فصلنامه علمی-پژوهشی
فقه و مبانی حقوق اسلامی
دانشگاه آزاد اسلامی واحد بناب
The Scientific Research Journal in Jurisprudence and Bases of Islamic law The 12 rd. Year/NO: 2 / summer 2019
فصلنامه علمی ، پژوهشی فقه و مبانی حقوق اسلامی سال دوازدهم / شماره ۲ / تابستان۱۳۹۸

تاریخ دریافت: ۹۷/۰۱/۲۲
تاریخ بازنگری: ۹۷/۱۱/۰۹
تاریخ پذیرش: ۹۸/۰۳/۱۱
تاریخ انتشار : ۹۸/۰۶/۰۱

بررسی مجازات های سرقت سایبری در حقوق ایران

سید محسن رضوی اصل [۱]

چکیده

سرقت سایبری از نظر ماهوی با سرقت سنتی تفاوتی نداشته و تنها تفاوت در محیط ارتکاب جرم موجب تمایز میان این دو نوع سرقت شده است در حالی که هر دو جرم در عناصر تشکیل دهنده مشترک بوده و تعریف فقهی و حقوقی سرقت شامل هر دوی آن ها می‌گردد. در بررسی کیفر سرقت سایبری در حقوق ایران مشاهده می‌شود که با توجه به رابطه عموم و خصوص میان دو جرم سرقت رایانه‌ای و سایبری، سرقت‌های سایبری مشمول مجازات‌های تعیین شده در قانون جرایم رایانه‌ای می‌باشند، ولیکن در این تحقیق که به شیوه توصیفی- تحلیلی انجام شده است هدف آن بوده که مشخص گردد که با توجه به تنوع و پیچیدگی نحوه ارتکاب سرقت‌های سایبری و ناشناخته بودن بیشتر جنبه‌های فضای سایبر، قانون‌گذار نتوانسته است با توجه به واقعیات موجود اقدام به تعیین مجازات‌های این نوع از سرقت بنماید و در همین راستا، تحلیل مواد قانون جرایم رایانه‌ای چنین نشان می‌دهد که مجازات‌های تعیین شده در این قانون، با توجه به وسعت خسارات ناشی از سرقت‌های سایبری، از بازدارندگی لازم برخوردار نبوده و علاوه بر تفاوت فاحش میان مجازات سارقان سایبری با سارقان سنتی، حتی در خود قانون جرایم رایانه‌ای تفاوت میان مجازات‌های اشخاص حقیقی و حقوقی نیز مشهود بوده و قانون گذار در مورد چالش هایی چون حدّ سرقت نیز سکوت کرده است.

واژگان کلیدی: سرقت سایبری؛ سرقت اینترنتی؛ قانون جرایم رایانه‌ای؛ حقوق موضوعه؛ مجازات‌ها

۱. مقدمه

با توجه به گستره‌ی استفاده از بستر فضای سایبری و بروز روش‌های جدید ارتکاب جرم و پیچیدگی‌های فضای مجازی و استفاده از روش‌های نوین ارتکاب جرم توسط مجرمان سایبری، به نظر می‌رسد قوانین و مقرّرات بازدارندگی لازم را نداشته و در عمل تناسبی میان جرم و مجازات ایجاد نشده است. فرض پژوهش حاضر این است که این چالش در کشور ما نیز وجود دارد.بررسی‌های انجام شده در خصوص سرقت‌های سایبری نشان می‌دهد که در همه آن‌ها چهار شرط اساسی سرقت موجود می‌باشد که عبارتند از: ۱. برداشتن مال ۲. از آن دیگری بودن مال مسروقه؛ ۳. پنهانی بودن عمل سرقت و ٤. منقول بودن مال مسروقه؛ و همچون سرقت‌های سنتی به طور منطقی چنانچه یکی از شروط یاد شده مفقود شود، مفهوم سرقت تحقّق پیدا نمی‌کند. عناصر تشکیل دهنده جرم نیز در سرقت‌های سایبری محقّق می‌باشند که عبارتند از: عنصر قانونی، عنصر مادی و عنصر معنوی یا روانی. لذا پرسش اصلی این تحقیق که به شیوه توصیفی_تحلیلی به روش کتابخانه‌ای انجام شده است و به دنبال پاسخ‌گویی به آن می‌باشد این است که با وجود ارکان و عناصر مشترک میان جرم سرقت در فضای سایبری با محیط فیزیکی و عدم وجود تفاوت ماهوی میان این دو نوع سرقت، آیا مجازات‌های تعیین شده برای اشخاص حقیقی یا حقوقی که مرتکب سرقت سایبری می‌گردند، متناسب با بزه انتسابی آن‌ها بوده و از توان بازدارندگی کافی برخوردارمی‌باشد؟ لذا در این تحقیق ابتدا ماده۱۲ قانون جرایم رایانه‌ای بررسی و سپس مجازات‌های اصلی و تبعی اشخاص حقیقی و حقوقی در این قانون مورد بحث و بررسی قرار خواهند گرفت و در نهایت چالش امکان یا عدم امکان اجرای حدّ سرقت از نظر فقهای معاصر مورد تحلیل قرار می‌گیرد و در پایان جمع‌بندی مطالب بیان می‌گردد.

۲. جرم‌انگاری سرقت‌های سایبری

رابطه میان سرقت‌های رایانه‌ای و سرقت‌های سایبری عموم و خصوص می‌باشد زیرا امروزه یکی از کاربردهای اینترنت، ایجاد یک فضای مجازی و یا به اصطلاح سایبری در کنار دنیای واقعی است و طبیعی است که در این دنیای مجازی و سایبری نیز همانند دنیای واقعی جرایمی رخ می دهد که یکی از آن جرایم سرقت می‌باشد. بنابراین سرقت‌های سایبری را می توان زیرمجموعه ای از سرقت های اینترنتی و به تبع آن، زیرمجموعه‌ای از جرایم رایانه

۱ – دکتری فقه و مبانی حقوق اسلامی، قم، ایران. پست الکترونیکی:mohsen.razavy@gmail.com

ای قلمداد کرد و به همین دلیل نسل سوم جرایم رایانه‌ای را به طور خاص، جرایم سایبری نامیده اند؛ ولیکن ممکن است یک سرقت به وسیله رایانه ولی در خارج از فضای سایبر رخ دهد که در این صورت یک سرقت رایانه‌ای می‌باشد، اما یک سرقت سایبری نیست. البته به سبب آن که در حال حاضر اهمّ جرایم رایانه ای را جرایم سایبری تشکیل می‌دهند، می‌توان آن را معادل جرایم رایانه‌ای در مفهوم عام و همچنین معادل و مترادف جرایم اینترنتی قلمداد کرد، چنان که کنوانسیون اروپایی جرایم سایبر این نام را انتخاب کرده و جرایم رایانه‌ای را به عنوان یکی از زیرمجموعه های خود آورده است.(جاویدنیا،۱۳۸۷)تمام این تفکیک ها از این نظر است که در حال حاضر فضای مجازی تبدیل به فضای سایبری چندرسانه ای شده است و شاید با پیشرفت فن آوری اطلاعات و ارتباطات در آینده ای نه چندان دور، فضای سایبری نیز جای خود را به فضای دیگری داده و در نتیجه نسل جدیدی از جرایم متولد و ایجاد شوند.

در ایران با تصویب قانون جرایم رایانه‌ای، ماده۱۲ این قانون در فصل‌سوم، با عنوان «سرقت و کلاهبرداری مرتبط با رایانه» به بیان حکم جرم سرقت رایانه‌ای پرداخته است که شامل سرقت‌های سایبری نیز می‌شود، زیرا در این ماده از قید واژه «برباید» سرقت به ذهن متبادر می گردد و توجه به معنا و منطوق این ماده مبیّن این مسئله است که ماده مذکور به جرم‌انگاری سرقت‌های رایانه‌ای و سایبری پرداخته است و این نکته بیان‌گر آن است که قانون‌گذار به این مطلب توجه نموده که سرقت با استفاده از رایانه و در فضای مجازی امکان پذیر می باشد و قید غیرمجاز حاکی از رخ دادن آن به صورت پنهانی و بدون اجازه مالک اطلاعات می‌باشد، چون اگر فردی که مالک اطلاعات می باشد متوجه ورود غیرمجاز دیگر کاربران به سیستم رایانه ای خود گردد، اقدام به جلوگیری از دسترسی غیرمجاز آن‌ها نموده و دسترسی چنین افرادی را به اطلاعات غیرممکن می‌سازد. پس قید غیرمجاز حاکی از در نظر گرفتن سرقت رایانه‌ای و سایبری در زمره اعمال پنهانی و مخفیانه می‌باشد و اگر عمل با اطلاع و اجازه مالک اطلاعات و سیستم رایانه‌ای باشد، جرم سرقت محقّق نمی گردد تا مستوجب مجازات باشد. البته گاهی سرقت سایبری در حالی انجام می‌شود که مالک اطلاعات متوجه سرقت می‌گردد ولی توانایی مقابله با آن را ندارد. پس می توان سرقت های سایبری را به دو دسته آشکار و پنهان دسته بندی نمود.

هم‌چنین قانون‌گذار قید «هرکس» را به کار برده است که می‌توان آن را به اشخاص حقیقی و حقوقی تسرّی داد، زیرا مباشرین سرقت‌های سایبری اعم از اشخاص حقیقی و حقوقی می‌باشند و اگر شائبه عدم مسئولیت کیفری اشخاص حقوقی مطرح شود، با توجه به کلی بودن ماده ۱۹ قانون جرایم رایانه‌ای و مجازات‌های تعیین شده در ماده ۲۰ این قانون، می‌توان چنین استنتاج نمود که قید «هرکس» عام بوده و شامل هر دو شخص حقیقی و حقوقی می‌شود. در این قانون، سرقت رایانه‌ای که موضوع ماده ۱۲ این قانون می باشد در کنار کلاهبرداری رایانه‌ای که موضوع ماده ۱۳ این قانون است، در کنار هم قرار گرفته‌اند و عده‌ای دلیل این مطلب را وجود بیشترین سازگاری میان این دو جرم دانسته اند.(عالی پور،۱۳۹۰) در خصوص تفاوت میان این دو جرم، سؤالی که مطرح می شود این است که اگر شخصی با ورود به سیستم رایانه ای یک بانک، وجوهی را از حساب دیگری به حساب خود انتقال دهد، آیا چنین موردی سرقت محسوب می شود یا کلاهبرداری؟ در نوع سنتی این جرایم تفاوت بسیار روشن است، زیرا آنچه در تحقّق عنوان کلاهبرداری مهم است تحصیل مال دیگران به روشی متقلّبانه است، یعنی هر چند در دزدی یا خیانت در امانت نیز بردن مال غیر مطرح است، ولی در جرم کلاهبرداری بردن مال غیر با انجام عملیات متقلّبانه صورت می‌گیرد و در واقع به دلیل اغفال، صاحب مال یا وکیل و یا امین وی مال را به کلاهبردار می‌دهد.(بوشهری،۱۳۸۷) ولیکن در سرقت های اینترنتی در واقع کسی که توانسته به سیستم و شبکه رایانه‌ای مورد نظر وارد شود، با دست کاری داده‌ها نوعی سندسازی و جعل انجام می‌دهد، به گونه‌ای که به نظر می‌رسد در حسابش مقداری پول وارد شده است. یعنی سارق نفوذ کننده به سیستم، کدهای ورود اطلاعات را پیدا کرده و داده‌های خودساخته را جایگزین می‌کند. تغییر در اطلاعات یکی از مهم‌ترین نوع حمله‌های اینترنتی به شمار می‌رود و در آن، کاربر اطلاعات تغییریافته را دریافت کرده و بدون اطلاع از تغییر، آن‌ها را مورد استفاده قرار می‌دهد.(محبوبی،۱۳۸۱)؛ برخی در تمایز و تفکیک میان سرقت اینترنتی و کلاهبرداری اینترنتی گفته‌اند که کلاهبرداری اینترنتی در مفهوم عام خود شامل سرقت اینترنتی نیز می‌شود، اما از آنجایی که سرقت اینترنتی ناظر به سرقت داده‌ها و فایل‌هاست، علاوه بر این که یک جرم رایانه‌ای محض محسوب می‌شود، موضوع آن نیز صرفاً مال نیست و در ماده ۱۲ قانون جرایم رایانه‌ای نیز اشاره‌ای به مالی بودن داده‌ها و ارزش داشتن آن‌ها نشده است و در نتیجه همه انواع داده‌ها را در بر می‌گیرد. در نتیجه از همین مجرا بین کلاهبرداری اینترنتی که منتج به تحصیل مال یا منافع مالی است و سرقت اینترنتی که منجر به ربودن داده‌ها و فایل‌های رایانه‌ای می‌شود، تفاوت حاصل می‌شود. مطابق نظر این عده، در واقع رایانه و اینترنت در کلاهبرداری اینترنتی «وسیله ارتکاب جرم» و در سرقت اینترنتی «موضوع ارتکاب جرم» است.(الهی منش،۱۳۹۱)

لیکن بهتر است گفته شود که وجه تمایز بین این دو جرم در داده، وجه و یا منافع مالی نیست، بلکه تفاوت بین این دو در اعمال تقلّب و عدم تقلّب است. ممکن است شخصی با توسل به تقلّب، پولی را از حساب دیگری بردارد و یا بدون هیچ تقلّبی پول دیگری را به حساب خودش انتقال دهد. علاوه بر آن، سرقت اینترنتی متفاوت از دسترسی غیرمجاز است، زیرا در دسترسی غیرمجاز لازم نیست که مالی برده شود، بلکه صرف نفوذ برای تحقّق جرم کافی است، در حالی که در سرقت، ربودن مال شرط اصلی تحقّق جرم سرقت است و ممکن است در مواردی نفوذ غیرمجاز مقدمه جرم سرقت اینترنتی گردد.(بای،۱۳۸۸) به دلیل همین پیچیدگی‌هاست که در بسیاری از مواقع قانون‌گذاران نیز میان این دو جرم تفاوتی قائل نشده اند(بجنوردی،۱۳۹۲) و بدون اشاره مستقیم به عنوان جرم، در ماده ۱۲ قانون مذکور از واژه «ربودن» برای رساندن مفهوم سرقت استفاده کرده‌اند و در ماده ۱۳ نیز از عبارت «تحصیل

وجه، مال، منفعت، خدمات و امتیازات» برای القاء مفهوم کلاهبرداری بهره برده شده است. ولی نه در ماده ۱۲ و نه در ماده ۱۳ قانون جرایم رایانه‌ای مستقیماً نامی از سرقت و کلاهبرداری برده نشده است و این عدم تصریح قانون گذار نشان دهنده سختی کار تفکیک میان این دو نوع جرم می‌باشد. از آنچه بیان گردید می توان چنین نتیجه گرفت که در فصل سوم قانون جرایم رایانه‌ای ماده ۱۲ به جرم سرقت اختصاص دارد و لذا جهت واکاوی مجازات-های جرم سرقت رایانه‌ای و به تبع آن، جرم سرقت سایبری می‌بایست به تحلیل این ماده پرداخت.

۳.تحلیل مجازات های اشخاص حقیقی

در بررسی مجازات های مشخص شده برای جرم سرقت در قانون جرایم رایانه‌ای می بایست میان مجازات‌های در نظر گرفته شده برای اشخاص حقیقی و حقوقی، همان‌گونه که در قانون مجازات اسلامی مصوّب ۱۳۹۲ بیان شده است، قائل به تفکیک شد و در هر کدام از این دو نیز مجازات ها را به تفکیک مجازات های اصلی و مجازات‌های تکمیلی و تبعی مورد بررسی قرار داد.

۳-۱ مجازات اصلی

بر طبق ماده ۱۲ قانون جرایم رایانه ای«هر کس به طور غیرمجاز داده‌های متعلّق به دیگری را برباید، چنانچه عین داده‌ها در اختیار صاحب آن باشد، به جزای نقدی از یک میلیون ریال تا بیست میلیون ریال و در غیر این صورت به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون ریال تا بیست میلیون ریال یا هر دو مجازات محکوم می‌شود.» با توجه به ارزش مالی بسیاری از داده‌ها و اطلاعاتی که در فضای سایبر به سرقت می‌روند، می‌توان گفت که مجازات تعیین شده رقم ناچیزی می‌باشد. در این خصوص توجه به نظریه انتخاب عقلانی شایان توجه است. بر اساس این نظریه، مرتکب جرم فردی حسابگر است که قبل از انجام هر کاری اقدام به محاسبه سود و زیان و خطرات عمل خود می کند.(رضوی،۱۳۹۵) بنابراین تمایل وی به ارتکاب جرم به دلیل شرایط سخت زندگی و یا تحت شرایط اضطراری نامتعارف قرار داشتن، نیست؛ بلکه دلیل ارتکاب جرم توسط یک فرد با انگیزه، در یک محاسبه منافع احتمالی ناشی از ارتکاب یک عمل خلاف است که موجب می شود کسب سود بر خطرات ناشی از آن جرم برتری یابد. نظریه انتخاب عقلانی، نشان داده است که اکثر مجرمین قبل از هر اقدامی که بخواهند انجام دهند، به عواقب آن فکر می‌کنند، حتی برای یک لحظه هم که شده باشد، مزایا و هزینه‌های ارتکاب جرم را در نظر می‌گیرند.

حال در ماده ۱۲ قانون جرایم رایانه‌ای برای کسی که به طور غیرمجاز اقدام به سرقت داده های دیگران با استفاده از نسخه‌برداری کرده است، فقط مجازات نقدی قرار داده و جنبه اخلال در نظم عمومی کشور، به ویژه ایجاد اختلال در جریان سالم اطلاعات و گردش‌های مالی را که از این طریق حاصل می‌شود، نادیده گرفته است و این به جز خسارات معنوی و روحی است که به مالک اصلی داده‌ها و اطلاعات نسخه‌برداری شده وارد می‌شود. در صورتی نیز که اصل داده‌ها در اختیار مالک اصلی نبوده و سارق با انتقال داده‌ها به سیستم خود یا هر سیستم دیگر، مالک را از دسترسی به داده‌های خود محروم سازد، چه مالک بتواند بعد از سرقت و انتقال داده‌ها از سیستم رایانه‌ای یا وب سایت خود، با استفاده از برنامه‌های مخصوص اقدام به بازگرداندن داده ها نماید، به گونه ای که اصل داده ها باز هم در اختیار مالک اصلی قرار بگیرد، و چه مالک توان بازگرداندن داده های انتقال یافته را به هر دلیل نداشته باشد، سارق به مجازات حبس از نود و یک روز تا یک سال و یا جزای نقدی از پنج میلیون تا بیست میلیون ریال یا هر دو مجازات محکوم خواهد شد که به نظر می رسد این مجازات ها نیز به نسبت بسیاری از سرقت هایی که در فضای مجازی رخ می دهند، از بازدارندگی لازم برخوردار نبوده و نمی تواند مرتکبین را به مجازاتی متناسب با جرم ارتکاب یافته برساند، به گونه ای که میان جرم ارتکابی و منافع حاصله از آن با مجازات های تعیین شده نوعی تناسب منطقی وجود داشته باشد. لذا به نظر می رسد که ماده ۱۲ قانون جرایم رایانه‌ای به لحاظ تعیین دو نوع مجازات متفاوت، حداقل در خصوص سرقت‌های سایبری با ابهام مواجه است، یعنی اگر عین داده‌ها در اختیار صاحب آن باشد، تنها مجازات نقدی وضع می‌گردد و اگر داده ها در اختیار صاحب آن نباشد، حبس یا جزای نقدی یا هر دو. در مورد این که از نظر میزان جزای نقدی در مورد دوم مقدار جزای نقدی بیشتری تعیین شده است، می‌توان این گونه توجیه نمود که در حوزه فن آوری های اطلاعاتی و ارتباطی با مفاهیمی از قبیل نسخه برداری یا انتقال در رابطه با داده‌ها و فایل‌ها مواجه هستیم و وقتی یک کاربر فایلی را نسخه برداری می کند، در واقع رونوشتی از آن فایل را در اختیار گرفته و می تواند آن را به هر فضای مورد نظرش منتقل کند. وی حتی قادر خواهد بود که تعداد زیادی از نسخه های مذکور را در فضاهای مختلف ذخیره و مورد پردازش قرار دهد. اما در حالت انتقال، کاربر اصل داده و یا فایل را از فضای حافظه برداشته و آن را به یک فضای دلخواه دیگر منتقل می کند به گونه ای که در فضای قبلی دیگر داده ای موجود نمی باشد. در نتیجه در قسمت اول ماده ۱۲ به مفهوم نسخه برداری و در قسمت دوم آن به مفهوم انتقال اشاره می شود و به همین دلیل قسمت اول شامل حالتی است که اصل داده ها کماکان در اختیار و دسترس مالک یا متصرف قانونی آن قرار دارد و در قسمت دوم، وی از داشتن داده ها محروم شده است. از بررسی این ماده چنین استنتاج می گردد که در قسمت اول این ماده با نادیده گرفتن مسأله «تناسب جرم و مجازات» مواجه هستیم، زیرا در بسیاری موارد، داده هایی که

متعلّق به دیگری است هنگامی که در اختیار صاحبش باشد بسیار ارزشمندتر و حیاتی تر از حالت دوم می باشد، و این در حالی است که در قانون جرایم رایانه ای مرتکب جرم نسخه برداری، مجازات سبک تری را نسبت به حالت انتقال داده ها تحمّل خواهد کرد.(الهی‌منش،۱۳۹۱)

مطابق ماده ٢١٤ و ٢١٥ قانون مجازات اسلامی، در سرقت‌های سنتی سارق مکلّف به ردّ عین مال مسروقه یا مثل و یا قیمت آن و جبران خسارات وارده می باشد، یعنی مجرم باید مالی را که در اثر ارتکاب جرم تحصیل کرده است، اگر موجود باشد عین آن را و اگر موجود نباشد مثل آن را و در صورت عدم امکان ردّ مثل، قیمت آن را به صاحبش رد کند و از عهده خسارات وارده نیز برآید و هرگاه از حیث جزائی وجهی بر عهده مجرم قرار بگیرد، استرداد اموال و تأدیه خسارت مدعیان خصوصی بر آن مقدّم است. از طرف دیگر چون سرقت های سایبری از لحاظ ماهیت متفاوت از سرقت-های سنتی نمی باشند، در این گونه از سرقت ها نیز سارق باید علاوه بر تحمّل مجازات های تعیین شده برای وی، داده ها و فایل های ربوده شده را هم به مالک اصلی برگردانده و اصل آن ها را نیز به گونه ای از روی سیستم محل ذخیره سازی اطلاعات مسروقه پاک کند که قابل بازیابی مجدّد نباشند. لازم به ذکر است موارد مشارکت و معاونت در سرقت سایبری همان مواد ۱۲۵و ١٢٦ قانون مجازات اسلامی است؛ بنابراین در این خصوص تفاوتی میان جرایم سنتی سرقت و سرقت سایبری وجود ندارد.

۲-۳ مجازات تکمیلی و تبعی

با توجه به اتحاد ماهوی سرقت های سنتی و سایبری، در سرقت های سایبری دادگاه می تواند سارق را در تکمیل مجازات های مقرّر در ماده ۱۲ قانون جرایم رایانه ای، به مجازات های تکمیلی ذکر شده در ماده ۲۳ قانون مجازات اسلامی محکوم نماید، برخلاف ماده ٦٢ قانون مجازات اسلامی مصوّب ۱۳۷۰، مشروط بر آن که عین داده ها در اختیار مالک اصلی نباشد، زیرا حداقل حبس لازم برای محرومیت از حقوق اجتماعی، مطابق بند ۳ ماده ٦٢ قانون مجازات اسلامی قدیم سه سال بود، در حالی که در قانون مجازات اسلامی جدید در صورت محکومیت به مجازات های تعزیری درجه شش تا درجه یک، می توان مجازات های تکمیلی و تبعی را اعمال نمود و مجازات های تعزیری درجه شش شامل حبس از شش ماه تا دو سال می باشند و همان طور که پیش از این بیان گردید، مطابق بخش دوم ماده ۱۲ قانون جرایم رایانه ای، مجازات حبس در سرقت های سایبری در صورت عدم دسترسی مالک به اصل داده ها، حداکثر یک سال می باشد، لذا مجازات های ماده ۲۳ فوق الذکر شامل سارقان سایبری نیز می گردد. همچنین با توجه به موارد فوق الذکر، مجازات های تبعی بیان شده در ماده ۲۵ قانون مجازات اسلامی شامل سرقت های سایبری نخواهد شد زیرا این مجازات ها حداکثر تا مجازات های تعزیری درجه ۵ را شامل می شوند که آن هم برای حبس بیش از دو سال یا جزای نقدی بیش از هشتاد میلیون ریال می باشد، مگر آن که سرقت های سایبری دارای جمیع شرایط اجرای حدّ را مشمول اجرای حدّ بدانیم که در این صورت سارق در چنین سرقتی مشمول مجازات تبعی ذکر شده در بند «ب» ماده ۲۵ قانون مجازات اسلامی نیز خواهد شد. حال با توجه به ماده ۲۳ قانون مجازات اسلامی که بیان داشته مجازات تکمیلی باید متناسب با جرم ارتکابی و خصوصیات آن تعیین شود؛ به نظر می رسد در خصوص سرقت سایبری بتوان بند (پ) "منع از اشتغال به شغل، حرفه، یا کار معین" و بند (ر) "توقیف وسایل ارتکاب جرم یا رسانه یا موسسه ی دخیل در ارتکاب جرم" را به عنوان مجازات تکمیلی تعیین نمود. زیرا یکی از اهداف مجازات های تکمیلی جلوگیری و پیشگیری از تکرار جرم توسط مجرم است. حال برای میل به این مقصود، کنترل ابزارهای ارتکاب جرم (کنترل تسهیل کننده ها) نقش بسیار موثری می تواند ایفا کند. منظور از ابزارهای جرم هر گونه سلاح، ابزار، مواد و سایر وسایلی است، که برای ارتکاب جرم لازم بوده و وقوع جرم را، هموار و تسهیل می‌کند و سبب می شود مجرمین بالقوه تشویق به ارتکاب جرم شوند. کنترل تسهیل کننده های وقوع جرم شامل تدابیری است که ناظر به محدود ساختن وسایل ارتکاب جرم برای مقابله با گذر اندیشه به عمل مجرمانه است. البته باید توجه داشت که هر چند اصولاً وسیله در ارتکاب بسیاری از جرایم نقش چندانی ندارد، اما جرایم سایبری مقید به وسیله هستند و وسیله در آن ها نقش کلیدی ایفاء می کند. مقید به وسیله بودن جرایم سایبری، بستر مناسبی برای پیشگیری از آن فراهم می نماید، زیرا استفاده از رایانه و تجهیزات مورد نیاز جهت اتصال و ورود به فضای سایبری، لازم و ضروری است. هنگامی که محدودیت های فنی بر ابزارهای ارتکاب جرم سایبری مانند بند (ر)، اعمال شود وقوع جرایم سایبری می تواند کاهش ملموسی داشته باشد.

٤.تحلیل مجازات های اشخاص حقوقی

علاوه بر فراوانی جرایم در اینترنت و فضای سایبر که خود سبب گستردگی مسئولیت کیفری است، فراوانی اشخاص حقوقی در این محیط نیز مرزهای مسئولیت کیفری را گسترده تر نموده است و به همین جهت، در فضای سایبری که کنش-گران عمده آن اشخاص حقوقی هستند، مسئولیت کیفری این گونه اشخاص از بایسته های بنیادین حقوق کیفری سایبری است. هر چند شکل گیری فضای مجازی اینترنت دست آورد تحقیقات و پروژه های علمی دولتی است، ولی دیگر نمی توان دولت ها را مالکان و حتی کنترل کنندگان آن به حساب آورد، به نحوی که در بررسی تقابل میان بخش خصوصی و بخش دولتی، باید حاکمان فضای مجازی را بخش خصوصی دانست. به عنوان مثال شرکت های ارائه دهنده خدمات جستجو مانند گوگل و یاهو بدون داشتن پیوند مستقیم با دولت ها، اقدام به آموزش شیوه تعامل درست با فضای سایبر به کاربران می-نمایند، تا آنجا که پا را فراتر گذاشته و به

دولت های قدرتمندی مانند چین به خاطر اعمال محدودیت در آزادی های فضای سایبر هشدار می دهند.(عالی پور،۱۳۹۰،ص۵۳) در قوانین ایران تا قبل از تصویب قانون مجازات اسلامی در سال ۱۳۹۲، مسئولیت کیفری اشخاص حقوقی به صورت پراکنده در قوانین موضوعه مورد پذیرش قرار گرفته بود. یکی از مهم ترین فواید پیش بینی مسئولیت کیفری برای اشخاص حقوقی، چه در قانون جرایم رایانه ای و چه در سایر قوانین، تضمین سلامت اشخاص حقوقی از راه اجبار سهام داران به دقت در انتخاب مدیران و واداشتن مدیران به دقت بیشتر در انتخاب مدیران میانی و به تبع آن کارکنان می باشد. علاوه بر آن، فواید دیگری از قبیل جبران بهتر خسارت افراد زیان دیده از فعالیت شخص حقوقی، اجرای کامل تر عدالت اجتماعی و ... را نیز برای مسئولیت کیفری اشخاص حقوقی برشمرده اند که با تصویب قانون مجازات اسلامی جدید در سال ۱۳۹۲، این موضوع به صراحت مورد پذیرش قرار گرفته است و در صورتی که در یک جرم، شخص حقوقی بر اساس ماده ۱۴۳ این قانون مسئول شناخته شود، با توجه به شدّت جرم ارتکابی و نتایج زیان بار آن به مجازات های تعیین شده برای اشخاص حقوقی محکوم می شود. ولی باید توجه نمود که مسئولیت شخص حقوقی و محکومیت وی مانع از مجازات شخص حقیقی نیست. برای مجرم دانستن شخص حقوقی باید انتساب عمل مجرمانه عمدی به وی محرز بوده و عنصر معنوی جرم و سوءنیّت وی احراز شود. ولی اگر احراز نشود و سوءنیّت به شخص حقوقی قابل انتساب نباشد، شخص حقوقی مجرم شناخته نمی شود. لیکن قصور و تقصیر شخص، اعم از حقیقی و حقوقی، در جرایم غیرعمدی موجب مسئولیت مدنی وی می شود. از مجازات های تعزیری ماده ۱۹ قانون مجازات اسلامی، حبس و شلاق که قابل اعمال بر شخص حقیقی است، بر شخص حقوقی قابل اعمال نیست، ولی بر مدیران اشخاص حقوقی قابل اعمال است. مجازات های این ماده طبق تبصره آن در مورد اشخاص حقوقی دولتی و یا عمومی غیردولتی در مواردی که اعمال حاکمیت می کنند، اعمال نمی شوند. لذا اگر اشخاص حقوقی با توجه به شرایط بیان شده در ماده ۱۹ قانون جرایم رایانه ای به ارتکاب جرم سرقت سایبری محکوم بشوند، مجازات های تعیین شده در ماده ۲۰ این قانون شامل آن ها خواهد بود. به همین دلیل در ادامه، مجازات اشخاص حقوقی که به سرقت سایبری مبادرت می نمایند، به تفکیک مجازات های اصلی و مجازات های تکمیلی و تبعی مورد بررسی قرار می گیرد.

۱-٤ مجازات اصلی

در ایران نقش گسترده ای که ارائه دهندگان خدمات سایبری در فضای مجازی ایفا می نمایند و تعداد فراوان آن ها سبب شد تا قانون گذار مسئولیت کیفری اشخاص حقوقی را در فضای سایبری به روشنی بپذیرد.(عالی پور،۱۳۹۰) بنابراین اگر شخص حقیقی مرتکب سرقت سایبری، مدیر یک شرکت یا سازمان بوده، یا به دستور مدیر خود و یا با اطلاع وی و در راستای منافع شرکت یا سازمان متبوع خود اقدام به سرقت سایبری نماید، شخص حقوقی یعنی سازمان یا شرکت مورد نظر، به جرم سرقت سایبری محاکمه خواهد شد. البته مطابق تبصره ۲ این ماده، محکومیت شخص حقوقی رافع مسئولیت شخص حقیقی نبوده و وی نیز به مجازات مندرج در ماده ۱۲ قانون جرایم رایانه ای خواهد رسید و مجازات وی به عنوان شخص حقیقی، علاوه بر مجازات شخص حقوقی خواهد بود. در واقع، ماده ۱۹ این قانون تفکیک میان مسئولیت کیفری اشخاص حقوقی از حقیقی را در گرو احراز سه مؤلفه دانسته است که همه آن ها باید در کنار هم وجود داشته باشند.

مؤلفه نخست آن که جرم رایانه ای به نام شخص حقوقی انجام شود. در حقوق موضوعه، شخص حقوقی هر شرکت یا مؤسسه ای می باشد که به ثبت رسیده باشد و اگر یک شرکت یا مؤسسه به ثبت نرسیده باشد، از نگاه قانون شخصیت نداشته و هر گروه یا هیأتی که در پیکره یک شرکت یا مؤسسه مرتکب جرم شوند، بر پایه قاعده های عمومی حقوق کیفری پیگرد می شوند. با این حال به نظر می رسد که میان شخص حقوقی در حقوق کیفری با شخص حقوقی در روابط خصوصی و تجاری باید قائل به تفاوت بود، زیرا در روابط تجاری، قانون تجارت به شرکت های تجاری شخصیت حقوقی بخشیده است و همچنان که ماده ۵۸۳ این قانون می گوید، کلیه شرکت های تجاری مذکور در این قانون شخصیت حقوقی دارند. این ماده و ماده ٥٨٤ نشان می دهند که قانون گذار، شرکت های تجاری به ثبت نرسیده را یک شخص حقوقی می داند، ولی چنین شخصیتی را برای یک شرکت غیرتجاری قائل نمی باشد. بر پایه ماده ٥٨٤ قانون تجارت، تشکیلات و مؤسساتی که برای مقاصد غیرتجارتی تأسیس شده یا بشوند، از تاریخ ثبت در دفتر ثبت مخصوصی که وزارت عدلیه معیّن خواهد کرد، شخصیت حقوقی پیدا می کنند. بنابراین اگر جرایم رایانه ای را شرکت های غیرتجاری ثبت شده یا شرکت های تجاری، اعم از ثبت شده یا ثبت نشده، انجام دهند، شخص حقوقی دارای مسئولیت کیفری می باشد و در این حال، شرکت های غیرتجاری ثبت نشده از بار مسئولیت کیفری می گریزند.

مطابق مفاد ماده ۱۹ قانون جرایم رایانه ای، مؤلفه دیگر برای مسئولیت کیفری شخص حقوقی آن است که جرم رایانه–ای در راستای سود و منافع آن شخص حقوقی انجام شود. به سخن دیگر، بزه ارتکابی باید بهره ای برای شرکت به همراه داشته باشد و این نشان می دهد که اگر در میان کارها و کنش های تجاری یا غیرتجاری شرکت، جرم رایانه ای نیز رخ دهد، سبب مسئولیت کیفری شخص حقوقی نمی گردد، مگر این که ثابت شود که انجام آن به سود شخص حقوقی بوده است.

مؤلفه سوم برای مسئولیت شخص حقوقی در جرایم رایانه ای، انجام رفتار از سوی افراد وابسته به شخص حقوقی است که می تواند به چهار حالت نمود یابد: ۱. مدیر شخص حقوقی مرتکب جرم رایانه ای شود. ۲. مدیر شخص حقوقی دستور ارتکاب جرم رایانه ای را صادر کند و جرم نیز به وقوع بپیوندد. ۳. یکی از کارمندان شخص حقوقی با اطلاع مدیر یا در اثر عدم نظارت وی، مرتکب جرم رایانه ای شود. ٤. تمام یا قسمتی از فعالیت های شخص حقوقی به ارتکاب جرم رایانه–ای اختصاص یافته باشد.(عالی پور،۱۳۹۰) مطابق تبصره ۱ ماده ۱۹ قانون جرایم رایانه ای، منظور از مدیر کسی است که اختیار نمایندگی یا تصمیم گیری یا نظارت بر شخص حقوقی را دارد. از آن جا که مدیر سمت و سو دهنده اراده شخص حقوقی است، اگر با وجود دو مؤلفه دیگر که پیش تر بیان شد، یعنی به نام شخص حقوقی و نیز در راستای منافع آن بودن، جرم رایانه ای را انجام دهد، مانند آن است که شخص حقوقی، خود این جرم را مرتکب شده است. به نظر می رسد چون قانون گذار در این تبصره از قید «کسی» استفاده کرده است، تعریف بیان شده از مدیر فاقد جامعیت و مانعیت لازم شده است. این تعریف جامع افراد نمی باشد، زیرا مطابق ماده ۱۱۰ لایحه اصلاحی قانون تجارت مصوّب ۱۳٤۷، اشخاص حقوقی نیز می توانند مدیر باشند، در حالی که واژه «کسی» شامل اشخاص حقوقی نمی شود و به حکم تبادر و قضاوت عرف، ظهور در اشخاص حقیقی دارد.

هم چنین تعریف مذکور مانع اغیار نمی باشد، چون این تعریف از مدیر شامل مجامع عمومی و بازرسان شرکت های سهامی نیز می گردد و این افراد به ترتیب قادر به تصمیم گیری و نظارت بر شخص حقوقی می باشند. لذا بهتر می باشد که در اصلاحات بعدی، در این تبصره از واژه «شخصی» به جای «کسی» در تعریف مدیر شخص حقوقی استفاده شود. حال اگر مدیر شخص حقوقی دستور ارتکاب جرم رایانه ای را صادر کرده و جرم نیز به وقوع پیوسته باشد، چون مدیر جزء معنوی و سبب انجام جرم می باشد و همچنین عمل مجرمانه در راستای انجام دستور او بوده است، مانند آن است که خود مدیر عمل مجرمانه را از طریق دیگری انجام داده است. در صورتی که فردی به صورت هم زمان در دو شخص حقوقی به عنوان مدیر فعالیت کند و به کارمند یکی از اشخاص حقوقی دستور ارتکاب جرمی را در راستای منافع شخص حقوقی دیگر بدهد، به نظر می رسد که نمی توان آن شخص حقوقی که کارمندش مرتکب جرم شده است را مقصر دانست، زیرا در این حالت، جرم در راستای منافع آن شخص حقوقی ارتکاب نیافته است و لذا جرم ارتکابی نسبت به آن شخص حقوقی فاقد مؤلفه دوم می باشد. در نتیجه آن شخص حقوقی در ارتکاب جرم مسئول خواهد بود که جرم در راستای تأمین سود و منافع وی انجام شده باشد و آن کارمند شخص حقوقی دیگر را نیز می توان در حکم اجیر دانست. در حالتی هم که یکی از کارمندان شخص حقوقی با اطلاع مدیر یا در اثر عدم نظارت وی، مرتکب جرم رایانه ای شود، باز هم این مدیر شخص حقوقی است که به طور غیرمستقیم موجب انجام جرم شده است. پس اگر از ارتکاب جرم آگاه بوده یا این که آن جرم در اثر عدم کنترل کارمندان توسط وی رخ دهد، جرمی که ارتکاب یافته متوجه شخص حقوقی می‌باشد. اما این که در این مورد، صرف اطلاع مدیر از ارتکاب جرم جهت مقصر دانستن شخص حقوقی کافی است یا این که علاوه بر آگاهی او از ارتکاب جرم، می‌بایست نسبت به ارتکاب آن نیز رضایت داشته باشد؟ آن چه از ظاهر ماده ۱۹ مذکور فهمیده می‌شود آن است که صرف اطلاع مدیر از ارتکاب جرم، به تنهایی جهت محکومیت شخص حقوقی کافی است، لیکن تفسیر مضیّق قانون به نفع متهم، صرف اطلاع مدیر را کافی ندانسته و از آن جا که مدیر شخص حقوقی، نماینده آن بوده و در صورت تقصیر وی، شخص حقوقی نیز مقصر می‌باشد، می‌توان گفت که اگر مدیر شخص حقوقی ار ارتکاب جرم توسط یکی از کارکنانش اطلاع داشته باشد اما توان مقابله با او و جلوگیری از ارتکاب جرم را نداشته باشد، وی مقصر نبوده و به تبع آن نمی‌توان شخص حقوقی را نیز مجرم دانست و صرف آگاهی و اطلاع مدیر از ارتکاب جرم جهت محکوم نمودن شخص حقوقی در جرایم سایبری و از جمله آن ها در سرقت‌های سایبری، لازم و کافی نمی‌باشد و نیازمند احراز رضایت وی و عدم توان او در مقابله با کارمند یا کارمندان خاطی می باشد.

قید عدم نظارت مدیر جهت محکوم نمودن شخص حقوقی نیز منوط به این است که این عدم نظارت به صورت غیرموجّه باشد. لذا اگر مدیر شخص حقوقی به دلیل موجّهی مانند بیماری، به فعالیت های کارکنان خود نظارت نکند و در نتیجه این عدم نظارت جرمی توسط کارکنان شخص حقوقی ارتکاب یابد، نمی توان مدیر شخص حقوقی را به دلیل عدم نظارت بر کارکنان خود مقصر دانست. در اینجا تفاوتی که میان قید اطلاع و قید عدم نظارت می توان بیان نمود آن است که اطلاع شامل هر یک از ارکان تصمیم گیری، نظارت و همچنین نمایندگی شخص حقوقی می شود، لیکن عدم نظارت فقط شامل افرادی می‌شود که این وظیفه را در شخص حقوقی بر عهده دارند. اما در خصوص این قید که اگر تمام یا بخشی از فعالیت شخص حقوقی به ارتکاب جرم سایبری اختصاص یافته باشد، شخص حقوقی مجرم می باشد، می‌توان گفت که با وجود حالت سوم که به آگاهی یا عدم نظارت مدیر شخص حقوقی پرداخته است، دیگر نیازی به حالت چهارم نبود، زیرا انجام جرایم سایبری اگر به عنوان فعالیت شخص حقوقی مطرح شود، از دو حالت خارج نخواهد بود: ۱. ارتکاب جرم با آگاهی مدیر می باشد؛ ۲. ارتکاب جرم با نظارت نکردن مدیر امکان پذیر می‌باشد.

در هر حال، به نظر می‌رسد بیان حالت چهارم به عنوان حالت برجسته مسئولیت کیفری شخص حقوقی بوده و از جهت برجسته کردن این حالت است که جداگانه به آن پرداخته شده است و منظور قانون گذار در این بند آن است که شخص حقوقی با رعایت کلیه ضوابط و شرایط قانونی تشکیل شده و بعد از کسب نمودن شخصیت، به ارتکاب جرم پرداخته باشد وگرنه اگر تشکیلاتی برای ارتکاب جرم تأسیس و تشکیل شود فاقد شخصیت حقوقی خواهد بود، زیرا مطابق قواعد حقوق مدنی، جهت قرارداد باید مشروع باشد. سپس در ماده ۲۰ قانون جرایم رایانه ای مجازات های در نظر گرفته شده برای اشخاص

حقوقی را بیان می دارد که کمی تأمل در این ماده نشان می دهد که مجازات های تعیین شده برای اشخاص حقوقی به مراتب سنگین تر از اشخاص حقیقی است و یا حداقل در خصوص سرقت های سایبری این گونه می‌باشد، زیرا در ابتدای این ماده آمده است که شخص حقوقی مرتکب جرایم رایانه ای را با توجه به شرایط و اوضاع و احوال جرم ارتکابی، میزان درآمد و نتایج حاصله از ارتکاب جرم، به سه تا شش برابر حداکثر جزای نقدی جرم ارتکابی محکوم می نماید که با توجه به مجازات های تعیین شده در ماده ۱۲ این قانون، دارای شدت بیشتری می باشد. از مجموع آن چه که گفته شد، مشاهده می شود که شخص حقیقی اگر مرتکب سرقت سایبری بشود، حداکثر به هر دو مجازات جزای نقدی و حبس محکوم می–شود و آن هم در صورتی است که عین داده ها در اختیار مالک اصلی نباشد. ولی شخص حقوقی در صورتی که مرتکب این جرم شود، هم به جزای نقدی و هم به تعطیلی یا انحلال محکوم خواهد شد، بدین صورت که در صورت باقی بودن عین داده ها در اختیار مالک اصلی، فقط شخص حقوقی به سه تا شش برابر حداکثر جزای نقدی که معادل شصت میلیون ریال تا یکصد و هشتاد میلیون ریال می شود، محکوم خواهد شد و در صورتی که سارق اقدام به انتقال داده ها کرده باشد، به گونه ای که اصل آن ها در اختیار مالک اصلی نباشد، هم به مجازات نقدی مذکور و هم به تعطیلی موقت از یک تا نه ماه محکوم خواهد شد و در صورت تکرار سرقت، شخص حقوقی به تعطیلی موقت از یک تا پنج سال محکوم خواهد شد.

٤-۲ مجازات تکمیلی و تبعی

بند «الف» ماده ۲۰ قانون جرایم رایانه ای را می توان مجازات تکمیلی و تبعی اشخاص حقوقی در سرقت های سایبری دانست، زیرا علاوه بر سه تا شش برابر حداکثر جزای نقدی جرم ارتکابی، تعطیلی موقت شخص حقوقی از یک تا نه ماه و در صورت تکرار جرم، تعطیلی موقت شخص حقوقی از یک تا تا پنج سال را برای اشخاص حقوقی مرتکب جرایم سایبری قرار می دهد، مشروط بر این که مجازات حبس آن جرم در مجازات اصلی، تا پنج سال باشد. با توجه به این که در ماده ۱۲ قانون جرایم رایانه ای، برای سرقت های سایبری حداکثر حبس یک سال در نظر گرفته شده است، اشخاص حقوقی مرتکب سرقت سایبری، در صورتی به عنوان مجازات تکمیلی و تبعی مشمول بند «الف» ماده ۲۰ این قانون خواهند شد که مطابق بخش دوم ماده ۱۲ قانون مذکور، عین داده ها در اختیار صاحب آن نباشد، زیرا اگر عین داده ها در اختیار صاحب آن ها باشد، سارق فقط به جزای نقدی از یک میلیون ریال تا بیست میلیون ریال محکوم خواهد شد. پس اگر شخص حقوقی مرتکب سرقت سایبری، این سرقت را با روش نسخه برداری به گونه ای انجام دهد که اصل داده ها در اختیار مالک اصلی باقی بماند، مشمول مجازات تکمیلی و تبعی بیان شده در بند «الف» ماده ۲۰ قانون جرایم رایانه ای نخواهد شد. همچنین مطابق ماده ۲۳ قانون مجازات اسلامی، دادگاه می تواند مدیر شخص حقوقی یا کارمند تحت نظارت وی را به مجازات های تکمیلی و تبعی دیگر مانند محرومیت از حقوق اجتماعی، ممنوعیت از اقامت در نقطه یا نقاط معیّن و یا اقامت اجباری در محل معیّن و ... محکوم کند، زیرا همان گونه که بیان شد سرقت های سایبری در صورتی که دارای تمام شرایط اجرای حدّ نباشند–زیرا بنابر نظر برگزیده ما که در بخش ٦ مقاله خواهد آمد حدّ سرقت در سرقت های سایبری امکان اجرا دارد– و یا بنابر نسظری که حدّ سرقت را در خصوص آن ها قابل اجرا نمی داند، جزء جرایم دارای مجازات تعزیری می باشند و لذا می توان حکم ماده ۱۹ قانون مجازات اسلامی را در خصوص مرتکبین آن اجرا نمود.

۵.تشدید مجازات در سرقت سایبری

در مورد تشدید مجازات در سرقت سایبری می توان به مواد ۲٦ و ۲۷ فصل هشتم قانون جرایم رایانه‌ای که تحت عنوان تشدید مجازات ها آمده است، تمسک جست. زیرا تشدید کیفرها به دو اعتبار صورت می گیرد: نخست، تشدید از جهت شدّت جرم ارتکابی که تابعی از اصل «تناسب میان جرم و کیفر» است و دوم، تشدید به اعتبار خطرناکی بزهکار که اصل «شخصی بودن کیفر» را به اصل «شخصی کردن کیفر» یا همان انطباق کیفر با شخصیت مرتکب متحوّل می سازد. در فصل هشتم قانون جرایم رایانه ای نیز تشدید کیفرها بر پایه چنین معیارهایی مورد توجه قرار گرفته است (الهی‌منش،۱۳۹۱) و ماده ۲٦ این قانون به تشدید خاص یعنی کیفیات مشدّده شخصی اختصاص یافته است. در خصوص بندهای «الف» و «ب» این ماده پرسشی که به ذهن می آید این است که آیا ارتکاب جرم کارمندان و کارکنان در حین انجام کار و وظایف و به واسطه کارمند دولت بودن، سبب تشدید مجازات می گردد و یا این که صرف کارمند دولت بودن این افراد را مشمول تشدید مجازات می نماید؟ با دقت در بندهای مذکور مشاهده می شود که آن ها به بیان اقسام کاربرانی می پردازند که مرتکب جرایم رایانه ای می شوند و عامل تشدید مجازات آن ها را می توان شخصیت حقوقی آن ها دانست، زیرا قیدهای «به مناسبت انجام وظیفه» و «به مناسبت شغل خود» در پایان بندهای «الف» و «ب» نشان دهنده آن است که دلیل تشدید مجازات این افراد، سوءاستفاده آن ها از موقعیت شغلی و جایگاه حقوقی خود می باشد. در نتیجه این قانون در خصوص کاربرانی می باشد که با سوءاستفاده از عنوان شغلی خود و امکاناتی که برای انجام وظیفه در اختیار آن ها قرار داده شده است، اقدام به سرقت سایبری می کنند. همچنین تفسیر مضیّق قوانین اقتضا می کند که اگر یکی از اشخاص نام برده شده در بندهای «الف» و «ب» این ماده، بدون سوءاستفاده از عنوان شغلی یا امکاناتی که در راستای انجام وظیفه در اختیار وی قرار دارد اقدام به سرقت سایبری نماید، مشمول تشدید مجازات نشود زیرا اصل در قوانین کیفری تفسیر مضیّق آن ها به نفع متهم می‌باشد. حتی می‌توان چنین گفت

که از آنجایی که هیچ یک از جرایم رایانه ای را نمی توان به واسطه انجام وظایف قانونی مرتکب شد، ذکر این قید در ماده ۲۶ مذکور نشان می دهد که مقصود قانون گذار در این ماده آن است که فرد با سوءاستفاده از امکانات، مجوزها و اختیاراتی که برای انجام وظایف محوله قانونی خود در اختیار دارد، اقدام به ارتکاب جرم رایانه ای و سایبری نماید. بنابراین با توجه به منطوق صریح ماده ۲۶ مذکور، دیگر نظر مخالفی نمی توان برای آن متصور شد.

بند «ج» ماده ۲۶ مذکور، تعلّق داشتن داده ها یا سامانه های رایانه ای و یا مخابراتی که مورد جرم رایانه ای واقع شده اند به دولت، نهادها و یا مراکز ارائه دهنده خدمات عمومی را عامل تشدید مجازات می داند. لذا اگر داده هایی که سرقت می شوند و سیستم های رایانه ای و مخابراتی و یا وب سایت هایی که مورد حمله سارقان سایبری قرار می گیرند، متعلّق به دولت، نهادها و یا مراکز ارائه دهنده خدمات عمومی باشند، سارق یا سارقان مشمول تشدید مجازات تصریح شده در این قانون، یعنی محکوم شدن به بیش از دو سوم حداکثر یک یا دو مجازات تعیین شده خواهند شد. بندهای «د» و «ه» این ماده نوع ارتکاب جرم را عامل مشدّده می دانند و بیان می دارند که اگر جرم رایانه ای به صورت سازمان یافته و یا در سطح گسترده ای ارتکاب یافته باشد، یعنی کسانی با تشکیل و رهبری شبکه چند نفری به این امر اقدام کرده باشند و یا اقدامات آن ها سطح گسترده–ای از جامعه را تحت شعاع خود قرار داده باشد، مرتکبان مشمول تشدید مجازات خواهند شد. البته در ایران هنوز قوانین و مقرّرات شکلی و ماهوی مدوّنی در رابطه با جرایم سازمان یافته به تصویب نرسیده است و به همین دلیل حقوق دانان، قضات و وکلاء، هر کدام تفسیرهای متفاوتی از «ارتکاب جرم به صورت سازمان یافته» بیان نموده اند.

هم‌چنین به نظر برخی صاحب‌نظران در بند «ه» بهتر بود که قانون‌گذار منظور خود را از ارتکاب جرم در سطح گسترده به دقت بیان می نمود، زیرا هر جرمی که در فضای مجازی به وقوع می پیوندد، به دلیل وسعت بی انتهای این فضا و تعداد کاربران بسیار زیاد آن، می تواند از مصادیق جرم گسترده باشد و تعیین دقیق دامنه و گستردگی چنین جرایمی تقریباً غیرممکن است.(الهی منش،۱۳۹۱،) لذا باید برای احراز شرایط مذکور در بندهای «د» و «ه» ماده ۲۶ مذکور به نوع ارتکاب سرقت سایبری و همچنین گستره‌ای را که در بر می گیرد توجه نمود. در نتیجه اگر سارقان، سرقت سایبری را به صورت سازمان یافته انجام داده باشند و یا گستره خسارت دیدگان از این سرقت وسیع بوده و افراد بسیاری یا کشورهای متعدّدی را درگیر خود کرده باشد، مشمول تشدید مجازات مطرح شده در ماده ۲۶ قانون جرایم رایانه ای می شوند.

٦.بررسی نظرات فقهای معاصر در خصوص امکان اجرای حدّ در سرقت‌های سایبری

با بررسی نظرات بیان شده توسط فقها، مشاهده می شود که تمامی آن ها در قالب دو نظریه عمده و متضاد قرار دارند: اول نظریه ای که مبنی بر تعزیری بودن سرقت‌های سایبری است و دوم نظریه ای که مبنی بر حدّی بودن این سرقت‌ها است که در اثبات نظریه دوم می‌توان به دو دلیل تمسک جست:

الف) سرقت سایبری به این‌صورت است که یک کاربر بدون اجازه مالک اصلی داده‌ها و با استفاده از امکانات فضای مجازی اینترنت و شکستن قفل سایت یا سیستم رایانه‌ای، وارد سیستم یا سایت دیگران شده و داده‌های ارزشمندی را ربوده و به سیستم خود منتقل می‌نماید. با توجه به اطلاق آیه ۳۸ سوره مائده و تفسیرهایی که از آن شده است و مفسرین قرآن در این آیه دو واژه «السارق و السارقه» را در همان معنای لغوی و عرفی خویش که دزدیدن اموال دیگران باشد، ترجمه و تفسیر نموده‌اند و نظرات علمای ادبیات عرب نیز مؤید نظر مفسرین می‌باشد، می‌توان آیه مذکور را در خصوص هر دو نوع سرقت‌های سنتی و اینترنتی صادق دانست. همچنین در روایتی که توسط محمد بن مسلم نقل شده است، امام صادق(علیه–السلام) فرموده اند: «سارق کسی است که از مسلمانی چیزی که مواظبت کرده و حفظ شده است را بدزدد.»(حرّعاملی،١٤١٦) علاوه بر آن که این تعریف بر سرقت سایبری نیز منطبق می-باشد، مشاهده می‌شود که در تعریف سرقت حدّی قیدی نیامده که بتوان با تمسک به آن سرقت سایبری را از تحت شمول تعریف خارج نمود. همچنین آن چیزی که در سرقت مورد نهی می باشد، نفس و اصل ربایش مال غیر است که این عمل ممکن است به شیوه‌های گوناگون و متعدّدی صورت گیرد، ولی در اصل عمل سرقت تغییری ایجاد نمی شود، یعنی ماهیت جدیدی حادث نمی شود، بلکه تنها شیوه تحقّق جرم تغییر می کند.(موسوی۱۳۸۹) نکته دیگر در تعریف سرقت، مال بودن عین مسروقه است که در عرف امروز، داده‌ها و اطلاعات اینترنتی در مصادیق متعدّد آن، مال محسوب شده و دارای ارزش اقتصادی هستند، زیرا اولاً قابل خرید و فروش و مبادله می باشند؛ ثانیاً عرف عقلا به آن رغبت نشان داده و مطلوب آنان است و ثالثاً رافع نیازها و حوایج مردم امروزی در زندگی مادی و معنویشان می باشد. بنابراین آن چه که در سرقت اینترنتی به سرقت می رود، همانند سرقت فیزیکی، می تواند مشمول سرقت حدّی باشد. امام خمینی(قدس سره) در کتاب تحریرالوسیله چنین می فرمایند: «اگر چیزی بود که ما دلیلی بر این که به ملکیت در نمی آید نداشتیم، به ملکیت در می آید و اگر منفعت عقلایی هم داشته باشد و کسی آن را تلف کند، فرد تلف کننده مانند سایر اموال ضامن است.»(خمینی،١٣٨٦) بنابراین اصل در فقه شیعه به ملکیت درآمدن اشیاء است مگر در مواردی که دلیلی بر عدم ملکیت اقامه شده باشد و به همین دلیل درخصوص داده‌ها و اطلاعات رایانه‌ای می توان چنین گفت که اگر دلیلی بر عدم ملکیت آن‌ها اقامه نشود، به ملکیت در می‌آیند.

ب) شرایط سرقت حدّی در اغلب موارد به گونه‌ای است که با نوع سایبری آن تعارضی نداشته و همه آن شرایط به نوعی در سرقت سایبری نیز موجود می‌باشند. بعضی از این شرایط مانند بلوغ و عقل به سارق بر می گردند و اصلاً ارتباطی با سایبری بودن یا نبودن سرقت ندارند. برخی دیگر به مال

مسروق بر می گردند که بخش اعظم آن اعم بوده و اختصاصی به غیر اینترنت ندارند. مثل این که گفته شده شیء سرقت شده متعلّق به دیگری باشد، محترم باشد، مال مشترک نباشد. برخی دیگر از این شرایط به مسروقٌ فیه بر می‌گردند که به نظر می‌رسد در ماهیت سرقت اینترنتی هیچ خللی به وجود نمی‌آورند و فقط در کیفیت مجازات، از این جهت که در دارالعدل است یا در دارالحرب، ممکن است مؤثر باشند. موضوع هتک حرز نیز که به عنوان یکی از شروط مهم و اساسی در سرقت حدّی مطرح است، در سرقت سایبری با شکستن قفل نرم افزاری یا رمز عبور وب سایت یا سیستم رایانه ای تحقّق پیدا می‌کند(موسوی،۱۳۸۹) و مبنای این نظر نیز قضاوت عرف متخصّصان و کاربران فضای سایبری می‌باشد.

۷.نتیجه‌گیری

با بررسی قانون جرایم رایانه‌ای مشاهده می‌گردد که مجازات‌های مقرّر در ماده ۱۲ این قانون با توجه به تنوع و گستردگی سرقت های سایبری و وسعت خسارت‌های ناشی از آن‌ها، از بازدارندگی کافی برخوردار نبوده و بسیاری از مسائل چالشی موجود در این حوزه را پوشش نمی‌دهد که یکی از آن‌ها مسئله اجرای حدّ سرقت در سرقت‌های سایبری است، مشروط به آن که جرم ارتکابی دارای تمام شرایط اجرای حدّ باشد. همچنین در بررسی‌های انجام شده، مشاهده می‌شود که در سرقت‌های سایبری امکان تحقّق جرم توسط هر دوی اشخاص حقیقی و حقوقی وجود داشته و مجازات‌های اشخاص حقوقی به مراتب شدیدتر می باشد و از آن جا که انجام هر تحقیق برای آن است که از نتایج حاصل از آن در بهبود وضعیت موجود و تصمیم‌گیری بهتر در مورد آینده استفاده شود. لذا مواردی به عنوان پیشنهادات و راه کارها بیان می‌گردد:

۱.لزوم وضع قوانین جدید و اصلاح قوانین موجود: در ایران که قوانین سنتی قدرت جواب‌گویی و رسیدگی به جرایم سایبری، بالاخص سرقت های سایبری را ندارند و قانون جرایم رایانه‌ای نیز دچار ابهام و اجمال می‌باشد، لزوم وضع قوانین کارآمد و متناسب و همچنین بازنگری در قوانین موجود، از ضرورت بیشتری برخوردار می‌باشد.

۲.استفاده از ظرفیت های فقهی: به نظر می‌رسد با توجه به پیچیدگی های جرایم سایبری به طور اعم و سرقت‌های سایبری به طور اخص، و مسئله امکان یا عدم امکان اجرای حدّ در این گونه سرقت‌ها و مسائل مشابه دیگر، ضروری است که فقها و مجتهدین در این گونه مسائل ورود کرده و با توجه به منابع اصیل فقه پویای شیعه، نظرات خود را بیان دارند تا قانون گذاران بتوانند قوانین جدید را در تطابق هر چه بیشتر با احکام شریعت اسلام وضع نمایند و بر همین اساس نیز به بازنگری قوانین موجود بپردازند.

۳.لزوم همکاری‌های بین المللی: همکاری های بین المللی در مسئله بررسی و تحلیل مجازات های متناسب و بازدارنده برای سرقت های سایبری را می‌توان در زمینه‌های ذیل مدّ نظر قرار داد:

الف. انجام تحقیقات جرم شناختی در این زمینه؛

ب. بررسی راه های مؤثر در پیشگیری از جرم سرقت سایبری؛

ج. بررسی شیوه های نوین کشف جرایم و تعقیب مجرمان سایبری؛

د. برگزاری نشست ها و کنگره های علمی در این زمینه با حضور اساتید صاحب نظردر این زمینه؛

ه. تشکیل کارگروه بین المللی و تبادل اطلاعات و یافته های علمی نوین در این زمینه میان کشورهای عضو.

منابع

۱.الهی منش، محمدرضا، سدره نشین، ابوالفضل، ۱۳۹۱، محشای قانون جرایم رایانه ای، تهران: مجد.

۲.بای، حسین علی، پورقهرمانی، بابک، ۱۳۸۸، بررسی فقهی حقوقی جرایم رایانه ای، قم: دفتر تبلیغات اسلامی حوزه علمیه قم، معاونت پژوهش، پژوهشگاه علوم و فرهنگ اسلامی.

۳.بجنوردی، سید محمد، بنی هاشمی، مریم، ۱۳۹۲، بررسی فقهی سرقت رایانه ای (اینترنتی) با رویکردی بر نظر امام خمینی، پژوهشنامه متین، سال پانزدهم، فصل پاییز، شماره ٦٠،ص۲۹-٤٠.

٤.بوشهری، جعفر، ۱۳۸۷، حقوق جزا: اصول و مسائل، تهران: شرکت سهامی انتشار.

۵.جاوید نیا، جواد، ۱۳۸۷، جرایم تجارت الکترونیکی: جرایم رایانه ای در بستر تجارت الکترونیکی، تهران: خرسندی.

٦.حرّعاملی، محمدبن الحسن، ١٤١٦ق.، تفصیل وسائل الشیعه إلی تحصیل مسائل الشریعه، چاپ دوم، ۳۰ جلد، قم: آل البیت(علیهم السلام) لإحیاء التراث.

۷.خمینی، روح الله، ۱۳۸٦، تحریرالوسیله، قم: دارالعلم.

۸.رضوی، سید محمدجعفر، ۱۳۹۵، پایان نامه کارشناسی ارشد، قم: دانشگاه آزاد اسلامی.

۹.عالی پور، حسن،۱۳۹۰، حقوق کیفری فناوری اطلاعات (جرایم رایانه ای)، تهران: خرسندی.

۱۰.محبوبی، فرخ، ۱۳۸۱، دانش آموز نفوذگر، چاپ اول، تهران: ناقوس.

۱۱.موسوی، روح الله، و قربانی، حبیب، ۱۳۸۹، سرقت های اینترنتی: عدالت در حد است یا تعزیر؟، مجموعه مقالات اولین همایش ملی فقه و مسائل مستحدثه (نوظهور)، ساری: مرکز انتشارات توسعه علوم.

12 . Casey, Edward. 2001. Digital evidence and computer crime. Academic press, New York: 53:1-21.

Penalties for cyber theft in Iranian law

Seyed-Mohsen Razavi-Asl[1]

Abstract

By development of internet and its effect on different parts of human life, different crimes happen in this context and one of them is robbery. Internet robbery is stealing of other's data by computer on the web and it has three special bases of robbery which are robber, victim and stolen. The general elements are material, logical and spiritual. So this kind of robbery has no basical different with traditional robbery and the only difference is the environment and way of doing crime. So we can say that internet robbery has the same laws like traditional robbery. In Iran, There is a common and special relation between computerize robbery and internet robbery. As any internet robbery is a computerize crime but not any computerize robbery an internet kind. Evidence show that even though internet robbery is a crime but its complexity and variety made it difficult to legislate proper rules because of that only article 12 is dedicated to internet robbery and it's very limited and silent in some cases like robbery hadd. More over in internet robbery retributory responsibility for juridical characters is possible and it's accepted in Iran computerized-crimes law.

Keywords:Cyber robbery; Computer theft; computer crime law; Iranian law; penalties

[1] Doctor of Jurisprudence and Principles of Islamic Law, Qom, Iran