فصلنامه پژوهش های نوین در علوم انسانی و حقوق دوره ۲- شماره۴ – صفحات۴۲۷-۴۱۵
Journal of new Researches in Humanities and Law
ISSN 3060-6101

اختلاس در فضای مجازی و جرائم سایبری مرتبط: چالش‌های حقوقی و قضایی

اکبر هوشیاری[۱] ، رضا امیری[۲] *
[۱].استادیار گروه معارف اسلامی دانشگاه ازاد اسلامی واحد سنندج، سنندج، ایران
[۲].دانشجوی کارشناسی ارشد ، رشته جزا و جرم شناسی دانشگاه آزاد اسلامی واحد سنندج، سنندج، ایران

چکیده

گسترش فناوری اطلاعات، بانکداری الکترونیکی و سامانه‌های پرداخت و ذخیره‌سازی برخط، ضمن افزایش سرعت و کارآمدی فعالیت‌های اقتصادی، زمینه شکل‌گیری شیوه‌های نوین جرائم مالی را نیز فراهم کرده است. یکی از این جرائم، سوءاستفاده از دسترسی‌های سازمانی برای برداشت، انتقال یا تصاحب غیرقانونی وجوه از طریق سامانه‌های رایانه‌ای است که با عنوان «اختلاس سایبری» شناخته می‌شود. با این حال، در حقوق کیفری ایران، تحقق عنوان اختلاس مستلزم وجود شرایط و ارکان مقرر در ماده ۵ قانون تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاهبرداری است و صرف استفاده از فناوری در ارتکاب جرم، موجب تحقق عنوان اختلاس نمی‌شود. از سوی دیگر، قانون جرائم رایانه‌ای مصوب ۱۳۸۸، رفتارهایی مانند دسترسی غیرمجاز، جعل رایانه‌ای و کلاهبرداری رایانه‌ای را جرم‌انگاری کرده است. مهم‌ترین چالش‌های این حوزه شامل پراکندگی مقررات، دشواری تعیین عنوان مجرمانه، احراز انتساب، اعتبارسنجی ادله دیجیتال، ردیابی وجوه و فرامرزی بودن جرائم سایبری است. همچنین، داده‌های بانکی، لاگ‌های سامانه، سوابق ورود و خروج کاربران و پیام‌های الکترونیکی نقش مهمی در اثبات جرم دارند. بنابراین، تقویت سازوکارهای حفظ و اعتبارسنجی ادله دیجیتال، آموزش تخصصی قضات و ضابطان، همکاری نهادهای مالی و قضایی و توسعه همکاری‌های فرامرزی ضروری است.

واژگان کلیدی: اختلاس، اختلاس سایبری، جرائم رایانه‌ای، کلاهبرداری رایانه‌ای، ادله الکترونیکی.

.مقدمه

تحول فناوری اطلاعات، شیوه ارتکاب جرائم مالی را دگرگون کرده و موجب شده است که تصاحب و انتقال غیرقانونی اموال، بدون دسترسی فیزیکی به مال و از طریق سامانه‌های بانکی و اداری امکان‌پذیر باشد. در نظام حقوقی ایران، عنوان مستقلی تحت عنوان «اختلاس سایبری» پیش‌بینی نشده و معیار اصلی تحقق اختلاس همچنان ماده ۵ قانون تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاهبرداری است؛ بنابراین، سپرده‌شدن مال به سبب وظیفه و برداشت یا تصاحب آن به نفع خود یا دیگری باید احراز شود. بااین‌حال، در صورت دخالت مرتکب در داده‌ها یا سامانه‌های رایانه‌ای، حسب نحوه ارتکاب ممکن است عناوین مجرمانه رایانه‌ای نیز مطرح شود. ازاین‌رو، صرف استفاده از رایانه برای تعیین عنوان مجرمانه کافی نیست و باید حدود دسترسی، نوع عملیات انجام‌شده، رابطه مرتکب با مال و نتیجه مالی رفتار مورد بررسی قرار گیرد. پراکندگی مقررات و نبود هماهنگی کامل میان مقررات جرائم اقتصادی و رایانه‌ای نیز از چالش‌های مهم در تشخیص عنوان مجرمانه محسوب می‌شود (زلفقاری و توانگر، ۱۳۹۸: ۱۹۸؛ یوسفی و احمدی، ۱۳۹۳: ۳۵۶؛ تولابی و همکاران، ۲۰۲۵: ۱۲). مهم‌ترین چالش اختلاس در بسترهای رایانه‌ای، کشف، اثبات و انتساب رفتار مجرمانه است؛ زیرا آثار جرم غالباً در قالب داده‌های الکترونیکی، سوابق تراکنش‌ها، گزارش فعالیت سامانه و اطلاعات ورود کاربران باقی می‌ماند. قانون تجارت الکترونیکی با پذیرش قابلیت استناد داده‌پیام، مبنای قانونی استفاده از ادله الکترونیکی را فراهم کرده است، اما احراز اصالت، تمامیت، قابلیت اعتماد و نحوه تحصیل و نگهداری این ادله همچنان اهمیت اساسی دارد (قانون تجارت الکترونیکی، ۱۳۸۲: مواد ۱۲ تا ۱۵؛ پورملایی و همکاران، ۱۴۰۳: ۱۸۳). همچنین، ثبت عملیات با نام کاربری یک فرد به‌تنهایی برای انتساب قطعی رفتار کافی نیست و عواملی مانند افشای رمز، استفاده اشخاص ثالث و نقص‌های امنیتی باید بررسی شود. در پرونده‌های فرامرزی نیز تعیین صلاحیت، حفظ و انتقال ادله و دسترسی به داده‌های خارج از قلمرو کشور، پیچیدگی بیشتری ایجاد می‌کند. بنابراین، مقابله مؤثر با این پدیده مستلزم رویکردی تلفیقی میان حقوق کیفری، مقررات جرائم رایانه‌ای، قواعد ادله، آیین دادرسی کیفری و همکاری قضایی بین‌المللی است و پژوهش حاضر با روش توصیفی ـ تحلیلی، این چالش‌ها و راهکارهای ارتقای پاسخ کیفری و قضایی به اختلاس ارتکابی از طریق سامانه‌های رایانه‌ای را بررسی می‌کند.

۲. پیشینه پژوهش

پورملایی، سالارزایی و طباطبایی (۱۴۰۳) در پژوهشی با عنوان «تحلیل حقوقی چالش‌ها و سازوکارهای اجرای ادله الکترونیکی در نظام قضایی ایران» به بررسی جایگاه ادله الکترونیکی و مشکلات مربوط به احراز اصالت، تمامیت، امنیت و قابلیت استناد آنها پرداختند. نتایج پژوهش نشان داد که کمبود زیرساخت‌های فنی، ضرورت تدوین مقررات جامع و نیاز به آموزش تخصصی قضات و فعالان حقوقی، از مهم‌ترین چالش‌های استفاده مؤثر از ادله الکترونیکی در فرایند دادرسی است. این پژوهش از حیث بررسی شیوه اثبات اختلاس ارتکابی از طریق سامانه‌های رایانه‌ای، ارتباط مستقیمی با موضوع حاضر دارد (پورملایی و همکاران، ۱۴۰۳).

تولابی، حبیبی‌تبار و رستمی نجف‌آبادی (۱۴۰۴) در پژوهشی درباره چالش‌های ماهوی سیاست جنایی ایران در قبال جرائم اقتصادی، به بررسی مشکلات ناشی از پراکندگی مقررات، نبود هماهنگی میان عناوین کیفری و دشواری انطباق مقررات موجود با تحولات جدید جرائم اقتصادی پرداختند. یافته‌های پژوهش نشان می‌دهد که تحول شیوه‌های ارتکاب جرائم مالی، ضرورت بازنگری و هماهنگ‌سازی مقررات کیفری را افزایش داده است. اهمیت این پژوهش برای تحقیق حاضر، فراهم‌کردن مبنایی برای تحلیل جایگاه اختلاس ارتکابی با استفاده از فناوری در میان مقررات جرائم اقتصادی است (تولابی و همکاران، ۱۴۰۴).

بشیری (۱۴۰۲) در پژوهشی با عنوان «تحلیل جرم‌شناختی اختلاس در بسترهای نوین» به بررسی عوامل و شرایط مؤثر بر شکل‌گیری اختلاس در محیط‌های جدید پرداخت. نتایج این پژوهش بر نقش موقعیت شغلی، میزان دسترسی به منابع مالی، سطح اختیار و ضعف سازوکارهای نظارتی در ایجاد فرصت ارتکاب اختلاس تأکید دارد. این یافته‌ها برای پژوهش حاضر اهمیت دارد؛ زیرا در اختلاس مبتنی بر سامانه‌های رایانه‌ای، دسترسی قانونی به سامانه و امکان سوءاستفاده از اختیارات سازمانی می‌تواند زمینه ارتکاب جرم را فراهم کند (بشیری، ۱۴۰۲).

کازینو و همکاران[۱] (۲۰۲۲) در پژوهشی با عنوان «بررسی نظام‌مند تحقیقات کیفری فرامرزی و ادله دیجیتال» چالش‌های حقوقی و عملی مربوط به جمع‌آوری، حفظ، تحلیل و تبادل ادله الکترونیکی در تحقیقات فرامرزی را بررسی کردند. نتایج نشان داد که تفاوت نظام‌های حقوقی، پراکندگی داده‌ها در قلمروهای مختلف و دشواری همکاری میان مراجع قضایی، از مهم‌ترین موانع تحقیقات کیفری در جرائم مبتنی بر فناوری است. این یافته‌ها در بررسی اختلاس سایبری دارای ابعاد فرامرزی و تعیین صلاحیت قضایی اهمیت ویژه‌ای دارد (کازینو و همکاران، ۲۰۲۲).

ژانگ و گونگ[۲] (۲۰۲۴) در پژوهشی با عنوان «پژوهش درباره نظام جرم‌یابی ادله الکترونیکی در جرائم سایبری فرامرزی» به بررسی روش‌های جمع‌آوری و بررسی ادله الکترونیکی در پرونده‌های فرامرزی پرداختند. پژوهش آنان نشان داد که استفاده از روش‌های نوین تحقیق باید با رعایت حاکمیت سرزمینی، تشریفات قانونی و حقوق اشخاص همراه باشد و ایجاد سازوکارهای منسجم برای همکاری میان مراجع تحقیقاتی ضروری است. این نتایج برای تحلیل چالش‌های کشف و اثبات اختلاس سایبری در موارد دارای عناصر فرامرزی قابل استفاده است (ژانگ و گونگ، ۲۰۲۴).

آدینْدا و عارفین[۳] (۲۰۲۵) در پژوهشی با عنوان «تحقیقات جرائم سایبری فرامرزی: چالش‌های حقوقی در دستیابی به ادله دیجیتال» به بررسی موانع حقوقی دسترسی مراجع تحقیقاتی به داده‌های الکترونیکی مستقر در کشورهای دیگر پرداختند. نتایج پژوهش بر مشکلات صلاحیت قضایی، همکاری قضایی متقابل، دسترسی به داده‌های ذخیره‌شده در خارج از کشور و ضرورت ایجاد سازوکارهای سریع‌تر برای تبادل ادله تأکید دارد. یافته‌های این پژوهش در بررسی اختلاس‌های سایبری فرامرزی و ضرورت توسعه همکاری قضایی بین‌المللی برای نظام حقوقی ایران قابل توجه است.

۳. مبانی مفهومی و تمایز اختلاس سایبری از جرائم مالی رایانه‌ای

۱. Casino and Associates.
۲. Zhang and Gong.
۳. Adinda and Arefin.

۱-۳-مفهوم اختلاس در حقوق کیفری ایران

اختلاس در نظام حقوق کیفری ایران از مهم‌ترین جرایم علیه اموال، سلامت نظام اداری و اعتماد عمومی محسوب می‌شود و علاوه بر ایراد خسارت به دارایی‌های عمومی یا سازمانی، می‌تواند موجب تضعیف اعتماد نسبت به اشخاصی شود که به موجب وظیفه قانونی، مسئولیت اداره، نگهداری یا تصرف در اموال عمومی را بر عهده دارند. مبنای قانونی این جرم، ماده ۵ قانون تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاهبرداری است که تحقق آن را به وجود رابطه‌ای خاص میان مرتکب، سمت قانونی وی و مال موضوع جرم منوط کرده است؛ بدین معنا که مال یا وجوه باید به سبب وظیفه و در چارچوب صلاحیت شغلی در اختیار مرتکب قرار گرفته باشد و وی سپس با عدول از حدود اختیار و تکلیف قانونی، آن را به نفع خود یا دیگری برداشت و تصاحب کند؛ بنابراین، صرف تصاحب مال متعلق به دیگری برای تحقق اختلاس کافی نیست و منشأ دسترسی، سمت مرتکب، حدود اختیار و نحوه ارتباط وی با مال باید احراز شود (قانون تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاهبرداری، ۱۳۶۷: ماده ۵). در واقع، ویژگی متمایزکننده اختلاس آن است که دسترسی اولیه مرتکب به مال، مشروع و مبتنی بر وظیفه است، اما این دسترسی مشروع در مرحله بعد به تصاحب نامشروع منتهی می‌شود و به همین دلیل، موقعیت شغلی، میزان اختیار و امکان سوءاستفاده از اعتماد سازمانی از عوامل مؤثر در شکل‌گیری فرصت ارتکاب این جرم به شمار می‌روند (بشیری، ۱۴۰۲: ۵۸). از این حیث، اختلاس با جرایمی نظیر سرقت، خیانت در امانت و کلاهبرداری تفاوت دارد؛ زیرا در سرقت، دسترسی مرتکب به مال اساساً فاقد مجوز است، در خیانت در امانت، مال بر مبنای رابطه امانی سپرده می‌شود و در کلاهبرداری، تحصیل مال معمولاً از طریق فریب و وسایل متقلبانه صورت می‌گیرد، حال آنکه در اختلاس، عنصر تعیین‌کننده، دسترسی قانونی و وظیفه‌ای مرتکب و سپس تجاوز به حدود آن از طریق برداشت یا تصاحب مال است (هادی‌تبار و یعقوبی گلوردی، ۱۴۰۲: ۱۲۵). این تمایز در محیط‌های رایانه‌ای اهمیت بیشتری می‌یابد؛ زیرا ممکن است کارمند یا مأمور دارای مجوز ورود و انجام عملیات در سامانه مالی، از همان دسترسی قانونی برای انتقال وجه، تغییر اطلاعات مالی یا انجام عملیات خارج از حدود وظیفه استفاده کند. در چنین وضعیتی، استفاده از رایانه یا سامانه الکترونیکی به‌خودی‌خود موجب تغییر عنوان اختلاس نمی‌شود، بلکه ابتدا باید ارکان مقرر در ماده ۵ قانون تشدید احراز و سپس، با توجه به نحوه رفتار، امکان انطباق آن با عناوین مجرمانه مرتبط با داده‌ها و سامانه‌های رایانه‌ای بررسی شود. قانون جرایم رایانه‌ای نیز رفتارهایی مانند دسترسی غیرمجاز، تغییر یا تخریب داده‌ها و برخی اشکال رفتار متقلبانه رایانه‌ای را مستقلاً جرم‌انگاری کرده است؛ ازاین‌رو، در پرونده‌های اختلاس ارتکابی از طریق سامانه‌های مالی و اداری، مرجع قضایی باید میان عنوان اصلی جرم و شیوه ارتکاب آن تفکیک کرده و حدود دسترسی، نوع اختیار مرتکب، نحوه ورود و استفاده از سامانه، عملیات انجام‌شده بر داده‌ها و نتیجه مالی حاصل از رفتار را به‌صورت دقیق بررسی کند (زلفقاری و توانگر، ۱۳۹۸: ۱۹۸؛ پورمولایی و همکاران، ۱۴۰۳: ۱۸۳؛ قانون جرایم رایانه‌ای، ۱۳۸۸: مواد ۱ تا ۵۴). بر این اساس، تحلیل اختلاس در بستر فناوری اطلاعات مستلزم توجه هم‌زمان به رابطه قانونی مرتکب با مال، حدود صلاحیت و اختیار وی و ویژگی‌های فنی شیوه ارتکاب است و استفاده از ابزار رایانه‌ای صرفاً زمانی می‌تواند در کنار عنوان اختلاس واجد آثار کیفری مستقل باشد که رفتار انجام‌شده، عناصر قانونی یکی از جرایم رایانه‌ای را نیز به‌طور جداگانه محقق سازد.

۲-۳- مفهوم «اختلاس سایبری»

در نظام حقوق کیفری ایران، اصطلاح «اختلاس سایبری» عنوان مجرمانه مستقلی ندارد، بلکه به وضعیتی اشاره می‌کند که در آن ارکان جرم اختلاس از طریق سامانه‌های رایانه‌ای، بانکی یا ارتباطی تحقق می‌یابد. بنابراین، مبنای اصلی تشخیص جرم همچنان ماده ۵ قانون تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاهبرداری است و استفاده از فناوری صرفاً شیوه ارتکاب را تغییر می‌دهد. در

صورتی که کارمند یا مأمور واجد شرایط قانونی، با استفاده از دسترسی مجاز خود به سامانه مالی، وجوه یا سایر اموال سپرده‌شده به سبب وظیفه را به نفع خود یا دیگری برداشت یا تصاحب کند، ابتدا باید رابطه وظیفه‌ای و سایر ارکان اختلاس احراز شود و سپس نحوه استفاده از سامانه و داده‌های رایانه‌ای مورد بررسی قرار گیرد. به همین دلیل، اقداماتی مانند انتقال الکترونیکی وجه، تغییر اطلاعات حساب، دستکاری داده‌های مالی یا ایجاد و حذف سوابق ممکن است، حسب شرایط، علاوه بر اختلاس، با برخی عناوین مقرر در قانون جرایم رایانه‌ای نیز ارتباط پیدا کند (قانون تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاهبرداری، ۱۳۶۷: ماده ۵؛ بشیری، ۱۴۰۲: ۶۹؛ هادی‌تبار و یعقوبی گلوردی، ۱۴۰۲: ۷۳) .از سوی دیگر، یکی از مهم‌ترین ویژگی‌های اختلاس سایبری، پیچیدگی کشف و اثبات آن است؛ زیرا بخش عمده آثار جرم در قالب داده‌های الکترونیکی، سوابق تراکنش‌ها، اطلاعات ورود کاربران و گزارش فعالیت سامانه باقی می‌ماند و شناسایی مرتکب و انتساب عملیات به شخص معین نیازمند بررسی تخصصی است. ویژگی‌هایی مانند سرعت انتقال و تغییر داده‌ها، امکان دسترسی از راه دور و فرامرزی‌شدن رفتار مجرمانه نیز فرایند تحقیقات کیفری را دشوارتر می‌کند (یوسفی و احمدی، ۱۳۹۳: ۳۵۵). در این میان، احراز اصالت و تمامیت ادله الکترونیکی، تعیین منشأ عملیات و نحوه تحصیل و نگهداری داده‌ها اهمیت اساسی دارد (پورمولایی و همکاران، ۱۴۰۳: ۱۷۵). بنابراین، اختلاس سایبری را باید حاصل پیوند جرم اختلاس به‌عنوان جرم پایه و فناوری رایانه‌ای به‌عنوان ابزار یا بستر ارتکاب دانست، نه عنوانی مستقل؛ رویکردی که مستلزم تحلیل هم‌زمان مقررات اختلاس، جرایم رایانه‌ای و ادله الکترونیکی و در عین حال رعایت اصل قانونی‌بودن جرایم و مجازات‌ها و حقوق دفاعی متهم است (زلفقاری و توانگر، ۱۳۹۸: ۱۹۸).

۳-۳-تمایز اختلاس سایبری و کلاهبرداری رایانه‌ای

تمایز میان اختلاس سایبری و کلاهبرداری رایانه‌ای از منظر حقوق کیفری، مستلزم توجه هم‌زمان به وضعیت مرتکب، منشأ دسترسی وی به مال، شیوه تحقق رفتار مجرمانه و نتیجه حاصل از آن است؛ زیرا صرف استفاده از سامانه‌های رایانه‌ای یا ابزارهای بانکی برای انتقال و تحصیل مال، به‌تنهایی نمی‌تواند مبنای تعیین عنوان مجرمانه قرار گیرد. در اختلاس، عنصر اساسی، وجود رابطه قانونی و وظیفه‌ای میان مرتکب و مال موضوع جرم است؛ به این معنا که مال یا وجه به سبب سمت و وظیفه در اختیار مرتکب قرار گرفته و وی با سوءاستفاده از این دسترسی، آن را به نفع خود یا دیگری برداشت و تصاحب می‌کند، در حالی که در کلاهبرداری رایانه‌ای، محور اصلی رفتار مجرمانه، استفاده متقلبانه از داده‌ها، اطلاعات یا سامانه‌های رایانه‌ای برای تحصیل مال یا منفعت مالی است و تحقق آن لزوماً متوقف بر وجود رابطه استخدامی یا سپرده‌شدن مال به مرتکب به موجب وظیفه نیست (قانون تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاهبرداری، ۱۳۶۷: ماده ۵؛ قانون جرایم رایانه‌ای، ۱۳۸۸: مقررات مربوط به کلاهبرداری رایانه‌ای). بر این اساس، اگر کارمند یک نهاد مالی یا دولتی که به اقتضای وظیفه به سامانه و حساب‌های مالی دسترسی دارد، از اختیار قانونی خود برای انتقال وجوه به حساب شخصی یا حساب دیگری استفاده کند، نخست باید رابطه وظیفه‌ای وی با مال و تحقق شرایط اختلاس احراز شود؛ اما چنانچه شخصی بدون آنکه مال به سبب وظیفه در اختیار وی قرار گرفته باشد، با ایجاد تغییرات متقلبانه در داده‌ها یا سامانه رایانه‌ای موجبات انتقال وجه و تحصیل مال را فراهم سازد، ممکن است رفتار وی تحت عنوان کلاهبرداری رایانه‌ای یا سایر عناوین مقرر در قوانین مربوط به جرایم رایانه‌ای قابل بررسی باشد. در پژوهش‌های مرتبط با جرایم رایانه‌ای نیز تأکید شده است که تشخیص صحیح عنوان کیفری در جرایم مالی رایانه‌ای نیازمند بررسی دقیق شیوه ارتکاب، نوع دسترسی مرتکب، رابطه وی با داده‌ها و سامانه و نتیجه اقتصادی رفتار است و نمی‌توان صرف وقوع انتقال مالی در بستر رایانه‌ای را دلیل تحقق یک عنوان مجرمانه خاص دانست (یوسفی و احمدی، ۱۳۹۳: ۸۴). همچنین، در تحلیل حقوقی جرایم رایانه‌ای و کلاهبرداری‌های سایبری، تفاوت میان دسترسی قانونی و استفاده مجرمانه از آن با دسترسی یا مداخله متقلبانه اشخاص فاقد اختیار، از معیارهای مهم برای تفکیک عناوین کیفری به شمار می‌رود (هادی‌تبار و یعقوبی گلوردی، ۱۴۰۲: ۱۴۸). از سوی دیگر، در پرونده‌های مالی مبتنی بر سامانه‌های رایانه‌ای، ادله الکترونیکی

مانند سوابق ورود به سامانه، گزارش تراکنش‌ها، اطلاعات ثبت عملیات و داده‌های مربوط به تغییرات انجام‌شده، می‌توانند در تعیین چگونگی وقوع جرم و انتساب رفتار به متهم نقش اساسی داشته باشند؛ بااین‌حال، اعتبار این ادله مستلزم احراز اصالت، تمامیت و قابلیت اعتماد آنهاست (پورمولایی و همکاران، ۱۴۰۳: ۱۷۹). بنابراین، در تمایز اختلاس سایبری از کلاهبرداری رایانه‌ای، مرجع قضایی باید مجموعه‌ای از عوامل شامل سمت و موقعیت مرتکب، منشأ دسترسی وی به مال و سامانه، حدود اختیار قانونی، نوع عملیات انجام‌شده، شیوه تحصیل یا انتقال مال، وجود یا فقدان وسایل متقلبانه، قصد مرتکب و رابطه میان رفتار رایانه‌ای و نتیجه مالی را به‌صورت یکپارچه بررسی کند؛ زیرا ممکن است استفاده از یک سامانه مالی در ظاهر رفتار مشابهی ایجاد کند، اما بر اساس منشأ دسترسی و نحوه ارتکاب، عنوان کیفری متفاوتی داشته باشد. ازاین‌رو، اختلاس سایبری را باید در اصل، اختلاسی دانست که ابزار یا بستر رایانه‌ای در تحقق آن نقش داشته است، در حالی که کلاهبرداری رایانه‌ای بر عنصر تقلب رایانه‌ای و تحصیل مال از طریق دستکاری یا بهره‌برداری متقلبانه از داده‌ها و سامانه‌ها استوار است؛ تفکیکی که رعایت آن برای تفسیر مضیق قوانین کیفری، جلوگیری از توسعه ناروا عناوین مجرمانه و تضمین حقوق متهم و بزه‌دیده اهمیت اساسی دارد (زلفقاری و توانگر، ۱۳۹۸: ۱۶۳؛ تولابی و همکاران، ۱۴۰۴: ۲۵۸).

۴-۳-اجتماع عناوین مجرمانه در اختلاس سایبری

در رسیدگی به اختلاس ارتکابی از طریق سامانه‌های رایانه‌ای، یکی از مسائل مهم، تعیین وضعیت تعدد یا اجتماع عناوین مجرمانه است؛ زیرا ممکن است مرتکب در یک فرایند مرتبط، علاوه بر تصاحب غیرقانونی مال، اقداماتی مانند تغییر یا حذف داده‌ها، ورود خارج از حدود اختیار به سامانه یا انتقال وجه از طریق عملیات رایانه‌ای انجام دهد. در صورتی که شرایط مقرر در ماده ۵ قانون تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاهبرداری، از جمله سپرده‌شدن مال به سبب وظیفه و برداشت یا تصاحب آن به نفع خود یا دیگری، احراز شود، عنوان اختلاس قابل طرح است و حسب نوع رفتار، عناوینی مانند دسترسی غیرمجاز، جعل یا تخریب داده‌ها، کلاهبرداری رایانه‌ای، استفاده از داده مجعول یا پولشویی نیز ممکن است مطرح شود. بنابراین، صرف استفاده از رایانه یا سامانه بانکی موجب تحقق خودکار جرایم رایانه‌ای نمی‌شود و تعیین عنوان صحیح مستلزم بررسی مستقل هر رفتار و تطبیق آن با عناصر قانونی، مادی و معنوی جرم مربوط است. این مسئله با توجه به پراکندگی و هم‌پوشانی مقررات جرایم اقتصادی و رایانه‌ای، می‌تواند موجب اختلاف در تشخیص عنوان مجرمانه و نحوه اعمال پاسخ کیفری شود (قانون تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاهبرداری، ۱۳۶۷: ماده ۵؛ قانون جرایم رایانه‌ای، ۱۳۸۸: مواد ۱ تا ۵۴؛ تولابی و همکاران، ۱۴۰۴: ۶۴) .در این چارچوب، تشخیص تعدد جرایم در اختلاس سایبری باید بر پایه تفکیک دقیق مراحل رفتار مرتکب و بررسی رابطه زمانی و ماهوی میان آنها صورت گیرد. برای نمونه، اگر شخصی با استفاده از دسترسی قانونی خود وارد سامانه شود، داده‌های مالی را تغییر دهد و سپس وجه را به نفع خود یا دیگری منتقل کند، باید مشخص شود که هر یک از این اقدامات چه عنوان کیفری مستقلی دارد و آیا رفتارها یک مجموعه واحد یا چند رفتار مستقل محسوب می‌شوند. در این فرایند، ادله الکترونیکی مانند سوابق ورود به سامانه، اطلاعات تراکنش‌ها، گزارش فعالیت کاربران و داده‌های ثبت‌شده، نقش مهمی در تعیین زمان، نحوه و انتساب هر رفتار دارند (پورمولایی و همکاران، ۱۴۰۳: ۲۸۳). ازاین‌رو، مرجع قضایی باید ابتدا هر رفتار را از حیث عناصر قانونی، مادی و معنوی بررسی و سپس قواعد مربوط به تعدد یا اجتماع جرایم را اعمال کند؛ رویکردی که ضمن جلوگیری از توسعه ناروا و انتساب عناوین کیفری بدون دلیل، مانع از نادیده‌گرفتن رفتارهای مجرمانه و تضییع حقوق بزه‌دیدگان می‌شود (هادی‌تبار و یعقوبی گلوردی، ۱۴۰۲: ۲۵؛ زلفقاری و توانگر، ۱۳۹۸: ۶۷).

۴. چالش‌های ماهوی و تقنینی اختلاس در فضای مجازی

یکی از مهم‌ترین چالش‌های ماهوی اختلاس ارتکابی در فضای مجازی، انطباق مفاهیم سنتی این جرم با ویژگی‌های غیرمادی و داده‌محور محیط‌های رایانه‌ای است. مطابق ماده ۵ قانون تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاهبرداری، تحقق اختلاس مستلزم وجود سمت و موقعیت قانونی مرتکب، سپرده‌شدن مال یا وجوه به سبب وظیفه و سپس برداشت یا تصاحب آن به نفع خود یا دیگری است (قانون تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاهبرداری، ۱۳۶۷: ماده ۵). بااین‌حال، در محیط دیجیتال، تصرف در مال می‌تواند از طریق تغییر داده‌های مالی، صدور دستور انتقال وجه یا دستکاری سوابق الکترونیکی انجام شود و بدون آنکه مال به صورت فیزیکی در اختیار مرتکب قرار گیرد، نتیجه مالی مورد نظر حاصل شود. در کنار این مسئله، پراکندگی و هم‌پوشانی مقررات اختلاس و جرایم رایانه‌ای نیز تشخیص عنوان مجرمانه را دشوار می‌سازد؛ زیرا یک رفتار ممکن است علاوه بر اختلاس، حسب شرایط با عناوینی مانند دسترسی غیرمجاز، جعل یا تغییر داده‌ها و کلاهبرداری رایانه‌ای مرتبط باشد (قانون جرایم رایانه‌ای، ۱۳۸۸: مواد ۱ تا ۵۴؛ زلفقاری و توانگر، ۱۳۹۸: ۱۹). همچنین پراکندگی مقررات در حوزه جرایم اقتصادی، ضرورت هماهنگی بیشتر میان قوانین کیفری را آشکار می‌کند (تولابی و همکاران، ۲۰۲۵: ۲۷). بنابراین، ضمن رعایت اصل قانونی‌بودن جرم و تفسیر مضیق قوانین کیفری، باید میان عنوان اصلی اختلاس و شیوه فناورانه ارتکاب آن تفکیک دقیق صورت گیرد (بشیری، ۱۴۰۲: ۵۸؛ یوسفی و احمدی، ۱۳۹۳: ۳۵). از منظر اثباتی، مهم‌ترین دشواری اختلاس رایانه‌ای، کشف، حفظ و انتساب ادله الکترونیکی است؛ زیرا آثار جرم غالباً در قالب داده‌های تراکنشی، سوابق ورود کاربران، گزارش فعالیت سامانه و اطلاعات تغییرات ثبت‌شده باقی می‌ماند. قانون تجارت الکترونیکی قابلیت استناد به داده‌پیام را پذیرفته است، اما احراز اصالت، تمامیت، قابلیت اعتماد و نحوه تحصیل و نگهداری داده‌ها همچنان اهمیت اساسی دارد (قانون تجارت الکترونیکی، ۱۳۸۲: مواد ۱۱ تا ۱۵؛ پورمولایی و همکاران، ۱۴۰۳: ۱۸). ثبت عملیات با نام کاربری یک فرد نیز به‌تنهایی برای انتساب قطعی رفتار کافی نیست و باید احتمال افشای رمز، استفاده اشخاص ثالث و ضعف‌های امنیتی بررسی شود؛ ازاین‌رو، همکاری میان ضابطان، قضات و کارشناسان فنی در کشف و ارزیابی ادله ضروری است (نوح و همکاران، ۲۰۱۹: ۲۵۸). افزون بر این، فرامرزی‌بودن برخی جرایم رایانه‌ای، مسائل مربوط به صلاحیت کیفری، دسترسی به داده‌های خارج از کشور، حفظ ادله و همکاری قضایی بین‌المللی را مطرح می‌کند (کازینو و همکاران، ۲۰۲۲: ۹۸). در این زمینه، کنوانسیون مقابله با جرایم سایبری، پروتکل الحاقی دوم و کنوانسیون سازمان ملل متحد درباره مقابله با جرایم سایبری بر توسعه همکاری دولت‌ها و تسهیل دسترسی و تبادل ادله الکترونیکی تأکید دارند (شورای اروپا، کنوانسیون مقابله با جرایم سایبری؛ شورای اروپا، پروتکل الحاقی دوم؛ سازمان ملل متحد، ۲۰۲۴). بنابراین، پاسخ مؤثر به اختلاس در فضای مجازی مستلزم هماهنگی مقررات ماهوی و آیین دادرسی، تقویت نظام ادله الکترونیکی، آموزش تخصصی و توسعه همکاری‌های قضایی داخلی و بین‌المللی است.

۵. ادله الکترونیکی و چالش‌های اثبات اختلاس سایبری

در پرونده‌های اختلاس ارتکابی در بستر سامانه‌های رایانه‌ای، ادله الکترونیکی نقش اساسی در کشف و اثبات جرم دارد؛ زیرا آثاری مانند سوابق تراکنش‌ها، اطلاعات ورود کاربران، گزارش فعالیت سامانه، تغییرات داده‌ها و سایر داده‌های ذخیره‌شده می‌توانند نحوه وقوع جرم و ارتباط آن با متهم را نشان دهند. قانون تجارت الکترونیکی نیز با پذیرش قابلیت استناد داده‌پیام، مبنای حقوقی استفاده از این ادله را فراهم کرده است، اما ارزش اثباتی آنها منوط به احراز اصالت، تمامیت، قابلیت اعتماد و نحوه صحیح تحصیل و نگهداری است (قانون تجارت الکترونیکی، ۱۳۸۲: مواد ۱۱ تا ۱۵؛ پورملائی، سالارزایی و طباطبایی، ۱۴۰۳: ۴۸). از مهم‌ترین چالش‌ها نیز انتساب عملیات رایانه‌ای به شخص معین است؛ زیرا ثبت یک تراکنش با نام کاربری یا حساب فرد، به‌تنهایی اثبات‌کننده انجام عملیات توسط وی نیست و عواملی مانند افشای رمز عبور، استفاده اشخاص دیگر از تجهیزات، ضعف‌های امنیتی و دسترسی از راه دور باید بررسی شود. بنابراین، کشف و اثبات اختلاس سایبری مستلزم استفاده از مجموعه‌ای هماهنگ از قرائن فنی و قضایی و بهره‌گیری از روش‌های جرم‌یابی دیجیتال است (فیانی، ۲۰۱۶: ۷۴؛ نوح و همکاران، ۲۰۱۹: ۶۷). از سوی دیگر، حفظ تمامیت و زنجیره نگهداری

ادله الکترونیکی از زمان کشف تا ارائه به مرجع قضایی اهمیت ویژه‌ای دارد؛ زیرا این داده‌ها به‌راحتی قابلیت تغییر، حذف یا جابه‌جایی دارند و هرگونه نقص در فرایند جمع‌آوری و نگهداری می‌تواند اعتبار اثباتی آنها را با تردید مواجه سازد (فرویس و همکاران[۴]، ۲۰۱۹: ۷۱؛ پورمولایی، سالارزایی و طباطبایی، ۱۴۰۳: ۱۴۲). در پرونده‌های فرامرزی نیز تفاوت قوانین کشورها، پراکندگی داده‌ها و محدودیت‌های صلاحیت سرزمینی، دسترسی و حفظ ادله را دشوارتر می‌کند و همکاری قضایی بین‌المللی را ضروری می‌سازد (کازینو و همکاران، ۲۰۲۲: ۱۱۴؛ شورای اروپا، کنوانسیون مقابله با جرایم سایبری؛ شورای اروپا، پروتکل الحاقی دوم؛ سازمان ملل متحد، ۲۰۲۴). در نتیجه، اثبات اختلاس سایبری در نظام حقوقی ایران نیازمند ترکیب قواعد حقوقی و آیین دادرسی با تخصص فنی، استانداردسازی فرایند جمع‌آوری و حفظ ادله، آموزش قضات و ضابطان و توسعه همکاری‌های بین‌المللی است؛ به‌گونه‌ای که ضمن افزایش توان کشف و اثبات جرم، اصالت و تمامیت ادله و حقوق دفاعی متهم نیز تضمین شود.

۶. چالش‌های آیین دادرسی و کشف جرم

کشف و تعقیب اختلاس ارتکابی در بستر سامانه‌های رایانه‌ای، به دلیل ماهیت داده‌محور و سرعت تغییر یا حذف آثار جرم، با چالش‌های خاص آیین دادرسی کیفری مواجه است. برخلاف اختلاس سنتی که اسناد مادی و دفاتر مالی نقش بیشتری دارند، در اختلاس سایبری بخش مهمی از ادله در قالب سوابق تراکنش‌ها، اطلاعات ورود کاربران و داده‌های سامانه‌ای باقی می‌ماند؛ بنابراین، سرعت عمل در کشف، جمع‌آوری و حفظ قانونی داده‌ها اهمیت ویژه‌ای دارد (قانون آیین دادرسی کیفری، ۱۳۹۲؛ قانون جرایم رایانه‌ای، ۱۳۸۸؛ قانون تجارت الکترونیکی، ۱۳۸۲: مواد ۱۱ تا ۱۵). در عین حال، احراز هویت واقعی مرتکب و انتساب عملیات رایانه‌ای به وی از مسائل اساسی است؛ زیرا استفاده از یک حساب کاربری یا ابزار دسترسی، به‌تنهایی اثبات‌کننده انجام عملیات توسط صاحب آن نیست. ازاین‌رو، بررسی سوابق ورود و خروج، زمان و نوع عملیات، سطح دسترسی، تجهیزات مورد استفاده و سایر قرائن فنی و بهره‌گیری از کارشناسی تخصصی برای بازسازی فرایند وقوع جرم ضروری است (فیانی، ۲۰۱۶: ۱۴۷؛ نوح و همکاران، ۲۰۱۹: ۶۵). همچنین، اصالت، تمامیت و نحوه تحصیل و نگهداری ادله باید احراز شود تا ارزش اثباتی آنها حفظ و حقوق دفاعی متهم نیز رعایت گردد (پورمولایی، سالارزایی و طباطبایی، ۱۴۰۳: ۲۹). در پرونده‌هایی که اختلاس سایبری دارای ابعاد فرامرزی است، دشواری‌های آیین دادرسی افزایش می‌یابد؛ زیرا ممکن است داده‌ها، زیرساخت‌های سامانه‌ای و حساب‌های مقصد در کشورهای مختلف قرار داشته باشند و دسترسی به اطلاعات نیازمند همکاری قضایی و رعایت مقررات کشور محل نگهداری داده باشد. تفاوت نظام‌های حقوقی، محدودیت صلاحیت سرزمینی و خطر حذف یا تغییر سریع اطلاعات، از موانع مهم تحقیقات کیفری فرامرزی محسوب می‌شوند (کازینو و همکاران، ۲۰۲۲: ۶۳). در این زمینه، کنوانسیون مقابله با جرایم سایبری و پروتکل الحاقی دوم آن، بر همکاری میان دولت‌ها و تسهیل دسترسی قانونی به ادله الکترونیکی تأکید دارند و کنوانسیون سازمان ملل متحد درباره مقابله با جرایم سایبری مصوب ۲۰۲۴ نیز همکاری بین‌المللی و تبادل ادله الکترونیکی را مورد توجه قرار داده است (شورای اروپا، کنوانسیون مقابله با جرایم سایبری؛ شورای اروپا، پروتکل الحاقی دوم؛ سازمان ملل متحد، ۲۰۲۴). بنابراین، افزایش کارآمدی رسیدگی به اختلاس سایبری مستلزم تکمیل مقررات آیین دادرسی، آموزش تخصصی قضات و ضابطان، استانداردسازی فرایند جمع‌آوری و حفظ ادله و تقویت همکاری قضایی بین‌المللی است؛ مشروط بر آنکه تمامی اقدامات تحقیقی با رعایت اصل قانونی‌بودن، حریم خصوصی، اصل برائت، حقوق دفاعی متهم و تناسب اقدامات کیفری انجام شود.

[۴] Frois et al..

۷.سیاست جنایی و راهکارهای مقابله با اختلاس سایبری

مقابله مؤثر با اختلاس ارتکابی در بستر سامانه‌های رایانه‌ای و ارتباطی، مستلزم اتخاذ سیاست جنایی منسجم و چندلایه‌ای است که هم‌زمان ابعاد تقنینی، پیشگیرانه، کشف جرم، تعقیب کیفری و رسیدگی قضایی را دربرگیرد. در نظام حقوقی ایران، اگرچه عنوان مستقلی تحت نام «اختلاس سایبری» پیش‌بینی نشده است، اما رفتارهای ارتکابی را می‌توان حسب مورد تحت مقررات ماده ۵ قانون تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاهبرداری و مقررات ناظر بر جرائم رایانه‌ای تحلیل کرد. چالش اساسی آن است که قوانین موجود عمدتاً به‌صورت پراکنده و در قالب عناوین مجرمانه مختلف، رفتارهای مرتبط با تعرض به اموال، داده‌ها و سامانه‌های رایانه‌ای را مورد حکم قرار داده‌اند؛ ازاین‌رو، تعیین عنوان مجرمانه دقیق، تشخیص نسبت میان جرائم و جلوگیری از تداخل یا توسعه ناروا در عناوین کیفری اهمیت فراوان دارد. در این زمینه، پژوهش‌های انجام‌شده درباره سیاست جنایی ایران در قبال جرائم اقتصادی بر پراکندگی مقررات، دشواری هماهنگ‌سازی مقررات کیفری و ضرورت بازنگری در سیاست تقنینی تأکید کرده‌اند (تولابی، حبیبی‌تبار و رستمی نجف‌آبادی، ۱۴۰۳: ۳۷). همچنین مطالعات مربوط به سیاست جنایی ایران در حوزه جرائم رایانه‌ای نشان می‌دهد که تحول سریع فناوری، ضرورت به‌روزرسانی مستمر مقررات و ایجاد سازوکارهای تخصصی برای شناسایی و مقابله با رفتارهای مجرمانه نوین را افزایش داده است (زلفقاری و توانگر، ۱۳۹۳، ۵۸). بنابراین، یکی از مهم‌ترین راهکارها، ایجاد هماهنگی تقنینی میان مقررات اختلاس، جرائم رایانه‌ای، ادله الکترونیکی و جرائم اقتصادی است تا در پرونده‌هایی که یک رفتار واحد واجد چند وصف کیفری است، حدود مسئولیت کیفری و نحوه اعمال مقررات به‌صورت روشن و قابل پیش‌بینی مشخص باشد. در کنار اصلاحات تقنینی، پیشگیری وضعی از طریق محدودسازی دسترسی کارکنان به سامانه‌های مالی، تفکیک وظایف، ثبت و نگهداری سوابق عملیات مالی، کنترل چندمرحله‌ای تراکنش‌های حساس و نظارت مستمر بر دسترسی کاربران می‌تواند نقش مهمی در کاهش فرصت ارتکاب جرم داشته باشد. اهمیت این اقدامات از آن جهت است که در جرائم مالی رایانه‌ای، مرتکب غالباً از اختیارات و مجوزهای قانونی موجود سوءاستفاده می‌کند و بنابراین پیشگیری صرفاً با افزایش مجازات کیفری تحقق نمی‌یابد، بلکه باید ساختارهای اداری و فنی تولیدکننده فرصت جرم نیز اصلاح شوند (بشیری، ۹۶:۱۴۰۲ ؛ هادی‌تبار و یعقوبی گلوردی، ۱۴۰۲: ۸۷). از منظر کشف، اثبات و تعقیب کیفری نیز مقابله با اختلاس سایبری نیازمند تقویت تخصص قضایی و فنی و ایجاد سازوکارهای استاندارد برای جمع‌آوری، حفظ، بررسی و ارائه ادله الکترونیکی است. قانون تجارت الکترونیکی با پذیرش داده‌پیام و شناسایی ارزش اثباتی آن، زمینه حقوقی استفاده از سوابق الکترونیکی را فراهم کرده و قانون جرائم رایانه‌ای نیز ابزارهای کیفری لازم برای برخورد با تعرض به داده‌ها و سامانه‌های رایانه‌ای را پیش‌بینی کرده است؛ بااین‌حال، در پرونده‌های اختلاس سایبری، صرف وجود یک سابقه رایانه‌ای برای انتساب رفتار مجرمانه کافی نیست و باید اصالت، تمامیت، منشأ، زمان ایجاد، نحوه نگهداری و ارتباط آن با رفتار متهم احراز شود (قانون تجارت الکترونیکی، ۱۳۸۲، مواد ۱۱ تا ۱۵؛ قانون جرائم رایانه‌ای، ۱۳۸۸). پژوهش‌های مرتبط با ادله الکترونیکی نیز بر اهمیت احراز اصالت و قابلیت اعتماد داده‌ها و ضرورت وجود سازوکارهای روشن برای جمع‌آوری و ارزیابی آنها در فرایند قضایی تأکید دارند (پورملائی، سالارزایی و طباطبایی، ۳۳:۱۴۰۳). از سوی دیگر، تجربه‌های بین‌المللی نشان می‌دهد که در جرائم سایبری، به‌ویژه زمانی که داده‌ها یا حساب‌های مورد استفاده در خارج از قلمرو یک کشور قرار دارند، همکاری قضایی و انتظامی میان دولت‌ها اهمیت اساسی پیدا می‌کند؛ زیرا ادله الکترونیکی ممکن است در کوتاه‌ترین زمان در حوزه‌های قضایی مختلف ایجاد، منتقل یا حذف شوند (کازینو و همکاران، ۲۰۲۲: ۳۴). کنوانسیون بوداپست و پروتکل الحاقی دوم آن نیز بر تقویت همکاری بین‌المللی، دسترسی سریع‌تر به ادله الکترونیکی و ایجاد سازوکارهای هماهنگ برای مقابله با جرائم سایبری تأکید دارند. در سطح ملی نیز ضروری است واحدهای تخصصی برای رسیدگی به جرائم مالی مبتنی بر فناوری تقویت شوند و قضات، ضابطان و کارشناسان رسمی دادگستری از آموزش‌های مستمر در

زمینه سامانه‌های بانکی، تحلیل تراکنش‌ها، ردیابی داده‌ها و جرم‌یابی دیجیتال برخوردار باشند. افزون بر این، حفظ زنجیره نگهداری ادله و جلوگیری از تغییر یا دستکاری داده‌های کشف‌شده باید به‌عنوان یکی از الزامات اساسی فرایند اثبات مورد توجه قرار گیرد؛ زیرا هرگونه خدشه در نحوه تحصیل یا نگهداری داده‌ها می‌تواند اعتبار استنادی آنها را با تردید مواجه سازد (فیانی، ۲۰۱۶: ۱۵؛ فرویس و همکاران، ۲۰۱۹: ۱۳۵). بر این اساس، سیاست جنایی مطلوب در برابر اختلاس سایبری باید از رویکرد صرفاً واکنشی و مجازات‌محور فاصله گرفته و به سمت سیاستی جامع حرکت کند که پیشگیری سازمانی، اصلاح مقررات، تخصصی‌سازی نهادهای کشف و رسیدگی، تضمین اعتبار ادله الکترونیکی و گسترش همکاری‌های قضایی داخلی و بین‌المللی را به‌صورت هم‌زمان دنبال کند.

۸. تحلیل تطبیقی و همکاری بین‌المللی

ماهیت فرامرزی جرائم مالی در فضای مجازی، به‌ویژه اختلاس سایبری، فرایند کشف جرم، شناسایی مرتکب، حفظ ادله و تعقیب کیفری را با دشواری‌های جدی مواجه می‌کند؛ زیرا داده‌ها، زیرساخت‌های سامانه‌ای و حساب‌های مالی مرتبط با جرم ممکن است در چند کشور قرار داشته باشند. در چنین شرایطی، همکاری قضایی و انتظامی بین‌المللی، حفظ فوری داده‌ها و تبادل سریع اطلاعات اهمیت اساسی دارد. کنوانسیون جرائم سایبری شورای اروپا، معروف به کنوانسیون بوداپست، با پیش‌بینی سازوکارهایی برای حفظ داده‌ها، مساعدت قضایی متقابل و همکاری میان دولت‌ها، یکی از مهم‌ترین چارچوب‌های بین‌المللی در این زمینه محسوب می‌شود و نشان می‌دهد که مقابله مؤثر با اختلاس سایبری صرفاً به جرم‌انگاری داخلی محدود نیست، بلکه به سازوکارهای مطمئن برای دسترسی و انتقال قانونی ادله الکترونیکی نیز نیاز دارد (کازینو و همکاران، ۲۰۲۲: ۶۴؛ شورای اروپا، کنوانسیون جرائم سایبری). پروتکل دوم الحاقی کنوانسیون بوداپست نیز با هدف تسهیل دسترسی فرامرزی به ادله الکترونیکی، همکاری با ارائه‌دهندگان خدمات، واکنش سریع در شرایط اضطراری و تقویت همکاری میان مراجع تحقیقاتی طراحی شده است و در عین حال بر رعایت حقوق بنیادین و حمایت از داده‌های شخصی تأکید دارد. در سطح جهانی نیز کنوانسیون سازمان ملل متحد علیه جرائم سایبری در سال ۲۰۲۴ به تصویب رسید که همکاری بین‌المللی و اشتراک‌گذاری ادله الکترونیکی را مورد توجه قرار داده است؛ بااین‌حال، مطابق وضعیت رسمی ثبت‌شده در ژوئیه ۲۰۲۶، این کنوانسیون هنوز لازم‌الاجرا نشده است. بنابراین، برای نظام حقوقی ایران، بهره‌گیری از تجارب بین‌المللی در زمینه حفظ فوری داده‌ها، ایجاد سازوکارهای تخصصی همکاری قضایی، ارتباط با ارائه‌دهندگان خدمات و انتقال قانونی ادله می‌تواند موجب افزایش کارآمدی مقابله با اختلاس سایبری شود؛ مشروط بر آنکه این اقدامات هم‌زمان با رعایت حریم خصوصی، حمایت از داده‌ها، اصل قانونی‌بودن اقدامات کیفری و حقوق دفاعی متهم همراه باشد (پورملائی، سالارزایی و طباطبایی، ۱۴۰۳: ۲۵؛ غاسمی، ۲۰۱۲: ۴۴؛ شورای اروپا، پروتکل الحاقی دوم؛ سازمان ملل متحد، ۲۰۲۴).

۹. چالش‌های قضایی در رسیدگی به پرونده‌های اختلاس سایبری

رسیدگی قضایی به پرونده‌های اختلاس ارتکابی در بستر سامانه‌های رایانه‌ای و بانکی، به دلیل هم‌زمانی مسائل ماهوی، شکلی و فنی، با چالش‌های قابل‌توجهی مواجه است؛ زیرا در این پرونده‌ها، مرجع قضایی افزون بر احراز عناصر اختصاصی جرم اختلاس، از جمله سمت و وضعیت خاص مرتکب، سپرده‌شدن مال یا وجوه به وی به سبب وظیفه و قصد تصاحب یا برداشت غیرقانونی، باید نحوه استفاده از سامانه، حدود دسترسی مرتکب، چگونگی ایجاد یا تغییر داده‌ها، مسیر انتقال وجوه و ارتباط میان رفتار دیجیتال و نتیجه مالی حاصل‌شده را نیز احراز کند (بشیری، ۱۴۰۲: ۶۴ هادی‌تبار و یعقوبی گلوردی، ۱۴۰۲: ۲۶). پیچیدگی اصلی در این زمینه آن است که بخش مهمی از آثار جرم نه در قالب اسناد سنتی، بلکه در قالب داده‌های ثبت‌شده در سامانه‌های بانکی و مالی، گزارش‌های ورود و خروج کاربران، سوابق تراکنش‌ها، نشانی‌های شبکه‌ای، اطلاعات ثبت‌شده در پایگاه‌های داده و سایر آثار الکترونیکی باقی می‌ماند؛ ازاین‌رو، اعتبار، تمامیت، اصالت و قابلیت انتساب این داده‌ها به شخص مرتکب از اهمیت اساسی برخوردار است و هرگونه

نقص در فرایند جمع‌آوری، حفظ، انتقال یا تحلیل آنها می‌تواند ارزش اثباتی ادله را با تردید مواجه سازد (پورملائی، سالارزایی و طباطبایی، ۱۴۰۳: ۲۵؛ قانون تجارت الکترونیکی، ۱۳۸۲، مواد ۱۲ تا ۱۵). از سوی دیگر، تخصص فنی مورد نیاز برای تفسیر داده‌های رایانه‌ای و پیوند دادن آنها با رفتار مجرمانه، ضرورت بهره‌گیری از ضابطان و کارشناسان متخصص و انجام اقدامات دقیق برای حفظ ادله را افزایش می‌دهد؛ زیرا صرف مشاهده یک تراکنش یا ورود به حساب کاربری، بدون احراز انتساب و ارتباط آن با قصد مجرمانه، برای اثبات مسئولیت کیفری کافی نیست (یوسفی و احمدی، ۱۳۹۳: ۲۴؛ پورمولایی، سالارزایی و طباطبایی: ۷۱). همچنین در مواردی که رفتار مرتکب واجد عناوین متعدد کیفری باشد، دادگاه باید با تفکیک دقیق رفتارهای ارتکابی، میان اختلاس، جعل یا تغییر داده‌های رایانه‌ای، دسترسی غیرمجاز، کلاهبرداری رایانه‌ای و سایر عناوین احتمالی تمایز ایجاد کند و از انتساب عنوان کیفری صرفاً بر مبنای استفاده از فناوری پرهیز نماید؛ بنابراین، رسیدگی مؤثر به این دسته از پرونده‌ها مستلزم ترکیب تحلیل حقوقی عناصر جرم با ارزیابی فنی ادله الکترونیکی، رعایت قواعد دادرسی کیفری، حفظ زنجیره نگهداری ادله، احراز اصالت و تمامیت داده‌ها و در صورت فرامرزی بودن بخشی از ادله، استفاده از سازوکارهای همکاری قضایی بین‌المللی است (زلفقاری و توانگر، ۲۰۱۹: ۸۴؛ کازینو و همکاران، ۲۰۲۲: ۳۹؛ شورای اروپا، کنوانسیون جرائم سایبری، سند شماره ۱۸۵). در نتیجه، چالش قضایی اصلی در پرونده‌های اختلاس سایبری صرفاً فقدان مقررات نیست، بلکه هماهنگ‌سازی قواعد حقوق کیفری سنتی با الزامات اثباتی و فنی محیط دیجیتال، ارتقای تخصص قضات و ضابطان، تضمین قابلیت استناد به داده‌های الکترونیکی و ایجاد رویه‌ای منسجم برای ارزیابی این ادله است؛ امری که می‌تواند دقت تشخیص قضایی، جلوگیری از انتساب ناروا و در عین حال کشف مؤثر جرایم مالی پیچیده را تضمین کند (تولابی، حبیبی‌تبار و رستمی نجف‌آبادی: ۲۱؛ فاینی، ۲۰۱۶: ۴۷).

۱۰. نتیجه‌گیری

گسترش فناوری اطلاعات و تحول ساختار سامانه‌های مالی و اداری، شیوه ارتکاب جرائم علیه اموال را دستخوش تغییر کرده و زمینه ظهور اشکال نوینی از سوءاستفاده مالی را فراهم آورده است؛ با این حال، در حقوق کیفری ایران عنوان مستقلی تحت نام «اختلاس سایبری» پیش‌بینی نشده و رایانه‌ای یا الکترونیکی بودن شیوه ارتکاب، به‌خودی‌خود موجب ایجاد عنوان مجرمانه جدید نمی‌شود. ازاین‌رو، مبنای اصلی تشخیص اختلاس همچنان ماده ۵ قانون تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاهبرداری است و احراز رابطه استخدامی یا سمت قانونی مرتکب، سپرده‌شدن مال یا وجوه به وی به سبب وظیفه و سپس برداشت، تصاحب یا مصرف آن به نفع خود یا دیگری، در تعیین وصف کیفری رفتار نقشی اساسی دارد. در مواردی که ارتکاب این رفتار با تعرض به داده‌ها، سامانه‌های رایانه‌ای یا فرایندهای الکترونیکی همراه باشد، حسب مورد مقررات مربوط به جرائم رایانه‌ای، جعل یا دستکاری داده‌ها، دسترسی غیرمجاز، کلاهبرداری رایانه‌ای و سایر عناوین قانونی نیز قابل بررسی خواهد بود؛ بنابراین، در تحلیل حقوقی این پدیده باید میان «عنوان مجرمانه» و «شیوه فناورانه ارتکاب» تفکیک قائل شد. مهم‌ترین چالش در این حوزه نیز اثبات رفتار مجرمانه است؛ زیرا در بسیاری از موارد، مال موضوع جرم بدون جابه‌جایی فیزیکی و از طریق تغییر اطلاعات، ثبت دستورهای الکترونیکی یا انتقال وجوه در سامانه‌های مالی مورد تعرض قرار می‌گیرد و آثار رفتار مجرمانه در داده‌پیام‌ها، سوابق تراکنش‌ها، گزارش‌های سامانه‌ای و سایر داده‌های الکترونیکی باقی می‌ماند. ازاین‌رو، احراز اصالت، تمامیت، قابلیت انتساب و نحوه تحصیل و نگهداری ادله الکترونیکی، در کنار تعیین رابطه میان شخص و عملیات انجام‌شده در سامانه، از ارکان اساسی فرایند اثبات محسوب می‌شود. بر مبنای این ملاحظات، سیاست جنایی مؤثر در برابر اختلاس ارتکابی با استفاده از فناوری، نمی‌تواند صرفاً بر تشدید ضمانت اجراهای کیفری استوار باشد، بلکه باید مجموعه‌ای هماهنگ از اقدامات تقنینی، قضایی، فنی و پیشگیرانه را دربرگیرد. تدوین دستورالعمل‌های تخصصی برای کشف و رسیدگی به جرائم مالی مبتنی بر فناوری، ایجاد استانداردهای ملی برای جمع‌آوری، حفظ و ارزیابی ادله الکترونیکی، آموزش تخصصی قضات، بازپرسان و ضابطان، تقویت همکاری میان دستگاه قضایی، بانک‌ها، نهادهای اجرایی و کارشناسان فناوری اطلاعات، و توسعه

سازوکارهای همکاری قضایی بین‌المللی در زمینه دسترسی و تبادل داده‌های الکترونیکی، از الزامات اساسی این سیاست محسوب می‌شود. در سطح پیشگیری نیز اجرای اصل تفکیک وظایف در سامانه‌های مالی، محدودسازی دسترسی کاربران بر مبنای وظایف، استفاده از سازوکارهای احراز هویت چندمرحله‌ای، ثبت و نگهداری منظم سوابق فعالیت کاربران و نظارت مستمر بر تراکنش‌های غیرعادی می‌تواند احتمال وقوع جرم و دامنه خسارات ناشی از آن را کاهش دهد. همچنین، بازنگری مستمر مقررات با توجه به تحولات فناوری و تفکیک دقیق اختلاس از عناوینی مانند کلاهبرداری رایانه‌ای، جعل رایانه‌ای و دسترسی غیرمجاز، به انسجام رویه قضایی و جلوگیری از تفسیرهای نادرست کمک خواهد کرد. در نهایت، مقابله مؤثر با اختلاس در بستر فناوری مستلزم تلفیق سه محور اساسی، یعنی تفسیر و اجرای صحیح مقررات کیفری، ارتقای ظرفیت‌های فنی کشف و اثبات جرم و تقویت پیشگیری فناورانه در ساختار سازمان‌هاست؛ زیرا امنیت سامانه‌ها، مدیریت صحیح سطوح دسترسی، کشف سریع رفتارهای مشکوک، حفظ اصولی ادله و همکاری تخصصی میان نهادهای ذی‌ربط، در کنار ضمانت اجراهای کیفری، اجزای ضروری یک سیاست جنایی کارآمد و متناسب با ماهیت متحول جرائم مالی در عصر فناوری اطلاعات به شمار می‌روند.

منابع

الف)کتب ومقالات

۱ .انصاری، یاسر؛ موسوی‌فرد، سیدمحمدرضا؛ نقی‌مخلص‌آبادی، مرجان؛ اختری، سجاد؛ و غفاری، مجتبی. (۲۰۲۵). «سیاست جنایی جمهوری اسلامی ایران در مواجهه با فیلترینگ محتوای جرائم سایبری با تأکید بر مسائل اقتصادی»

۲ .بشیری، محمد. (۱۴۰۲). تحلیل جرم‌شناختی اختلاس در بسترهای نوین. تهران: انتشارات میزان.

۳ .پورمولایی، علیرضا؛ سالارزایی، امیرحمزه؛ و طباطبایی، سعیدشرف‌الدین. «تحلیل حقوقی چالش‌ها و سازوکارهای اجرای ادله الکترونیکی در نظام قضایی ایران». مطالعات حقوقی در عصر دیجیتال.

۴ .پورملائی، علی؛ سالارزایی، مریم؛ و طباطبایی، سیدحسن. (۱۴۰۳). چالش‌های حقوقی ادله الکترونیکی در جرایم مالی. تهران: انتشارات خرسندی.

۵ .تولابی، بهروز؛ حبیبی‌تبار، محمود؛ و رستمی نجف‌آبادی، حامد. «چالش‌های ماهوی سیاست جنایی ایران در قبال جرایم اقتصادی». مطالعات حقوقی در عصر دیجیتال.

۶ .زلفقاری، سهیل؛ و توانگر، علی. (۲۰۱۹). «سیاست تقنینی جمهوری اسلامی ایران در قبال جرایم سایبری». مجله بین‌المللی چندرشته‌ای زندگی ناب، جلد ۶، شماره ۱۹، صص. ۱۶۳ـ۱۹۸.

۷ .غاسمی، قاسم. (۲۰۱۲). «جرایم سایبری در ایران: دیدگاه‌ها، سیاست‌ها و قوانین». در کتاب جرایم سایبری: یافتن تعادل میان آزادی و امنیت.

۸ .هادی‌تبار، رضا؛ و یعقوبی گلوردی، مریم. (۱۴۰۲). بررسی ابعاد حقوقی جرایم رایانه‌ای و کلاهبرداری‌های سایبری. تهران: انتشارات دادگستر.

۹ .یوسفی، زاهد؛ و احمدی، احمد. (۲۰۱۵). «بررسی کلاهبرداری رایانه‌ای در نظام عدالت کیفری ایران». مجله علمی دانشکده علوم و ادبیات دانشگاه جمهوریت، جلد ۳۶، شماره ۳.

ب)قوانین و مقررات

۱۰ .قانون آیین دادرسی کیفری. (۱۳۹۲) و اصلاحات بعدی.

۱۱ .قانون تجارت الکترونیکی. (۱۷/۱۰/۱۳۸۲)، به‌ویژه مواد ۱۱ تا ۱۵ در خصوص سوابق و ادله الکترونیکی.

۱۲ .قانون جرایم رایانه‌ای. (۰۵/۰۳/۱۳۸۸)، مواد ۱ تا ۵۴؛ الحاق‌شده به قانون مجازات اسلامی در قالب مواد ۷۲۹ تا ۷۸۲.

۱۳ .قانون تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاهبرداری. (۱۵/۰۹/۱۳۶۷)، مصوب مجمع تشخیص مصلحت نظام، به‌ویژه ماده ۵.

۱۴. قانون مجازات اخلالگران در نظام اقتصادی کشور. (۱۹/۰۹/۱۳۶۹) و اصلاحات بعدی.

۱-Bada, Masarah؛ Nurse, Jason R. C. (۲۰۲۱). Profiling the Cybercriminal: A Systematic Review of Research.

۲-Casino, Fran؛ Pina, Chiara؛ López-Aguilar, Pablo؛ Batista, Eduardo؛ Solanas, Agusti؛ Patsakis, Constantinos (۲۰۲۲). SoK: Cross-border Criminal Investigations and Digital Evidence.

۳-Choshen, Leshem؛ Eldad, Daniel؛ Hershcovich, Daniel؛ Sulem, Elior؛ Abend, Omri (۲۰۱۹). The Language of Legal and Illegal Activity on the Darknet.

۴-Fianyi, Israel D. (۲۰۱۵). Curbing Cyber-Crime and Enhancing E-Commerce Security with Digital Forensics.

۵-Fröwis, Michael؛ Gottschalk, Thilo؛ Haslhofer, Bernhard؛ Rückert, Christian؛ Pesch, Paulina (۲۰۱۹/۲۰۲۰). Safeguarding the Evidential Value of Forensic Cryptocurrency Investigations.

۶-Mauko, Elina؛ Johnson, Shane D.؛ Mariconti, Enrico (۲۰۲۶). Cybercrime as a Service: A Scoping Review.

۷-Nouh, Mahmoud؛ Nurse, Jason R. C.؛ Webb, Helena؛ Goldsmith, Michael (۲۰۱۹). Cybercrime Investigators are Users Too! Understanding the Socio-Technical Challenges Faced by Law Enforcement.

۸-Council of Europe. Convention on Cybercrime (Budapest Convention), CETS No. ۱۸۵.

۹-Council of Europe / Eurojust. Second Additional Protocol to the Budapest Convention on Cybercrime and Cross-Border Access to Electronic Evidence.

۱۰-United Nations. (۲۰۲۴). United Nations Convention against Cybercrime: Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes.