

## چالش‌های مقررات تعدد جرم در جرایم سایبری

حمید بهره‌مند\*

### چکیده

یکی از ویژگی‌های جرایم سایبری آن است که مرتکب به دلیل امکان گمنام ماندن و با یافتن روش‌های ارتکاب جرم می‌تواند در آن واحد جرایم متعددی را علیه بزه‌دیدگان متعدد مرتکب شود. از سویی، ارتکاب برخی از جرایم با به کار بستن شیوه‌هایی چون فیشینگ به نحوی است که دامنه گسترده‌ای از بزه‌دیدگان را در بر می‌گیرد. از سوی دیگر مرتکبان این جرایم با توجه به ویژگی‌های شخصیتی که دارند، همان‌گونه که به فنون ارتکاب جرم آشنایی دارند، از قوانین و مقررات کیفری و اینکه ارتکاب جرم، بیش از تعدادی خاص تأثیری در میزان مجازات آنها ندارد، آگاهی دارند. این امر باعث می‌شود این مقررات که قاعداً برای اشخاصی کاربرد دارد که تعدد جرایم در مورد آنها استثنا است، در مورد مجرمان سایبری که ارتکاب جرم واحد در مورد آنها غالباً استثناست، اثربخش نباشد و پاسخ‌های کیفری مانع بازدارنده‌ای از ارتکاب جرایم دیگر توسط مجرمان نشود. عدم وضع مجازات‌هایی چون محرومیت از خدمات عمومی الکترونیکی، چه به عنوان مجازات اصلی و چه به عنوان مجازات تکمیلی، نیز موجب می‌شود که این مجرمان پس از تحمل مجازات اصلی خلع سلاح نشوند و امکان ارتکاب مجدد جرایم را داشته باشند. ابهام در مقررات تعدد و شفاف نبودن مرز میان تعدد مادی و معنوی و نتایج مجرمانه متعدد نیز باعث شده است که در رویه قضایی اختلافاتی در تعیین مجازات‌های متناسب به وجود آید. این مقاله به دنبال ارائه راهکارهایی مناسب برای حل مشکلات موجود بوده است.

**کلیدواژه‌ها:** تعدد جرم، جرم سایبری، فضای سایبر، اقتصاد جرم و مجازات.

فضای سایبر علاوه بر امکاناتی که برای رشد و توسعه در اختیار بشر قرار داده، فرصتهایی نیز برای مجرمان ایجاد کرده است. از این روست که امروزه سخن از وجه سیاه اینترنت به میان می‌آید.<sup>۱</sup> از جمله ویژگی‌های این فضا آن است که مجرمان می‌توانند راحت‌تر مرتکب جرم شده، جرایم بیشتری مرتکب شوند و آماج مجرمانه متکثرتری را هدف بگیرند. این ویژگی‌های فضای سایبر باعث شده است تا مقرراتی که در خصوص پاسخ‌دهی کیفری برای مجرمان مرتکب جرایم متعدد وضع شده است، با چالش روبرو شود. به عبارت دیگر، برخلاف جرایم سنتی که ارتکاب جرایم متعدد علی‌الاصول متضمن صرف زمان بیشتری از جرم واحد بود، در جرایم سایبری مرتکب هم می‌تواند در زمانی کوتاه مرتکب رفتارهای مجرمانه متعددی شود که هر کدام جرمی مستقل از دیگری را تشکیل می‌دهد و هم می‌تواند با رفتار واحد عده زیادی را بزه‌دیده قرار دهد و نتایج مجرمانه گسترده‌ای ایجاد کند. از این رو، در این مقاله تلاش می‌شود به این سؤال پاسخ داده شود که آیا مقررات تعدد جرم که به عنوان یک قاعده هم در جرایم سنتی و هم در جرایم سایبری جاری است، در مورد بزهکاران سایبری اثربخشی کافی را دارد یا باید برای این دسته از جرایم و مجرمان آنها سیاست کیفری خاصی در نظر گرفت. از این رو، پس از بررسی ویژگی‌های جرایم سایبری و مرتکبان آنها و لزوم اتخاذ سیاست کیفری افتراقی در مورد این جرایم، پاسخ‌های کیفری در دو بخش مجازات‌های اصلی و تکمیلی مورد بحث قرار خواهند گرفت و اثربخشی یا عدم اثربخشی این مجازات‌ها در سه حوزه تعدد معنوی، تعدد مادی و نتایج مجرمانه متعدد در خصوص جرایم سایبری مورد مطالعه قرار خواهد گرفت.

### ۱. مبانی تعیین مجازات در جرایم سایبری متعدد

برای اتخاذ سیاست کیفری کارآمد در خصوص جرایم سایبری متعدد لازم است ابتدا ویژگی‌های این جرایم شناسایی شود و با شناخت دقیق مجرمان این جرایم، پاسخ‌های کیفری مؤثری پیش‌بینی شود. در غیر این صورت ممکن است قواعد عامی که در تعیین کیفرها مقرر شده است، برای این دسته از مجرمان اثربخشی کافی را نداشته باشد. به عبارت دیگر، شناسایی ویژگی‌های جرایم سایبری و مرتکبان آنها می‌تواند قانون‌گذار را در اتخاذ سیاست کیفری افتراقی کمک کند. در واقع باید توجه داشت سیاست کیفری اتخاذ شده در مرحله تقنین باید به نحوی باشد که موجبات دست

یافتن به اهداف را در مرحله تعیین مجازات در محاکم فراهم کند. به دیگر سخن زمانی می‌توان انتظار داشت در مرحله تعیین مجازات از سوی محاکم (مجازات‌دهی) پاسخ‌های مناسبی بر مجرمان تحمیل شود که در مرحله وضع مجازات از سوی قانون‌گذار (مجازات‌گذاری) مقررات مناسبی وضع شده باشد. تنها در این صورت است که می‌توان حصول اهداف مجازات‌ها را انتظار داشت؛ خواه این اهداف حصول بازدارندگی کافی باشد، خواه توان‌گیری از مجرم و خواه بازپروری او.<sup>۱</sup>

### ۱-۱. ویژگی‌های فضای سایبر و جرایم سایبری

برخلاف فضای فیزیکی که دارای محدودیت‌های زیادی چون محصور بودن شخص در زمان و مکان است، به نحوی که یک شخص در زمان واحد نمی‌تواند در چند مکان حضور داشته باشد، فضای سایبر به گونه‌ای است که اشخاص می‌توانند در یک زمان در قلمروهای سایبری مختلفی حضور داشته باشند و فعالیت کنند. علاوه بر این، گمنام ماندن در فضای سایبر و اتخاذ نام‌های مستعار و یا جعلی نسبت به فضای فیزیکی بسیار ساده‌تر است. از این رو ممکن است شخصی که در فضای واقعی نمی‌تواند ویژگی‌هایی چون سن و جنس خود را به راحتی مخفی کند، در فضای سایبر نه تنها می‌تواند این ویژگی‌ها را تغییر دهد، بلکه می‌تواند هویت‌های بی‌شماری برای خود ایجاد کند و با هر یک از این هویت‌ها مرتکب جرم شود. از این روست که گفته می‌شود سرعت، کثرت، سهولت ارتکاب جرم، ارزان بودن، مقید نبودن به مرزهای جغرافیایی، ناشناختگی باعث بروز جرایمی شده است که از سایر جرایم متمایز است.<sup>۲</sup> علاوه بر اینکه این ویژگی‌ها باعث می‌شود اشخاص به راحتی مرتکب جرایم سایبری متعدد شوند یا با ارتکاب جرم واحد، نتایج مجرمانه متعددی را رقم بزنند، مرتکبان این‌گونه جرایم کمتر تحت تعقیب، محاکمه و مجازات قرار گیرند، به نحوی که مطابق یک مطالعه از هر ۲۲۰۰۰ مجرم سایبری تنها یک نفر به مجازات حبس محکوم شده است.<sup>۳</sup>

### ۱-۲. ویژگی‌های مجرمان سایبری

علاوه بر ویژگی‌های فوق که جرم سایبری را از جرایم سنتی متمایز می‌سازد، مرتکبان جرایم سایبری هم عموماً نسبت به مرتکبان جرایم سنتی متفاوت هستند.

۱. برای اطلاع بیشتر از اهمیت مرحله تعیین مجازات و اهداف کیفرها، ر.ک.: مهرا، نسرين، «کیفر و چگونگی تعیین آن در فرایند کیفری انگلستان (با تأکید بر کارکرد کیفرها)»، مجله تحقیقات حقوقی، شماره ۴۵، بهار و تابستان ۱۳۸۶، صص: ۶۵-۷۸.
۲. جوان‌جعفری، عبدالرضا، «جرایم سایبر و رویکرد افتراقی حقوق کیفری (با نگاهی به قانون مجازات اسلامی بخش جرایم رایانه‌ای)»، مجله دانش و توسعه، شماره ۳۴، اسفند ۱۳۸۹، ص. ۱۷۱.
۳. زبیر، اولریش، جرایم رایانه‌ای، ترجمه محمدعلی نوری و دیگران، چاپ دوم، انتشارات گنج دانش، ۱۳۹۰، ص. ۶۱.

توضیح آنکه با توجه به فضای ارتکاب جرم، مجرمانی می‌توانند از این فضا برای ارتکاب جرم بهره جویند که آگاهی‌هایی نسبت به این فضا و فرصت‌هایی که برای ارتکاب جرم در اختیار قرار می‌دهد داشته باشند. به عبارت دیگر، بر خلاف بزه‌دیدگان سایبری که ممکن است به دلیل ناآشنا بودن از ویژگی‌های فضای سایبر و موقعیت‌هایی که برای ارتکاب جرم علیه آنها وجود دارد، مورد حمله بزهکاران قرار گیرند، بزهکاران سایبری خصوصاً در جایی که جرم ارتكابی جرم سایبری محض است، عموماً دارای دانشی بالاتر از سطح عمومی هستند.<sup>۱</sup> حتی ارتکاب برخی از جرایم رایانه‌ای مستلزم دانش و استفاده از نرم‌افزارهایی است که برای عموم کاربران فضای سایبر ناآشناست و کشف این جرایم جز با بهره گرفتن از کارشناسان مجرب و متخصص ممکن نیست.<sup>۲</sup> از این رو، مرتکبان جرایم سایبری عموماً به جای اتکا به قدرت فیزیکی، از قوه تفکر و تحلیل خود برای ارتکاب جرم استفاده می‌کنند. لذا در دسته‌بندی‌های مرسوم معمولاً جرایم رایانه‌ای به عنوان دسته‌ای از جرایم یقه‌سفیدها قلمداد می‌شوند.<sup>۳</sup> در جرم‌شناسی نیز تلاش می‌شود که بر مبنای نظریه انتخاب عقلانی،<sup>۴</sup> چرایی ارتکاب جرایم، شخصیت مرتکبان و نحوه پیشگیری از آنها مورد بررسی قرار گیرد.<sup>۵</sup> از این رو، اگر در مورد جرایم خیابانی بتوان مواردی را یافت که مرتکب در ارتکاب جرم، توجه چندانی به هزینه‌ها و منافع جرم نداشته است، در مورد مجرمان یقه‌سفید عموماً با مرتکبان حسابگر روبرو هستیم. لذا در تعیین پاسخ‌های کیفی ناظر به این دسته از مجرمان باید هزینه‌های ناشی از جرم به گونه‌ای تعیین شود که بتواند در تحلیل هزینه-منفعت<sup>۶</sup> جرم انگیزه‌ای برای ارتکاب جرم پیدا نکند. به عبارت دیگر، این دسته از مجرمان، برخلاف مجرمان هیجانی که تحلیل منطقی از جرم ندارند و مجرمان خیابانی که ممکن است به زندان رفتن برای آنها یک افتخار تلقی شود، مجرمان منطقی محسوب می‌شوند که هزینه‌ها و منافع ارتکاب جرم را می‌سنجند و فقط در صورتی مرتکب جرم می‌شود که منافع بیشتر از هزینه‌ها باشند.<sup>۷</sup>

۱. محمدکوره‌پز، حسین؛ و دیگران، «نیم‌رخ جرم‌شناختی بزهکاران سایبری»، پژوهش حقوق کیفری، سال سوم، شماره نهم، زمستان ۱۳۹۳، ص. ۱۲۵.

2. Wiles, Jack; Reyes, Anthony, *The Best Damn Cybercrime and Digital Forensics Book Period*, Rockland, Mass, Syngress, 2007, p. 18.

3. Scheb, John M; Scheb, John M, *Criminal Law and Procedure*, Belmont, CA, Wadsworth Cengage Learning, 2011, p. 210.

4. Rational choice perspective theory.

5. Akhgar, Babak; Yates, Simeon, *Intelligence Management*, London, Springer, 2011, p. 188.

6. Cost-benefit analysis.

۷. البته برخی از مجرمان سایبری هم وجود دارند که ارتکاب جرم از سوی آنها نوعی لذت و تفریح محسوب می‌شود و بنابراین ممکن است درک کاملی از آسیب‌ها و خسارت‌هایی که وارد می‌کنند، نداشته باشند؛ وینتر، هارولد، اقتصاد جرم، ترجمه حمید بهره‌مند و زهرا ساکبانی، تهران، انتشارات دادگستر، ۱۳۹۴، ص. ۲۹.

لازم به ذکر است که امروزه بحث تحلیل اقتصادی جرم و توجه به انگیزه‌های مرتکب موضوع دانشی به نام اقتصاد جرم است. در این دانش علاوه بر توجه به تحلیل‌های اقتصادی در جرم‌انگاری رفتارها، تأکید ویژه‌ای بر پاسخ‌های کیفی می‌شود و با مدل‌های اقتصادی مقدار بهینه مجازات‌ها تعیین می‌شود.<sup>۱</sup> از این رو، چنانچه در جرایمی چون سرقت و کلاهبرداری رایانه‌ای منافع ناشی از جرم و در برخی از جرایم چون تخریب رایانه‌ای خسارت‌های ناشی از جرم می‌تواند عوامل مهمی در تعیین مجازات‌ها باشد، باید توجه داشت در جرایم متعدد نیز که مرتکب منافع متعددی تحصیل می‌کند یا خسارت‌های متعددی ایجاد می‌کند، پاسخ‌های متناسبی باید در نظر گرفته شود.

لذا با توجه به اینکه جرایم سایبری با جرایم سنتی و مجرمان سایبری با سایر مجرمان تفاوت‌های معناداری دارند، لازم است سیاست کیفری اتخاذی در خصوص این جرایم و مجرمان وجوه افتراق را در نظر بگیرد. این وجوه افتراق را می‌توان در مجازات‌های اصلی و در مجازات‌های تکمیلی در نظر گرفت که ذیلاً مورد بررسی قرار می‌گیرند.

## ۲. پاسخ‌های تقنینی به جرایم سایبری متعدد

مجازات‌هایی که در نظام حقوقی ایران برای مجرمان در نظر گرفته می‌شود یا مجازات‌های اصلی است که قانون‌گذار با در نظر گرفتن جرم ارتكابی و فارغ از اینکه چه شخصی مرتکب آن شده است، تعیین می‌کند. البته توجه به عواملی چون شخصیت مرتکب جرم و نتایج زیان‌بار ناشی از جرم در تعیین حداقل تا حداکثر مجازات اصلی مؤثر است.<sup>۲</sup> افزون بر این مجازات، قاضی می‌تواند در جرایم تعزیری درجه ۱ تا ۶ بسته به جرم ارتكابی و شخصیت مرتکب، او را به مجازات‌های تکمیلی نیز محکوم کند.<sup>۳</sup> همچنین در جرایمی که شدت کمتری دارد، دادگاه می‌تواند ضمن تعیین مجازات جایگزین حبس،<sup>۴</sup> مرتکب را به یکی از محرومیت‌های مقرر در مجازات‌های تکمیلی یا تبعی محکوم کند.

۱. صادقی، حسین؛ و دیگران، اقتصاد جرم، تهران، نور علم، ۱۳۸۹، ص. ۱۲۴.

۲. مطابق ماده ۱۸ قانون مجازات اسلامی مصوب ۱۳۹۲: «... دادگاه در صدور حکم تعزیری، با رعایت مقررات قانونی، موارد زیر را مورد توجه قرار می‌دهد: الف: انگیزه مرتکب و وضعیت ذهنی و روانی وی حین ارتکاب جرم؛ ب: شیوه ارتکاب جرم، گستره نقض وظیفه و نتایج زیان‌بار آن؛ پ: اقدامات مرتکب پس از ارتکاب جرم؛ ت: سوابق و وضعیت فردی، خانوادگی و اجتماعی مرتکب و تأثیر تعزیر بر وی»

۳. مطابق ماده ۲۳ قانون مجازات اسلامی مصوب ۱۳۹۲: «دادگاه می‌تواند فردی را که به حد، قصاص یا مجازات تعزیری از درجه شش تا درجه یک محکوم کرده است با رعایت شرایط مقرر در این قانون، متناسب با جرم ارتكابی و خصوصیات وی به یک یا چند مجازات از مجازات‌های تکمیلی زیر محکوم نماید.»

۴. مطابق ماده ۸۷ قانون مجازات اسلامی مصوب ۱۳۹۲: «دادگاه می‌تواند ضمن حکم به مجازات جایگزین حبس، با توجه به جرم ارتكابی و وضعیت محکوم، وی را به یک یا چند مورد از مجازات‌های تبعی و یا تکمیلی نیز محکوم نماید. در این صورت مدت مجازات مذکور نباید بیش از دو سال شود.»

از آنجا که این دو نوع مجازات ستون اصلی پاسخ‌های کیفری جرایم محسوب می‌شود، لازم است بررسی شود با توجه به ویژگی‌هایی که برای جرایم و مجرمان سایبری بیان شد، مقررات موجود و قواعد تعیین این دو دسته مجازات برای برخورد با مرتکبان جرایم سایبری متعدد مناسب‌اند یا باید قواعدی افتراقی برای این دسته از جرایم و مجرمان اتخاذ شود.

## ۲-۱. مجازات‌های اصلی جرایم سایبری متعدد

همان‌طور که بیان شد، تعدد جرایم یا مادی است و یا معنوی. البته قانون‌گذار در قانون مجازات اسلامی، در مورد جرایمی که موجب نتایج متعدد می‌شود، حکم خاصی در نظر گرفته است که در این بخش قواعد و مقررات ناظر بر تعیین مجازات‌های اصلی هریک از این حالات به طور مجزا مورد بررسی قرار خواهد گرفت.

### ۲-۱-۱. تعدد معنوی جرایم سایبری

در تعدد معنوی میان جرایم سایبری یا میان جرایم سایبری و سنتی، چنانچه این جرایم تعزیری باشند، مطابق مقررات ماده ۱۳۱ قانون مجازات اسلامی، مرتکب به مجازات اشد محکوم می‌شود. مانند آنکه شخصی با استفاده از داده مجعول دیگری را فریب دهد و با او ازدواج کند. در این صورت از میان مجازات دو جرم موضوع مواد ۶۴۷ (حبس از شش ماه تا دو سال) و ۷۳۵ کتاب پنجم قانون مجازات اسلامی (حبس از یک تا پنج سال یا جزای نقدی از ۲۰ میلیون تا ۱۰۰ میلیون ریال یا هر دو مجازات) مرتکب به مجازات جرم دوم محکوم خواهد شد. همچنین اگر شخصی فیلم خصوصی دیگری را که بنا به دلایلی طبقه‌بندی و سری محسوب شده است، در دسترس اشخاص دیگر قرار دهد و از این طریق موجب هتک حیثیت او شود، از میان مجازات دو جرم جاسوسی رایانه‌ای موضوع ماده ۷۳۱ (حبس از ۲ تا ۱۰ سال) و هتک حیثیت رایانه‌ای موضوع ماده ۷۴۵ (حبس از ۹۱ روز تا دو سال یا جزای نقدی از ۵ میلیون تا ۴۰ میلیون یا هر دو مجازات) به مجازات جرم نخست محکوم خواهد شد. در این موارد چون به واقع شخص مرتکب جرایم متعددی نشده است بلکه رفتار او مشمول عناوین مختلفی قرار گرفته است، همین که مجازات جرمی بر مرتکب تحمیل شود که شدیدتر است کفایت می‌کند.

### ۲-۱-۲. تعدد مادی یا واقعی جرایم سایبری

در جایی که شخصی مرتکب رفتارهای مختلفی شده است که هر کدام جرم تعزیری محسوب می‌شود، موضوع مشمول ماده ۱۳۴ قرار خواهد گرفت. برخلاف قانون مجازات اسلامی مصوب ۱۳۷۰ که در خصوص تعدد مادی میان جرایم مشابه و

غیرمشابه تمایزی برقرار کرده بود و در مورد نخست، تعدد را موجب تشدید<sup>۱</sup> و در مورد دوم تعدد را موجب جمع مجازات‌ها می‌دانست، در قانون مجازات اسلامی ۱۳۹۲ با بازگشت به مقررات قانون ۱۳۵۲، این تمایز حذف و تعداد جرایم ملاک نحوه تعیین مجازات‌ها<sup>۲</sup> در نظر گرفته شده است.<sup>۳</sup> بدین نحو که در جرایم تعزیری درجه ۷ و ۸ و در اجتماع این جرایم با جرایم تعزیری درجه ۱ تا ۶ جمع مجازات‌ها صورت می‌گیرد و در تعدد جرایم تعزیری ۱ تا ۶ چنانچه تعداد جرایم ۲ یا ۳ مورد باشد، چنانچه مجازات دارای حداقل و حداکثر باشد، تشدید به نحو اجرای حداکثر مجازات یا مجازات‌های شدیدترین جرم ارتكابی و چنانچه مجازات فاقد حداقل و حداکثر باشد، تشدید به نحو اجرای مجازات ثابت به علاوه مجازاتی تا یک چهارم آن مجازات صورت می‌پذیرد و چنانچه تعداد جرایم ۴ مورد یا بیشتر باشد، در مجازات‌هایی که دارای حداقل و حداکثر است تشدید مجازات به نحو اجرای حداکثر مجازات یا مجازات‌های شدیدترین جرم به علاوه مجازاتی تا نصف حداکثر مجازات قانونی و چنانچه مجازات فاقد حداقل و حداکثر باشد، تشدید به نحو اجرای مجازات ثابت به علاوه مجازاتی تا یک دوم آن مجازات صورت می‌پذیرد.

در قانون جرایم رایانه‌ای موارد معدودی وجود دارد که مجازات جرمی از درجه ۷ یا ۸ باشد. برای مثال اگر شخصی مرتکب سرقت رایانه‌ای شود بدون آنکه موجب حذف داده شود، به جزای نقدی از یک میلیون تا ۲۰ میلیون ریال محکوم خواهد شد. چنین شخصی اگر چند بار مرتکب این جرم شده باشد، برای هر مرتبه به این مجازات محکوم و جمع مجازات‌ها در خصوص او اعمال خواهد شد.<sup>۴</sup> همچنین اگر چنین شخصی برای ارتکاب جرم سرقت، مرتکب دسترسی غیرمجاز شده باشد، علاوه بر مجازات مذکور به مجازات مقرر برای جرم اخیر نیز (جزای نقدی از ۵ میلیون تا ۲۰ میلیون ریال یا حبس

۱. لازم به ذکر است با توجه به اینکه در ماده ۴۷ قانون مجازات اسلامی مصوب ۱۳۷۰ میزان تشدید معین نشده بود، رأی وحدت رویه شماره ۶۰۸ مورخ ۱۳۷۵/۶/۲۷ امکان تعیین مجازات بیش از حداکثر مجازات قانونی را ممنوع دانست و عملاً مفهوم تشدید را به نفع اصل قانونی بودن جرایم و مجازات‌ها به تعیین حداکثر مجازات تغییر داد. برای مطالعه بیشتر در این خصوص، رک: پوربافرانی، حسن، «تعدد و تکرار در حقوق کیفری ایران»، فصلنامه مدرس علوم انسانی، ویژه‌نامه بهار ۱۳۸۴، ص. ۳۶.

۲. عباسی، اصغر، «نقدی بر مقررات تعدد جرم در قانون مجازات اسلامی مصوب ۱۳۹۲»، فصلنامه تعالی حقوق، دوره جدید، شماره ۷، تابستان ۱۳۹۳، ص. ۱۶۲.

۳. البته در آرای برخی از محاکم اعتقاد بر آن است که قواعد تعدد جرم که در ماده ۱۳۴ ذکر شده است تنها در خصوص جرایم غیرمشابه اعمال می‌شود و جرایم مشابه از شمول مقررات این ماده مستثنا هستند.

۴. در حالی که مطابق قانون مجازات اسلامی مصوب ۱۳۷۰ در خصوص این شخص تنها یک مجازات اعمال و مشمول تشدید می‌شد و چون میزان تشدید مشخص نشده بود، نهایتاً به حداکثر مجازات یعنی ۲۰ میلیون ریال جزای نقدی محکوم می‌شد.

از ۹۱ روز تا یک سال یا هر دو مجازات) محکوم شده و هر دو مجازات در مورد او اعمال خواهد شد.

اما در مورد غالب جرایم رایانه‌ای که مجازات‌هایی از درجه ۶ به بالا دارند، مطابق قاعده پیش‌گفته عمل می‌شود. برای مثال، اگر شخصی مرتکب دو جرم جعل رایانه‌ای و دو جرم کلاهبرداری رایانه‌ای شود، از آنجا که مجازات این دو جرم دارای حداقل و حداکثر است برای هر چهار جرم او حداکثر مجازات تا حداکثر مجازات به علاوه نصف تعیین می‌شود. یعنی برای دو جرم نخست به ۱۰ میلیون تا ۱۵ میلیون ریال جزای نقدی یا دو تا سه سال حبس یا هر دو مجازات و برای دو جرم اخیر به جزای نقدی از ۱۰۰ میلیون تا ۱۵۰ میلیون ریال یا حبس از ۵ تا ۷.۵ سال یا هر دو مجازات محکوم و مجازات اخیر در مورد او اعمال خواهد شد.

این گونه تشدید مجازات‌ها شاید در مورد جرایمی که مرتکبان آنها کمتر مرتکب جرایم متعدد می‌شود، موجب بازدارندگی از جرایم متعدد شود، اما در مورد مرتکبان جرایم سایبری چنین تشدید نمی‌تواند بازدارندگی کافی را ایجاد کند. توضیح آنکه در خصوص مجرمان سایبری وضعیت غالباً به نحوی دیگر است و ارتکاب جرایم متعدد از سوی آنها بیشتر از جرایم سنتی است. به عبارت دیگر، ارتکاب جرم از سوی آنها به کرات صورت می‌پذیرد، مانند آنکه کسانی که مرتکب نفوذ در سامانه‌ها می‌شوند، تنها یک سامانه را آماج جرم خود قرار نمی‌دهند، بلکه این رفتار مجرمانه را در ارتباط با سامانه‌های متعدد انجام می‌دهند. همچنین همان‌طور که در بخش نخست مقاله نیز بیان شد جرایم سایبری معمولاً با جرایم سایبری دیگر همراه هستند. به دیگر سخن، معمولاً مرتکب جرم دسترسی غیرمجاز، مرتکب جرایم دیگری چون جعل و تخریب رایانه‌ای و سرقت و کلاهبرداری رایانه‌ای هم می‌شود.

همچنین با توجه به سهولت ارتکاب جرم سایبری، احتمال اینکه اشخاص بسیار زیادی بزه‌دیده یک رفتار مجرمانه شوند، بالا است و در جرایمی که از طریق روش‌هایی چون فیشینگ واقع می‌شود، بزه‌دیدگان فراوانی درگیر جرم می‌شوند و موضوع ممکن است مشمول مقررات صدر ماده ۱۳۴ قرار گیرد.

از آنجا که معمولاً مجرمان سایبری از هوش و استعداد بالاتری نسبت به سایر مجرمان برخوردارند و آگاهی آنها نیز از قوانین و مقررات بیشتر است، به نظر می‌رسد محدودیت‌هایی که در میزان تشدید مجازات‌ها برای این دسته از بزه‌کاران در نظر گرفته شده است، کافی نیست. توضیح آنکه همان‌طور که در مثال بیان شد، چه تعداد جرایم ارتكابی سایبری چهار مورد باشد و چه صدها مورد، به لحاظ کیفی تفاوتی در میزان مجازات مرتکبان جرایم ندارد. از این رو بزه‌کاری که چهار جرم سایبری را



مرتکب شده است، می‌داند از این پس هر چقدر مرتکب جرم دیگر شود، تأثیری در میزان مجازات او ندارد.

البته با وضع قانون مجازات اسلامی جدید و پیش‌بینی جرمی به نام افساد فی‌الارض، این امکان برای قضات به وجود آمده است که با استناد به مقررات این ماده، مجازات اعدام را برای برخی از مرتکبان این جرایم اجرا کنند. اما علاوه بر نقد جدی که بر مقررات این ماده وجود دارد، باید توجه داشت در بسیاری از موارد نه شرایط اعمال مقررات این ماده وجود دارد و نه ضرورتی به تشدید مجازات مرتکبان جرایم سایبری متعدد به این اندازه وجود دارد.

البته باید توجه داشت هر چند اعمال نظامی چون جمع مجازات‌ها به نتایج بسیار سهمگینی می‌انجامد که ممکن است در عمل قابل اجرا نباشد،<sup>۱</sup> لکن باید توجه داشت با محدودیتی که در نظام ایجاد شده در ماده ۱۳۴ وجود دارد، نمی‌توان برای مرتکبان جرایم رایانه‌ای که معمولاً در ارتکاب جرم حساب سود و زیان ارتکاب جرم را می‌کنند، بازدارندگی مناسبی را ایجاد کرد. از این رو، باید راهکاری مدنظر قرار گیرد که بتواند انگیزه‌ای برای خودداری از ارتکاب جرایم دیگر برای بزهکاران سایبری ایجاد کند. از این رو، شاید وضع ضمانت‌اجراهایی چون تحمیل محرومیت از خدمات عمومی الکترونیک که در ادامه مقاله مورد توجه قرار خواهد گرفت برای این دسته از مجرمان مؤثرتر واقع شود.

### ۳-۱-۲. جرایم سایبری منجر به نتایج مجرمانه متعدد

با اینکه وقوع نتایج مجرمانه متعدد از رفتار واحد، همانند تعدد معنوی به واقع از مصادیق تعدد جرم نیست، اما قانون‌گذار نظام مشابهی با نظام تعدد مادی برای تعیین مجازات در این‌گونه موارد پیش‌بینی کرده است.<sup>۲</sup> به عبارت دیگر، مطابق تبصره ۱ ماده ۱۳۴ قانون مجازات اسلامی، چنانچه از رفتار مجرمانه واحد نتایج مجرمانه متعددی حاصل شود، مجازات‌ها به نحوی که در ماده ۱۳۴ بیان شده است، تعیین خواهد شد. برای مثال، چنانچه شخصی با انتشار صوت یا تصویر خصوصی دیگران موجب هتک حیثیت اشخاص مختلفی شود، با توجه به تعداد اشخاصی که از آنها هتک حیثیت شده

۱. جعفری، مجتبی، «تعدد جرم و آثار آن در قانون جدید مجازات اسلامی (مصوب ۱۳۹۲)»، مجله پژوهش حقوق کیفری، دوره ۲، شماره ۵، زمستان ۱۳۹۲، ص. ۱۸۹.

۲. برای مطالعه بیشتر راجع به تمایز این دو مورد، رک: فروغی، فضل‌الله؛ جودکی، بهزاد، «تعدد نتیجه در جرایم تعزیری بر اساس قانون مجازات اسلامی ۱۳۹۲»، فصلنامه دیدگاه‌های حقوق قضایی، شماره ۷۰، تابستان ۱۳۹۴، ص. ۱۰۳؛ بسامی، مسعود؛ وروایی، اکبر، «تعدد نتایج مجرمانه در فقه و حقوق کیفری ایران»، نشریه مطالعات فقه و حقوق اسلامی، سال ۷، شماره ۱۳، پاییز و زمستان ۱۳۹۴، ص. ۳۵؛ قیاسی، جلال‌الدین، «بررسی وحدت یا تعدد جرم در حالت تعدد نتیجه»، نشریه حقوق اسلامی، سال پنجم، شماره ۲۰، بهار ۱۳۸۸، ص. ۱۳۳.

است، مجازات مطابق ماده ۷۴۵ و به نحوی که فوقاً در خصوص تعدد مادی اشاره شد، تعیین می‌شود. یعنی اگر تعداد اشخاص ۲ یا ۳ نفر باشند مرتکب به ۲ سال حبس یا ۴۰ میلیون ریال جزای نقدی یا هر دو مجازات و اگر تعداد اشخاص ۴ نفر یا بیشتر باشند مرتکب به ۲ تا ۳ سال حبس یا جزای نقدی از ۴۰ میلیون تا ۶۰ میلیون ریال یا هر دو مجازات محکوم خواهد شد.

البته بند هـ ماده ۷۵۴ مقرر داشته است چنانچه جرم در سطح گسترده‌ای ارتکاب یافته باشد، مرتکب به بیش از دو سوم حداکثر یک یا دو مجازات مقرر محکوم خواهد شد. در این خصوص به نظر می‌رسد با وضع تبصره ۱ ماده ۱۳۴ قانون مجازات اسلامی که به نوعی مربوط به این موضوع می‌شود، این بند نسخ شده است و امکان جمع میان مقررات این بند و تبصره ۱ ماده ۱۳۴ وجود ندارد.

در این موارد هم به نظر می‌رسد با اینکه قانون‌گذار در مقام تشدید مجازات مرتکبان جرایمی است که از جرم واحد آنها نتایج مجرمانه متعددی حاصل شده است، لکن این تشدید ممکن است حداقل در مواردی با نتایج زیان‌بار جرم تناسب کافی را نداشته باشد و وضع محرومیت‌هایی مشابه آنچه در مورد تعدد مادی جرایم بیان شد، به ارتقای بازدارندگی مجازات‌ها کمک کند.

## ۲-۲. مجازات‌های تکمیلی جرایم سایبری متعدد

مجازات‌های تکمیلی مقرر در قانون مجازات اسلامی را می‌توان اقداماتی تأمینی دانست که قانون‌گذار اعمال آنها را برای پیشگیری از جرایم دیگر در خصوص مرتکبان پیش‌بینی کرده است. البته با توجه به تحولاتی که قانون مجازات اسلامی در خصوص اقدامات تأمینی و تربیتی ایجاد کرده است، این عنوان تنها در خصوص مجرمان غیرمسئول به کار می‌رود و اقدامات تأمینی‌ای که سابقاً در خصوص مجرمان مسئول اتخاذ می‌شد، در حال حاضر یا در قالب مجازات اصلی و یا مجازات تکمیلی تعیین می‌شوند.

قانون‌گذار در خصوص جرایم سایبری واحد، مجازات تکمیلی خاصی پیش‌بینی نکرده است. اما در قانون جرایم رایانه‌ای مجازات‌های تکمیلی خاصی برای مرتکبان تکرار جرم سایبری مقرر شده است. این مجازات‌ها شامل محرومیت از خدمات الکترونیکی عمومی است.<sup>۱</sup> این نوع مجازات‌ها از این جهت که مشمول هیچ‌یک از بندهای ماده ۲۳

۱. ماده ۷۵۵: در صورت تکرار جرم برای بیش از دو بار دادگاه می‌تواند مرتکب را از خدمات الکترونیکی عمومی از قبیل اشتراک اینترنت، تلفن همراه، اخذ نام دامنه مرتبه بالای کشوری و بانکداری الکترونیکی محروم کند: الف) چنانچه مجازات حبس آن جرم نودویک روز تا دو سال حبس باشد، محرومیت از یک ماه تا یک سال. ب) چنانچه مجازات حبس آن جرم دو تا پنج سال حبس باشد، محرومیت از یک تا سه سال.

نمی‌شوند، در خصوص مرتکبان جرایم سایبری واحد نمی‌شود. وضع این محرومیت‌ها نشان از این دارد که قانون‌گذار به حالت خطرناک مرتکبان تکرار جرم سایبری توجه داشته است. این در حالی است که در جرایم سایبری متعدد نیز که ممکن است مرتکب با ارتکاب جرایم متعدد یا با ایجاد نتایج مجرمانه متعدد خطرناکی خود را نشان داده باشد، تحمیل محرومیت از خدمات عمومی الکترونیک مجاز نیست با اینکه لازم است در چنین مواردی با وضع محدودیت‌هایی ابزار ارتکاب جرم را از دست این اشخاص دور نگاه داشت. مجازات‌هایی چون محرومیت از اشتراک اینترنت، تلفن همراه، اخذ دامنه مرتبه بالای کشوری و بانکداری الکترونیکی که در مورد مرتکبان تکرار از جرم پیش‌بینی شده است، می‌توانند اقدامات مناسبی برای جلوگیری از ارتکاب جرایم دیگر از سوی مرتکبان جرایم سایبری متعدد تلقی شوند. همچنین محرومیت‌های دیگری چون مسدودسازی وبگاه یا کانال‌های شبکه‌های مجازی متعلق به مرتکب، سلب نام‌های دامنه‌ای که مرتکب از آنها برای ارتکاب جرم استفاده کرده است و محروم کردن او از راه‌اندازی وبگاه یا کانال جدید، می‌توانند تأثیر به‌سزایی در ایجاد بازدارندگی و همچنین ناتوان‌سازی مرتکب از ارتکاب مجدد جرم داشته باشد.

البته باید توجه داشت از آنجا که برخی از این محرومیت‌ها می‌تواند بسیار شدید تلقی شده و با توجه به اینکه امروزه بخش عمده‌ای از خدمات عمومی از طریق یا به کمک فضای مجازی ارائه می‌شود، چنین محرومیت‌هایی ممکن است زندگی عادی مجرم را با محدودیت‌های زیادی روبرو سازد. از این جهت همان‌طور که در مقررات تکرار جرایم سایبری پیش‌بینی شده است، اعمال این محدودیت‌ها باید موقت و به صلاح‌دید قاضی صادرکننده حکم باشد. برای مثال، این امکان وجود دارد که محرومیت از اشتراک اینترنت به صورت خاص و محدود به اشتراک خانگی یا از طریق وسایل ارتباطی همراه مانند تلفن همراه یا وایمکس باشد.

افزون بر این محرومیت‌ها، شاید الزام به انجام خدمات عمومی رایانه‌ای مانند خدمت به نهادهای عمومی جهت شناسایی نقاط ضعف امنیتی سامانه‌های رایانه‌ای و مخابراتی مناسب باشد. البته در این خصوص با توجه به اینکه بند د ماده ۲۳ الزام به خدمات عمومی را به عنوان یکی از مجازات‌های تکمیلی مقرر کرده است، نقض قانونی وجود ندارد و لازم است قضات در هنگام تعیین مجازات‌ها به این بند و آیین‌نامه اجرایی آن<sup>۱</sup> توجه کافی داشته باشند. همچنین شاید مناسب باشد، امکان تخفیف مجازات اصلی

← (ج) چنانچه مجازات حبس آن جرم بیش از پنج سال حبس باشد، محرومیت از سه تا پنج سال.  
۱. لازم به ذکر است که مطابق ماده ۱۶ آیین‌نامه راجع به نحوه اجرای مجازات‌های تکمیلی موضوع ماده ۲۳ قانون مجازات اسلامی مصوب ۹۳/۱۱/۲۶ رییس قوه قضاییه که مقرر می‌دارد: «نحوه اجرای حکم دادگاه مبنی بر الزام



---

با توجه به میزان پایبندی محکوم به انجام این خدمات را به عنوان عاملی تشویقی برای ایجاد انگیزه در محکومان مورد توجه قرار داد.

محکوم به خدمات عمومی بر اساس آیین‌نامه اجرایی ماده ۷۹ قانون مجازات اسلامی است» این امکان وجود دارد که قضات در الزام محکوم به انجام خدمات عمومی از خدماتی چون خدمات مربوط به امور آموزشی و فنی و حرفه‌ای (موضوع بندهای الف و پ آیین‌نامه اجرایی ماده ۷۹ قانون مجازات اسلامی مصوب ۹۳/۶/۱۵ هیأت وزیران استفاده کنند.

## نتیجه‌گیری

ویژگی‌های فضای سایبر و امکان ارتکاب آسان جرایم سایبری متعدد از یک‌سو و ویژگی‌های مجرمان سایبری از سوی دیگر اقتضا می‌کند، پاسخ‌های کیفری خاصی در مورد این مجرمان اتخاذ شود. با توجه به مقررات فعلی تعیین مجازات در خصوص تعدد معنوی، تعدد مادی و جرایم موجب نتایج متعدد، لازم است در دو مورد اخیر، علاوه بر تشدید مجازات، محرومیت‌های متناسبی با جرایم سایبری بر مرتکبان این جرایم تحمیل شود. تحمیل این محرومیت‌ها چه به عنوان مجازات اصلی و چه به عنوان مجازات تکمیلی باعث می‌شود از یک سو مرتکبان، خود را در ارتکاب جرایم سایبری متعدد مطلق‌العنان ندانند و این پیام به آنها داده شود که هر چند مجازات‌هایی چون حبس و جزای نقدی در صورت ارتکاب جرایم بیشتر، از حد خاصی شدیدتر نمی‌شود، اما این امکان وجود دارد که قاضی با در نظر گرفتن تعداد جرایم یا نتایج مجرمانه محرومیت‌هایی بر او وضع کند که اثر شدیدی بر زندگی روزمره او خواهد گذاشت و از سوی دیگر باعث شود، مرتکبان جرایم سایبری متعدد خلع سلاح شده و ابزار ارتکاب جرایم احتمالی بعدی از دست آنها خارج می‌شود. لذا تعیین محرومیت از حقوق خدمات عمومی الکترونیک چون محرومیت از اشتراک اینترنت، تلفن همراه، اخذ دامنه مرتبه بالای کشوری و بانکداری الکترونیکی که در مورد مرتکبان تکرار از جرم پیش‌بینی شده است و همچنین محرومیت‌های دیگری چون مسدودسازی وبگاه یا کانال‌های شبکه‌های مجازی متعلق به مرتکب، سلب نام‌های دامنه‌ای که مرتکب از آنها برای ارتکاب جرم استفاده کرده است و محروم کردن او از راه‌اندازی وبگاه یا کانال جدید، می‌توانند تأثیر به‌سزایی در ایجاد بازدارندگی و جلوگیری از ارتکاب جرایم دیگر از سوی مرتکبان جرایم سایبری متعدد تلقی شوند.

## منابع

- بسامی، مسعود؛ وروایی، اکبر، «تعدد نتایج مجرمانه در فقه و حقوق کیفری ایران»، نشریه مطالعات فقه و حقوق اسلامی، سال ۷، شماره ۱۳، پاییز و زمستان ۱۳۹۴.
- پوربافرانی، حسن، «تعدد و تکرار در حقوق کیفری ایران»، فصلنامه مدرس علوم انسانی، ویژه‌نامه بهار ۱۳۸۴.
- جعفری، مجتبی، «تعدد جرم و آثار آن در قانون جدید مجازات اسلامی (مصوب ۱۳۹۲)»، مجله پژوهش حقوق کیفری، دوره ۲، شماره ۵، زمستان ۱۳۹۲.
- جوان جعفری، عبدالرضا، «جرایم سایبر و رویکرد افتراقی حقوق کیفری (با نگاهی به قانون مجازات اسلامی بخش جرایم رایانه‌ای)»، مجله دانش و توسعه، شماره ۳۴، اسفند ۱۳۸۹.
- زیبر، اولریش، جرایم رایانه‌ای، ترجمه محمدعلی نوری و دیگران، چاپ دوم، انتشارات گنج دانش، ۱۳۹۰.
- صادقی، حسین؛ و دیگران، اقتصاد جرم، تهران، نور علم، ۱۳۸۹.
- عباسی، اصغر، «نقدی بر مقررات تعدد جرم در قانون مجازات اسلامی مصوب ۱۳۹۲»، فصلنامه تعالی حقوق، دوره جدید، شماره ۷، تابستان ۱۳۹۳.
- فروغی، فضل‌الله؛ جودکی، بهزاد، «تعدد نتیجه در جرایم تعزیری بر اساس قانون مجازات اسلامی ۱۳۹۲»، فصلنامه دیدگاه‌های حقوق قضایی، شماره ۷۰، تابستان ۱۳۹۴.
- قیاسی، جلال‌الدین، «بررسی وحدت یا تعدد جرم در حالت تعدد نتیجه»، نشریه حقوق اسلامی، سال پنجم، شماره ۲۰، بهار ۱۳۸۸.
- محمدکوره‌پز، حسین؛ و دیگران، «نیم‌رخ جرم‌شناختی بزهکاران سایبری»، پژوهش حقوق کیفری، سال سوم، شماره نهم، زمستان ۱۳۹۳.
- مهرا، نسرین، «کیفر و چگونگی تعیین آن در فرایند کیفری انگلستان (با تأکید بر کارکرد کیفرها)»، مجله تحقیقات حقوقی، شماره ۴۵، بهار و تابستان ۱۳۸۶.
- وینتر، هارولد، اقتصاد جرم، ترجمه حمید بهره‌مند و زهرا ساکیانی، تهران، انتشارات دادگستر، ۱۳۹۴.
- Akhgar, Babak; Yates, Simeon, Intelligence Management, London, Springer, 2011.
- Scheb, John M; Scheb, John M, Criminal Law and Procedure, Belmont, CA, Wadsworth Cengage Learning, 2011.
- Williams, Matthew, Virtually Criminal, London, Routledge, 2007.
- Wiles, Jack; Reyes, Anthony, The Best Damn Cybercrime and Digital Forensics Book Period, Rockland, Mass, Syngress, 2007.