صرفاً یک واسطه بی‌مسئولیت محسوب می‌شود؟ آیا تکلیفی برای احراز هویت کاربران، نظارت بر آگهی‌ها و جلوگیری از فعالیت حساب‌های مشکوک دارد؟

به نظر من، نه می‌توان تمام پلتفرم‌ها را مسئول هر کلاهبرداری دانست و نه می‌توان صرفاً به دلیل واسطه‌بودن، آنها را از هرگونه مسئولیت معاف کرد.

پلتفرم‌های اینترنتی نقش یکسانی ندارند. برخی فقط امکان انتشار آگهی و ارتباط خریدار و فروشنده را فراهم می‌کنند. برخی دیگر در دریافت وجه، نگهداری پول، تأیید معامله یا ارائه تضمین‌های قراردادی دخالت دارند. طبیعی است که تعهدات هر پلتفرم باید متناسب با نوع فعالیت و نقشی که واقعاً بر عهده گرفته، بررسی شود. در مواردی که پلتفرم از ابتدا مسئولیت نگهداری پول را پذیرفته و تضمین‌های قراردادی در این خصوص داده، مسئولیت کیفری و مدنی دارد، اما اگر پلتفرم صرفاً نقش واسطه‌گری داشته و همچنین از ابتدا با هشدارهای روشن از خود سلب مسئولیت کرده، پذیرش مسئولیت وی مشکل است.

برای مثال، تصور کنید شخصی با یک حساب جعلی، کالایی را برای فروش آگهی می‌کند و پس از دریافت پول ناپدید می‌شود. صرف وقوع این کلاهبرداری، الزاماً به معنای مسئولیت پلتفرم نیست.

اگر پلتفرم تعهد مشخصی برای احراز هویت فروشنده پذیرفته باشد، از فعالیت مشکوک و تکراری یک حساب اطلاع معتبر داشته باشد یا برخلاف تکلیف قانونی خود به گزارش‌های مؤثر رسیدگی نکند، موضوع مسئولیت آن مطرح می‌شود؛ مشروط بر اینکه نقض تعهد و ارتباط آن با خسارت احراز شود.

من معتقدم باید میان نظارت متعارف و تضمین مطلق سلامت معاملات تفاوت گذاشت. نمی‌توان انتظار داشت پلتفرم وقوع هر تخلفی را غیرممکن کند، اما می‌توان انتظار داشت تکالیف قانونی و قراردادی خود را رعایت کند.

قانون تجارت الکترونیکی، قواعد عمومی قراردادها و مسئولیت مدنی، در کنار مقررات تخصصی مربوط به هر نوع فعالیت، می‌توانند در تعیین حدود این تعهدات مؤثر باشند. از نگاه من، مشکل مهم این است که بسیاری از کاربران نمی‌دانند پلتفرم مورد استفاده آنها چه مسئولیتی پذیرفته است. آیا فقط آگهی منتشر می‌کند؟ آیا هویت فروشنده را بررسی کرده؟ آیا پرداخت امن ارائه می‌دهد؟

من معتقدم شفافیت درباره مسئولیت پلتفرم‌ها هم از حقوق مصرف‌کننده حمایت می‌کند و هم اعتماد عمومی به تجارت اینترنتی را افزایش می‌دهد.

در بسیاری از کلاهبرداری‌های اینترنتی، پول قربانی از طریق چند حساب بانکی و درگاه پرداخت جابه‌جا می‌شود. از نظر حقوقی، مسئولیت شرکت‌های ارائه‌دهنده خدمات پرداخت، بانک‌های پذیرنده و سایر واسطه‌های فنی در این زنجیره چیست؟ آیا در صورت وجود نقص امنیتی یا کوتاهی در اجرای الزامات نظارتی، امکان مطالبه خسارت از آنها وجود دارد؟

یکی از پیچیدگی‌های کلاهبرداری‌های اینترنتی، سرعت انتقال پول است. ممکن است وجه در مدت کوتاهی از چند حساب عبور کند یا به دارایی‌های دیگری، از جمله رمزارز، تبدیل شود. همین موضوع ردیابی و بازیابی آن را دشوار می‌کند.

من معتقدم پیچیده‌بودن مسیر انتقال وجه نباید به معنای از بین رفتن امکان پیگیری حقوقی باشد. در این پرونده‌ها باید نقش هر شخص در زنجیره پرداخت مشخص شود. بانک مبدأ، بانک مقصد، بانک پذیرنده، شرکت ارائه‌دهنده خدمات پرداخت و سایر واسطه‌های فنی، لزوماً تعهدات یکسانی ندارند.

برای بررسی مسئولیت هرکدام باید پرسید چه تکلیف قانونی یا قراردادی داشته‌اند، آیا آن تکلیف نقض شده و آیا این نقض در وقوع یا افزایش خسارت مؤثر بوده است؟

برای مثال، اگر یک شرکت پرداخت موظف به رعایت استاندارد امنیتی مشخصی بوده و نقض آن استاندارد در وقوع خسارت نقش داشته باشد، امکان مطالبه خسارت با احراز شرایط قانونی وجود دارد، اما صرف عبور پول از یک درگاه یا حساب بانکی، دلیل کافی برای مسئولیت آن نهاد نیست. در پرونده‌های مرتبط با رمزارز نیز همین قاعده اهمیت دارد. تبدیل پول به رمزارز ممکن است بازیابی دارایی را دشوار کند، اما نمی‌توان تمام اشخاصی را که خدمات فنی یا مالی ارائه کرده‌اند، بدون اثبات مبنای قانونی مسئول دانست. به نظر من، در کنار مسئولیت مدنی، مسئله سرعت واکنش اهمیت بسیار زیادی دارد. ممکن است مرتکب بعداً شناسایی و محکوم شود، اما در آن زمان مالی برای بازگرداندن باقی نمانده باشد.

بنابراین توصیه من به قربانیان این است که به‌محض اطلاع از برداشت غیرمجاز، موضوع را به بانک گزارش کنند، مستندات تراکنش‌ها و پیام‌ها را حفظ کنند و از طریق پلیس فتا و مراجع قضایی پیگیری کنند.

در عین حال، توقف یا مسدودسازی وجوه باید با رعایت قانون، صلاحیت مراجع مربوط و حقوق اشخاص ثالث انجام شود.

به اعتقاد من، حمایت مؤثر از مالباخته زمانی امکانپذیر است که ردیابی وجوه از همان مراحل اولیه مورد توجه قرار گیرد، نه صرفاً پس از صدور حکم محکومیت.

اگر قرار باشد برای حمایت مؤثرتر از قربانیان کلاهبرداری اینترنتی یک اصلاح حقوقی یا قانونی انجام شود، اولویت شما چیست؟ ایجاد صندوق جبران خسارت قربانیان جرائم سایبری، الزام بانک‌ها به جبران برداشت‌های غیرمجاز در شرایط مشخص، مسئولیت بیشتر پلتفرم‌ها یا ایجاد سازوکار فوری مسدودسازی و بازگرداندن وجوه مشکوک؟ چرا؟

اگر قرار باشد فقط یک اصلاح را در اولویت قرار دهم، من معتقدم مهم‌ترین اقدام، ایجاد سازوکاری سریع، هماهنگ و قانونمند برای ردیابی و جلوگیری از انتقال بیشتر وجوه ناشی از کلاهبرداری است.

دلیل این انتخاب روشن است که در بسیاری از پرونده‌ها، حتی اگر کلاهبردار شناسایی و محکوم شود، مالباخته موفق به بازپس‌گیری پول خود نمی‌شود، زیرا وجوه پیش‌تر منتقل یا از دسترس خارج شده‌اند.

به نظر من، باید میان بانک‌ها، شرکت‌های پرداخت، پلیس فتا و مراجع قضایی هماهنگی مؤثرتری برقرار شود تا در موارد واجد شرایط قانونی، امکان شناسایی مسیر وجوه و اقدام فوری فراهم باشد.

البته چنین سازوکاری نباید به مسدودسازی خودسرانه حساب‌ها منجر شود. نظارت مرجع صالح، رعایت حقوق اشخاص ثالث و امکان اعتراض به محدودیت‌های غیرضروری، بخش جدایی‌ناپذیر این اصلاح است.

در مرحله بعد، من معتقدم مسئولیت بانک‌ها و پلتفرم‌ها باید شفاف‌تر شود. قانون باید مشخص کند در چه شرایطی نقض تعهدات امنیتی یا نظارتی، مسئولیت جبران خسارت ایجاد می‌کند. این شفافیت هم برای مردم مفید است و هم برای ارائه‌دهندگان خدمات.

ایجاد صندوق جبران خسارت قربانیان جرائم سایبری نیز پیشنهاد قابل بررسی است. به‌ویژه برای مواردی که مرتکب شناسایی نمی‌شود یا اموال کافی برای جبران خسارت ندارد. البته چنین صندوقی در اینجا یک پیشنهاد اصلاحی است، نه حقی که بتوان بدون وجود مقررات مربوط، آن را از دولت یا بانک مطالبه کرد.

من معتقدم سیاست حقوقی ما نباید صرفاً مجازات‌محور باشد. مجازات کلاهبردار ضروری است، اما برای شهروندی که تمام پس‌اندازش را از دست داده، بازگشت پول نیز اهمیت اساسی دارد.

در نهایت، هدف باید ایجاد نظامی باشد که در آن مرتکب جرم پاسخگو باشد، بانک‌ها و پلتفرم‌ها متناسب با تکالیف و نقش خود مسئولیت بپذیرند و قربانی نیز در پیچیدگی فرایندهای بانکی و قضایی سرگردان نماند. به نظر من، موفقیت در مقابله با کلاهبرداری اینترنتی فقط با تعداد محکومیت‌های کیفری سنجیده نمی‌شود، بلکه باید دید چه میزان از حقوق مالی قربانیان واقعاً احیا شده است.

سخن پایانی.

کلاهبرداری اینترنتی صرفاً مسئله‌ای کیفری نیست، بلکه با حقوق بانکی، مسئولیت مدنی، تجارت الکترونیکی و حمایت از مصرف‌کننده نیز ارتباط مستقیم دارد.

من معتقدم پاسخ مؤثر به این جرائم، مستلزم مجموعه‌ای از اقدامات هماهنگ است؛ از جمله پیشگیری از وقوع جرم، ارتقای امنیت خدمات مالی، شناسایی و مجازات مرتکبان، تعیین مسئولیت اشخاص دخیل و فراهم کردن امکان بازیابی سریع وجوه. اعتماد عمومی به اقتصاد دیجیتال زمانی تقویت می‌شود که شهروندان بدانند قانون، علاوه بر مجازات مجرم، برای حمایت از حقوق مالی آنان نیز راهکار مؤثر دارد.