سیاست کیفری افتراقی در قلمرو ارکان متشکله جرائم سایبری

داود کرمی *

تاریخ دریافت ۱۳۹۵/۸/۳۰	تاریخ پذیرش ۱۳۹۶/۷/۲۳

سیاست کیفری افتراقی به جهت عدول از برخی اصول و معیارهای متعارف حقوق کیفری یا قبض و بسط آنها، یک سیاست کیفری ویژه و متمایز محسوب می‌شود. جرائم سایبری به‌عنوان دسته‌ای از جرائم نوظهور به جهت اینکه فضای سایبری را به‌عنوان موضوع یا وسیله جرم انتخاب می‌کند به دلایل مختلف نیازمند چنین سیاست کیفری افتراقی است. در این مقاله تلاش شده است تا ضرورت تدوین یک سیاست کیفری افتراقی برای جرائم سایبری در حوزه ارکان متشکله جرائم سایبری، براساس تفاوت‌های برجسته این جرائم با جرائم سنتی ازجمله تفاوت در ماهیت، گستره و بستر ارتکاب جرم تبیین شود و به دنبال آن گونه‌های این سیاست کیفری افتراقی با رویکردی توصیفی و توصیه‌ای در قلمرو این دسته از جرائم به‌ویژه در چارچوب نیازمندی‌های نظام کیفری ایران شناسایی و معرفی شود. نتیجه این تحقیق نشان می‌دهد منطق حاکم بر حقوق کیفری ماهوی جرائم سایبری در بسیاری موارد متفاوت از جرائم سنتی است. ازاین‌رو تدوین یک سیاست منسجم کیفری در برخورد با جرائم سایبری را ضروری می‌سازد. اثربخشی و کارایی قوانینی که برای مقابله با جرائم سایبر تصویب می‌شوند، مستلزم نگاهی متفاوت به مقولاتی مانند تعریف جرم، ارکان جرم، مسئولیت کیفری و امثال آن است. گرچه قانون جرائم رایانه‌ای مصوب ۱۳۸۸ به میزان چشمگیری در این مسیر گام نهاده است اما نیازمند تکامل و ارتقای بیشتری است.

کلیدواژه‌ها: جرائم سایبر؛ سیاست کیفری؛ فضای مجازی؛ رویکرد افتراقی؛ حقوق کیفری ماهوی

---

* استادیار دانشکده حقوق و علوم سیاسی، دانشگاه آزاد اسلامی واحد کرج؛
Email: karami.law@gmail.com

مقدمه

تبیین واکنش‌های کیفری در قوانین جزایی سنتی، عموماً از اصول و مبانی مشترکی پیروی می‌کند. در تعیین این واکنش‌ها تعریف جرم، عناصر متشکله آن، معیارهای مسئولیت کیفری و قواعد حاکم بر اعمال کیفرها، به‌گونه‌ای اجرا می‌شوند که عموماً کاربردی کمابیش یکسان و مشابه در مورد انواع جرائم و مجازات‌ها داشته باشند. سیاستگذاران حوزه کیفر تلاش می‌کنند برای تحقق عدالت و حفظ حقوق و آزادی‌های فردی قواعدی نسبتاً یکسان را برای مقابله با همه مصادیق بزه و بزهکاری به‌کار بندند. اما گاه ظهور و بروز مصالح و ارزش‌های نوین، ویژگی‌های خاص بزهکار و گستره بزه‌دیدگان یا آثار گسترده‌ای که گونه‌ای خاص از بزه (ازجمله جرائم سایبری) در جامعه دارد، باعث می‌شود قانونگذار در موارد استثنایی، معیارها، ضوابط و قوانین متمایز از معیارها، ضوابط و قوانینِ متعارف حاکم بر بزه وضع کرده یا به همین سبب آیین‌هایی متفاوت از شیوه‌های متداول دادرسی تعریف و تدوین کند.

نکته مهم و اساسی درباره جرائم سایبری، ویژگی‌های انحصاری آنها در مقایسه با جرائم سنتی است. در این نوع بزه، مرتکبان ناشناس در فضایی ناشناخته دست به اعمال مجرمانه می‌زنند. برخلاف جرم کلاسیک، جرم سایبری برخوردار از فناوری برتر و وسایل پیشرفته‌تری است. مرتکبان این جرائم با استفاده از فناوری نوین و ابزارهای جدید به اهداف شوم خود دست پیدا می‌کنند بدون آنکه اثری همانند جرم کلاسیک از خود برجای گذارند. ویژگی دیگر این دسته از جرائم عدم تشخیص درست طیف بزه‌دیدگان است؛ زیرا افراد و سازمان‌های متعددی می‌توانند هدف این مجرمان قرار گیرند. لذا جرم سایبری نشان‌دهنده محدوده گسترده از مجرمیت یا بزه‌دیده‌ای نامشخص است. این موضوع نشان می‌دهد مجرمان سایبری فارغ از زمان و مکان بوده و این نوع از جرائم هم‌اکنون جنبه فراملی و فراسرزمینی به خود گرفته است. فناوری‌های نوین در این عرصه و پیشرفت تجهیزات ارتباطی، مخابراتی و الکترونیکی، سهولت ارتکاب جرم در فضای سایبر، مجرمان را قادر ساخته که فعالیت‌های خود را بدون داشتن ارتباطی خاص با یک محل معین و مشخص، انجام دهند. پرواضح است که با وقوع این نوع از جرائم، خطری جدی برای جامعه بین‌المللی و جامعه داخلی یک کشور رقم می‌خورد.

با توجه به ویژگی‌های بیان‌شده برای جرائم ارتکابی در محیط سایبر، متوجه می‌شویم در این دنیا با ساختاری متفاوت نسبت به محیط فیزیکی و واقعی مواجه‌ایم که جرائم رخ داده در آن نیز دارای ویژگی منحصربه‌فرد است؛ برای مقابله با این‌گونه جرائم نمی‌توان با استراتژی‌های سنتی که در محیط واقعی کاربرد داشته، وارد این محیط شد و با آن برخورد کرد. جرائمی با این وسعت و ویژگی‌های انحصاری، مستلزم راهبرد ویژه‌ای در ابعاد مختلف است که بایستی الزاماً مختص این جرائم باشد. پژوهش پیش‌ِرو، تلاش دارد در مقام تبیین و تشریح سیاست کیفری متناسب جرائم سایبری، ضرورت‌های گزینشِ سیاست کیفری ویژه و متمایز از جرائم سنتی را از محور تحلیل ویژگی‌های خاص جرائم سایبری، تبیین کند و با توجه به شرایط و اقتضائات نظام کیفری ایران، گونه‌های این سیاست کیفری افتراقی را در برخی حوزه‌های حقوق کیفری ماهوی ازجمله قلمرو و ارکان متشکله جرم معرفی کند. البته اعمال یک سیاست کیفری افتراقی در ابعاد مختلف دیگر ازجمله حوزه مسئولیت کیفری، مجازات‌ها و قواعد شکلی نیز ضرورت اتخاذ دارد که تحلیل آنها در این مقال نمی‌گنجد و به نوشته‌های دیگر موکول می‌شود.

۱. اوصاف ویژه جرم سایبری

جرائم سایبری نوعی جرائم جدید است که طیف گسترده‌ای از افعال مجرمانه در این مفهوم جا دارد و ماهیت متغیر آن ناشی از پیشرفت لحظه به لحظه فناوری اطلاعات و شیوه‌های سوءاستفاده از آن است. تا آنجا که در جدیدترین و جامع‌ترین سند بین‌المللی در این زمینه که در کنوانسیون جرائم سایبر ۲۰۰۱ بوداپست به تصویب رسید، تعریفی از این جرائم به عمل نیامده و اختلاف‌نظرهایی نیز دراین‌باره وجود دارد (خرم‌آبادی، ۱۳۸۴: ۴۹). به‌طورکلی می‌توان گفت در تعریف جرائم سایبری دو معنی و مفهوم وجود دارد. در تعریف مضیق، جرم سایبری صرفاً عبارت از جرائمی است که در فضای سایبر رخ می‌دهد از این نظر جرائمی مثل هرزه‌نگاری، افترا، آزار و اذیت و سوءاستفاده از پست الکترونیکی و سایر جرائمی که در آنها کامپیوتر به‌عنوان ابزار و وسیله ارتکاب جرم به‌کار گرفته می‌شود، در زمره جرم سایبری قرار نمی‌گیرد. در تعریف موسع از جرم سایبری هر فعل و

ترک فعلی که «در» یا «از طریق» یا «به کمک» از طریق اتصال به اینترنت، چه به‌طور مستقیم، یا به‌طور غیرمستقیم رخ می‌دهد و توسط قانون ممنوع و برای آن مجازات در نظر گرفته شده است جرم سایبری نامیده می‌شود. بر این اساس جرائم سایبری را می‌توان به سه دسته تقسیم کرد: دسته اول، جرائمی هستند که در آنها رایانه و تجهیزات جانبی آن موضوع جرم واقع می‌شوند مانند سرقت، تخریب و ... . دسته دوم، جرائمی هستند که در آنها رایانه به‌عنوان ابزاری برای مجرم در ارتکاب جرم به‌کار گرفته می‌شود. دسته سوم، جرائمی هستند که می‌توان آنها را جرائم سایبری محض نامید. این نوع از جرائم کاملاً با جرائم کلاسیک تفاوت دارند و تنها در دنیای مجازی به‌وقوع می‌پیوندند اما آثار آنها در دنیای واقعی ظاهر می‌شود؛ مانند دسترسی غیرمجاز به سیستم‌های رایانه‌ای (حسن‌بیگی، ۱۳۸۴: ۱۸۷). به‌نظر می‌رسد صرف‌نظر از اختلاف‌نظرها در این مقوله کامل‌ترین تعریفی که با توجه به رویکرد قانون جرائم رایانه‌ای مصوب ۱۳۸۸، بتوان ارائه کرد بدین صورت باشد: «هر جرمی که قانونگذار به‌صراحت رایانه را به‌منزله موضوع یا وسیله جرم جزء رکن مادی آن اعلام کرده باشد، یا عملاً رایانه به‌منزله موضوع یا وسیله ارتکاب یا وسیله ذخیره یا پردازش یا انتقال دلایل جرم در آن نقش داشته باشد»، جرم رایانه‌ای تلقی می‌شود.

بستر جرائم سایبری که نشانگر محل ارتکاب بزه‌های سایبری است، جایگاهی هم‌اندازه جهان واقعی و چه‌بسا بزرگ‌تر از آن است که از ابزارهایی همچون رایانه، شبکه، اطلاعات و موج آفریده شده که شناسایی تک‌تک جرائم سایبری منوط به شناخت این بستر است. گفتنی است نوین بودن جرائم سایبری به‌دلیل نوین بودن بستر ارتکاب این جرائم است که این خود وابسته به اجزای جدیدی است که پدیدآورنده این بسترند؛ درواقع همین نوین بودن بستر ارتکاب جرم به‌دلیل ویژگی‌های خاص و منحصربه‌فرد آن، سبب تغییر شیوه ارتکابی جرائم سایبری نسبت به جرائم سنتی شده است و نتیجتاً زمینه را برای ویژه‌سازی سیاست کیفری فراهم کرده است. ماهیت خاص و منحصربه‌فرد فضای سایبر سبب شده تا شیوه ارتکابی جرائم سایبری در تقابل با جرائم سنتی تغییرات اساسی کند؛ ازجمله می‌توان سرعت بالای ارتکاب جرم، فنی و تخصصی بودن ارتکاب جرم، بالا بودن رقم سیاه بزهکاری یا گستره نتایج جرم را ذکر کرد که ذیلاً به آنها پرداخته می‌شود.

۱-۱. سرعت بالای ارتکاب جرم

در ارتکاب جرم سنتی، مرحله اول قصد مجرمانه است که به نیت مجرمانه فرد برمی‌گردد و بعد از مرحله قصد که خواست انجام عمل شکل می‌گیرد، نوبت به تهیه مقدمات می‌رسد. بعد از تهیه مقدمات، عملیات اجرایی جرم شروع می‌شود. در مرحله عملیات اجرایی ممکن است ارتکاب جرم به سرانجام نرسد. گاهی علت انصراف، ارادی و گاهی غیرارادی است. به‌هرحال اگر به علل غیرارادی، جرم به انجام نرسد مورد شروع به جرم، جرم عقیم و جرم محال پیش می‌آید. اما اگر مجرم عمل خود را به اتمام رسانده و موفق به ارتکاب جرم شود با جرم تام روبه‌رو می‌شویم؛ نکته جالب توجه اینکه در همه این مراحل گذشت زمان مشهود است. این مرحله زمانی از چند ثانیه تا چند روز یا چند ماه می‌تواند مطرح باشد. اما در مقابل، در جرائم سایبری این مدت زمان به چند ثانیه یا کسر ثانیه تبدیل می‌شود. فرد مرتکب از لحظه ورود داده غیرواقع تا کسب مال، زمان بسیار کمی را طی می‌کند. از لحظه ارسال تا دریافت مطالب افتراآمیز در کل شبکه فقط ثانیه‌ای یا کمتر زمانی می‌گذرد، برعکسِ زمان ارتکاب جرم در فضای واقعی که می‌توانستیم بین مراحل تفکیک قائل شویم، در این حالت مراحل زمانی ارتکاب جرم را همزمان نشان می‌دهد؛ در فضای سایبر زمان به حداقل ممکن رسیده است. از طرف دیگر مرتکب می‌تواند، با استفاده از خصوصیات پیش‌گفته، برای یک‌بار برنامه‌ای را روی رایانه هدف نصب کند که مثلاً به‌طور مکرر مبالغ ناچیزی از حساب یک فرد یا شرکت برای او واریز شود و این امر تا بی‌نهایت تکرار شود؛ این بدان علت است که عمل فیزیکی که مجرم انجام می‌دهد یک‌بار انجام می‌شود، اما رایانه به‌طور خودکار آن را تکرار می‌کند (زیبر، ۱۳۸۳: ۶۹). به‌موازات همین سرعت، همه فعالیت‌های غیرمشروع انجام شده در آن، که گاهی عنوان جرم سایبری به‌خود می‌گیرد، در مدت خیلی کوتاهی به‌طور همزمان و در امکنه متعدد و مختلف انجام می‌شود. به‌تبع همین ویژگی یعنی خروج از قیود زمان و مکان، معادلات کیفری که به‌طور معمول تابع زمان یا مکان یا هر دو می‌باشند، نظیر قواعد سنتی مربوط به صلاحیت دادگاه‌ها که به‌تبع چالش تعیین مکان و زمان وقوع جرم دچار ابهام شده‌اند، بهم خورده است که خود ایجاد قواعد جدید با جرم‌انگاری‌های جدید را درزمینه مسائل کیفری در فضای سایبر می‌طلبد (Wilson, 2003: 146).

۲-۱. فنی و تخصصی بودن

جرائم سایبری از نظر ساختاری، غالباً جرائمی پیچیده هستند؛ چراکه ساختار فضای سایبر، ساختاری فنی و پیچیده است. در غالب موارد مرتکبان زمان زیادی را برای برنامه‌ریزی و پنهان‌سازی اعمالشان صرف می‌کنند تا جرم را به‌طور کامل و بدون نقص انجام دهند و در نتیجه کشف جرم و تعقیب مجرم آن با دشواری همراه می‌شود. مرتکبان دارای چندین هویت مجعول و بعضاً در مواردی که عواید مالی به‌همراه دارد از طریق پاک‌سازی درآمدهای حاصله به‌واسطه شرکت‌های قانونی اقدام می‌کنند که کاملاً پیچیده است. منظور از تخصصی بودن، صرفاً وجود توانایی خاص در ورود به این فضا نیست؛ چراکه هر شخص عادی با استفاده از رایانه قادر به ورود به این فضا خواهد بود. لیکن، پیچیدگی این فضا امری فراتر از صرف ورود به این دنیاست. برنامه‌ریزی‌های رایانه‌ای تخصصی، تشخیص اقدامات آسیب‌رسان در فضای سایبر، نحوه استفاده ایمن از این فضا، نحوه شناسایی و مقابله با مجرمان سایبری، تأثیر فضای سایبر بر فرهنگ و جامعه و بسیاری از امور اساسی و کلیدی که در این راستا باید بر آن اشراف داشت، نیازمند وجود تخصصی متناسب با پیچیدگی و فنی بودن این فضاست. جرائم سایبری غالباً جنبه حیله‌آمیز دارد و بیشتر مبتنی‌بر سوءاستفاده از نبوغ، تواناییِ فکری و استعداد هستند و وسیله ارتکابی جرم غالباً مبهم و نامحسوس است یا میزان تأثیر وسیله در ارتکاب جرم مشخص نیست. به‌طور مثال، جرائمی همچون پولشویی الکترونیکی یا کلاهبرداری رایانه‌ای با سوءاستفاده از داده پیام‌های مالیِ افراد، سرقت اطلاعات مالی و سوءاستفاده از آن، همواره مبتنی‌بر اشراف و درایت مرتکب است و نیز، وسایل ارتکاب این جرائم رؤیت‌پذیر نیستند. در این دسته جرائم، وسایل ارتکاب جرم، همچون خودِ جرم جنبه تخصصی و فنی داشته و با میزان حرفه‌ای و کارشناس بودن مرتکب ملازمه دارند، چراکه جرم سایبری اعمالی غیرخشن است. این جرائم با استفاده از رایانه، سامانه‌های مخابراتی، تبلیغات و ... ارتکاب می‌یابند و نه با چاقو و سلاح گرم. ویژگیِ نوعی جرم سایبری تقلب است و نه خشونت. از طرفی، ویژگی فنی بودن جرائم سایبری سبب می‌شود، میزان کشف جرم نسبت به جرائم سنتی کاهش یابد؛ چراکه ازیکسو مأموران کشف جرم تخصص کافی در مقابله با جرائم فنی و

انجام تحقیقات را ندارند و ازسوی‌دیگر، بزهکار بدون حضور در صحنه جرم می‌تواند آثار ارتکاب و ادله جرم را از بین ببرد. امری که در جرائم سنتی امکان وقوع آن بسیار پایین است و در صورت رجوع مرتکب به صحنه ارتکاب جرم احتمال دستگیری آن وجود دارد اما در جرائم سایبری مرتکب بدون حضور در محل وقوع جرم می‌تواند ادله جرم را مدیریت کند.

۳-۱. حجم و مقیاس جرائم سایبری

از ویژگی‌های جرائم دنیای واقعی این است که مدل ارتکابی جرم به‌صورت نرم «یک‌به‌یک» تبعیت می‌کند. بدین بیان که مرتکب معمولاً با قربانی درگیر می‌شود. در جرائم اساسی ازجمله قتل، تجاوز به عنف، احراق و ...، مرتکب معمولاً یک قربانی را هدف قرار می‌دهد و تمام توجهش به تکمیل آن جرم متمرکز می‌شود (Brenner and Rico, 1993: 255). وقتی جرم کامل شد در آن صورت مرتکب به سمت دیگر بزه‌دیدگان و دیگر جرائم حرکت می‌کند. قاعده «یک‌به‌یک» در جرائم دنیای واقعی ناشی از محدودیت فیزیکی تحمیل‌شده به فعالیت‌های انسان، است؛ یک سارق نمی‌تواند در آن‌واحد بیش از یک کیف پول بردارد؛ ازاین‌رو جرائم دنیای واقعی، جرائم سریالی هستند. مضاف بر اینکه مجرم و قربانی عموماً در یک روستا یا یک محله شهری زندگی می‌کنند و مجرم از قبل قربانی خود را شناسایی کرده آنگاه روی وی مرتکب جرم می‌شود. لذا همین امر فرصت مناسبی است که مجرم ازسوی قربانی جرم شناسایی شود؛ اگر مرتکب با مجرم روابط اجتماعی نداشته باشد و اصطلاحاً غریبه باشند، غریبگی مجرم احتمال شناسایی وی را افزایش می‌یابد و شهروندان محلی نقش بسزایی جهت توجه به کسانی می‌کنند که تعلقی به آن محل ندارند. بنابراین، تحقیقات یک جرم سنتی اساساً روی منطقه جغرافیایی خاص که جرم در آن رخ داده متمرکز می‌شود (Egger and Blindness, 1990: 163). این محدودیت‌ها به دستگاه عدالت کیفری این اجازه را می‌دهد که برنامه‌های ضروری را برای مقابله با جرم و مجرم آن پیش‌بینی کند. اما در جرائم سایبری با استفاده از تکنولوژیِ نوین، قاعده «یک به چند» مورد استفاده قرار می‌گیرد. لذا با توجه به ویژگی‌های انحصاری فضای

سایبر، قربانی کردن هزاران یا حتی میلیون‌ها نفر طی اقدامی واحد، فرضی حقیقی و باورکردنی در این فضا است (Brenner, 2005: 53). این امر باعث می‌شود که حجم و آمار بزه در دنیای دیجیتال با دنیای واقعی قابل قیاس نباشد. به‌طور مثال در سال ۲۰۰۲ در ایالات متحده، بیش از ۹۰ درصد بنگاه‌های صنعتی تحت تأثیر حملات سایبری بوده‌اند و صدها میلیون دلار خسارت دیده‌اند (Vaca, 2002: 68).

۴-۱. وسعت ایراد خسارت

موضوع جرائم سایبری از لحاظ اهمیت و میزان خسارات وارده با جرائم سنتی تفاوت دارد. تصور کنید یک یا چند نفر سارق با ورود به منزل یا حتی بانک کلیه اثاثیه منزل یا وجوه موجود در بانک را سرقت می‌کنند. حداکثر خسارات وارده را که می‌توان در اثر ارتکاب این جرم تصور نمود چقدر است؟ حال سرقت اطلاعات محرمانه یک شرکت تجاری یا سرقت فعالیت‌های پژوهشی که روی شبکه قرار دارد، حداقل خسارتی را که می‌توان از آن صحبت کرد شاید فراتر از میلیون‌ها دلار باشد که با ده‌ها سرقت گانگستری بزرگ نیز برابری نمی‌کند. تفاوت بین این دو از آنجا ناشی می‌شود که سرقت اطلاعات از روی شبکه با محدودیت‌های فیزیکی که در سرقت از منازل یا بانک وجود دارد مواجه نیست و تنها چیزی که می‌تواند برای متجاوز به سیستم محدودیت ایجاد کند، امکانات کامپیوتری است که در اختیار دارد. یا در جرمی مثل ترویج عکس‌ها و تصاویر مستهجن و مبتذل، اگر حالت سنتی و فیزیکی آن را در نظر بگیریم، مرتکب مزبور اگر امکانات بسیار پیشرفته تکثیر و چاپ و نیروی انسانی کافی در اختیار داشته باشد، چه تعداد ازاین‌گونه تصاویر را در اختیار چند نفر می‌تواند قرار دهد؟ درحالی‌که کافی است بزهکار با نشستن پشت کامپیوتر و اتصال به اینترنت، تنها با فشار یک کلید و در مدت زمان بسیار کوتاهی هزاران تصویر از این دست را منتشر کنند.

تا یک دهه پیش، جرائم سایبری حجمی در کل جرائم جهان نداشت اما این رقم در سال‌های اخیر به صدها میلیارد دلار رسیده است؛ یافته‌های مؤسسه پژوهشی CSIS نشان می‌دهد جرائم سایبری سالانه ۴۴۵ میلیارد دلار به اقتصاد جهانی لطمه می‌زند و بیش از ۱۶۰

میلیارد دلار از این رقم خسارت به صاحبان مشاغل مربوط است. علت اصلی وارد شدن چنین خسارت سنگینی به صاحبان مشاغل و کسب‌وکار، نقض حقوق مالکیت معنوی و سرقت داده‌های حساس است که در اثر فعالیت‌های مختلف هکری اتفاق می‌افتد. در گزارش CSIS (مرکز مطالعات استراتژیک و بین‌المللی)، تصریح شده که جرائم سایبری ازجمله جرائم در حال رشد است که به خلاقیت، فضای رقابتی بازار و انواع تجارت، آسیب وارد می‌کند. این مؤسسه میزان خسارت را در یک برداشت محافظه‌کارانه ۳۷۵ میلیون دلار و در برداشتی حداکثری بیش از ۵۷۵ میلیون دلار برآورد کرده است (http://www.cyberbannews.com).

بی‌شک از عمده عواملی که سبب می‌شود جرمی دارای نتایج زیانبار بیشتری نسبت به سایر جرائم باشد، ارتکاب آن از طریق شبکه است. این امر اختصاص به شبکه‌های رایانه‌ای ندارد بلکه ارتکاب جرم از طریق شبکه اعم از شبکه‌های انسانی یا شبکه اشخاص حقوقی به‌طورکلی دارای چنین ویژگی‌ای است. درواقع قاعده مسلم این است که جرائمی که با زنجیره‌ای از عوامل تأثیرگذار ارتکاب می‌یابند به‌مراتب آثار بیشتر، قدرتمندتر و البته زیانبارتری نسبت به سایر جرائم دارند و از همین روست که قانونگذاران ارتکاب جرم از طریق شبکه‌های سازمان‌یافته را از علل مشدده مجازات می‌دانند. جرائم سایبر نیز در ارتکاب از فضای شبکه بهره می‌گیرند و بهره‌گیری از فضای گسترده شبکه‌های مجازی، گستره‌ای عظیم‌تر از دنیای واقعی را در اختیار می‌گذارد که آنان را قادر می‌سازد با صرف نیروی فکری، ضرباتی جبران‌ناپذیر و خساراتی سهمگین در بُعد بین‌المللی وارد آورند. به‌طور مثال، در شهریورماه سال ۱۳۷۸ یک مهاجم اینترنتی در گوشه نامعلومی از جهان هنگامی‌که احزاب سیاسی استرالیا، سرگرم مبارزات انتخاباتی بودند وارد تارنمای وب حزب حاکم لیبرال استرالیا شد و ضمن ایجاد تغییرات در محتوا، مطالب آن را به‌صورت مضحکی درآورد و در پایان چند عکس مستهجن نیز ضمیمه آن کرد. این عمل مهاجم ناشناس، لطمه شدیدی به حیثیت حزب لیبرال وارد ساخته بود (.Ibid).

بنابراین، خسارات ناشی از جرائم سایبری که بیشتر مبتنی‌بر سوءاستفاده از نبوغ، توانایی فکری و استعداد افراد می‌باشد، در دهه اخیر بیش‌ازپیش افزایش یافته است. در کشورهای

توسعه‌یافته، محدود کردن آثار این نوع جرم به‌دلیل سازوکارهای قانونیِ مناسب، برای جلوگیری از تکرار آن امکان‌پذیر است؛ اما در کشورهای در حال توسعه، ضعف و ناتوانی برخی نهادها و سازمان‌ها موجب شده است هزینه بزهکاری سایبری و نیز تأثیر درازمدت آن بر توسعه پایدار چشمگیر باشد؛ درواقع آسیب‌پذیری این دسته از کشورها در مقابل جرائم سایبری بیشتر است (Ringwelski, 2001). عواقب جرائم سایبری نه تنها خسارت‌های اقتصادی سنگینی را به دنبال داشته بلکه تهدیدی جدی برای امنیت بشر است؛ زیرا تمام کشورها در امور حساس اعم از پزشکی، مخابراتی، هواپیمایی، امور امنیتی و ... وابسته به عملکردهای رایانه بوده که کوچک‌ترین اخلال در سیستم، صدمات جبران‌ناپذیری را بر جای خواهد گذاشت. بنابراین بدون توجه به تدوین رویکرد افتراقی که متناسب با این حجم از آثار زیانبار جرائم سایبری باشد، نمی‌توان انتظار مقابله کارآمد با تهدیدات سایبری را داشت.

۵-۱. بالا بودن رقم سیاه بزهکاری

با افزایش به‌کارگیری رایانه در همه عرصه‌های زندگی و همچنین سهولت استفاده از آن و گسترش شبکه جهانی اینترنت، امروزه جرائم سایبری می‌تواند به‌وسیله هر شخصی در هر نقطه‌ای از دنیا به‌وقوع پیوندد و با آنکه تحقیقات به‌عمل آمده نشان از روند رو به رشد جرائم سایبری دارند اما تعداد آمار موجود نمی‌تواند ما را به نتیجه‌گیری مطلوب رهنمون سازد چه‌بسا این آمار منعکس‌کننده تعداد جرائم مکشوفه‌اند و نه تعداد جرائم واقعی (Rizgar, 2010: 610). به‌عنوان یکی از بارزترین خصوصیات جرائم اینترنتی که ناظر به ماهیت ویژه آنهاست، می‌توان به غیرقابل تخمین بودن میزان ارتکاب دقیق این‌گونه جرائم اشاره کرد؛ یعنی همان وجود رقم سیاه[1] بسیار بالا در بزهکاری است. بالا بودن رقم سیاه در جرائم سایبری مبتنی‌بر چند عامل است: اول آنکه تکنولوژی پیشرفته یعنی ظرفیت حافظه رایانه و سرعت بالای عملیات موجب کشف دشوار جرائم سایبری است. دوم، به‌دلیل نبود سابقه و شناخت درخصوص جرائم سایبری، بزه‌دیدگان و مأموران اجرای قانون پس از مدتی متوجه وقوع جرم می‌شوند و دسته آخر بسیاری از بزه‌دیدگان توان تشخیص، پیشگیری و

1. Dark Number

مقابله با حوادث مربوط به این‌گونه جرائم را ندارند. از طرف دیگر مرتکبان حرفه‌ای، غالباً از خود مدرکی به‌جا نمی‌گذارند. اطلاعات قابل نسخه‌برداری است بدون آنکه از محل خود برداشته شود و سوابق هم قابل پاک شدن هستند. همچنین عدم تمایل بزه‌دیدگان برای اعلام وقوع جرائم سایبری پس از کشف آنها می‌باشد. در بخش تجارت این عدم تمایل به دو امر مربوط می‌شود. برخی بزه‌دیدگان ممکن است به‌دلیل هراس از تبلیغات سوء، رسوایی یا از دست دادن حسن شهرت خود تمایلی به فاش ساختن اطلاعات نداشته باشند. دیگر بزه‌دیدگان نیز از سلب اعتماد سرمایه‌گذاران و یا عامه مردم و پیامدهای اقتصادی ناشی از آن واهمه دارند (Dorumodd and Foss, 2006: 56). برخی کارشناسان بر این باورند که این عامل تأثیر چشمگیری بر کشف جرائم سایبری دارند. «قربانی که کارش برمبنای شهرت به مورد اعتماد بودن استوار است ـ مانند بانک یا شرکت بیمه ـ بعید است این واقعیت را که سوابق اطلاعاتی آن دست‌کاری شده و مجرم نیز ناشناس است، علنی سازد»(Sieber, 1994: 476). همچنین بزه‌دیدگان چون احتمال کمی برای پیدا کردن مجرم با گرفتن غرامت به‌دلیل ضرر وارده می‌دهند، از پیگیری آن دوری می‌کنند. لذا برای مبارزه و پیشگیری از جرائم سایبری همکاری بزه‌دیده بسیار مهم و حائز اهمیت است (گرایلی، ۱۳۸۹: ۱۶۲).

ازجمله مهم‌ترین آثار بالا بودن رقم سیاه یک بزه، کاهش اثر بازدارندگی مجازات‌های احتمالی موجود است؛ زیرا بالا بودن رقم سیاه به معنی کاهش احتمال دستگیری و اعمال کیفر است. در تحلیل اقتصادی از جرم و مجازات و در چارچوب تئوری انتخاب عقلایی[1] هرچه احتمال دستگیری و در نتیجه اجرای مجازات کاهش یابد، اثر بازدارندگی مجازات‌های قانونی موجود کمتر شده و در نتیجه احتمال ارتکاب جرم افزایش می‌یابد (Cooter and Ulen, 2004: 34).

۶-۱. پراکندگی جغرافیایی جرائم سایبری

درواقع، جرائم سنتی از یک الگوی دموگرافیک و جغرافیایی معین پیروی می‌کنند. جرائم معمولاً در مکان‌های مشخص از یک شهر رخ می‌دهند. از طرفی، گروه‌های انسانی که

1. Rational Choice

مرتکب جرم می‌شوند، قابل شناسایی هستند. جرائم در حد قابل شناسایی در یک حوزه مشخص جغرافیایی و دموگرافیک رخ می‌دهند. این امر نهادهای اجرای قانون را قادر می‌سازد تا نیروها و منابع خود را در مناطقی که جرائم احتمالاً واقع می‌شوند متمرکز سازند و نسبت به ارتکاب آنها، واکنش‌های بموقع و مناسب از خود بروز دهند. اما در محیط سایبر به‌دلیل عدم حضور فیزیکی مجرم در صحنه وقوع جرم، سبب می‌شود شیوه‌های کلاسیک کشف جرم و شناسایی مجرم با دشواری یا کُندی صورت گیرد؛ و در غالب موارد مرتکب و بزه‌دیده هزاران کیلومتر از هم فاصله دارند و معمولاً بزهی که واقع می‌شود، بزهکار و بزه‌دیده ناشناس باقی می‌ماند و غالباً نیز دستگیر نمی‌شود (Campbell, 2000). بنابراین، این خصیصه جرائم سایبری، روند جمع‌آوری ادله اثبات جرم را با مشکلات و محدودیت‌های خاص خود توأمان می‌سازد. ازاین‌رو، مفهوم متعارف زمان و مکان در فضای سایبر دچار تحول شده است؛ زیرا ازجمله فاکتورهای کُندی وقوع پدیده مجرمانه در دنیای واقعی بعد مکانی میان سه ضلع بزهکاری یعنی بزهکار، بزه‌دیده و مکان ارتکاب بزه است. ساختار فضای سایبر به نحوی است که در آن قرابت مکان میان سه عنصر مذکور، ضرورتی ندارد. این وضعیت موجب صرفه‌جوییِ شگرفی از بعد زمان و هزینه‌بری بزهکاران سایبری شده و آنها را قادر ساخته بدون وجود مانعی به نام مکان، جرائم متعددی را در سریع‌ترین زمان مرتکب شوند.

توجه به ویژگی‌ها و تمایزات بزه‌های فضای سایبر، تبیین یک رویکردِ ویژه در مقایسه با بزه‌های ارتکابیِ دنیای واقعی را امری قابل درک می‌سازد. بررسی اختصاصاتِ جرائم سایبری ما را به این حقیقت رهنمون می‌سازد که مدل‌های ارتکاب جرم در این فضا با مدل‌های جرائم سنتی تمایزات و تقابلات قابل توجهی دارند. رویکرد کیفری سنتی موجود مربوط به زمانی است که تکنولوژی، دوران ابتداییِ خود را سپری می‌کرد. اما امروزه رشد و توسعه فناوری، امکان استفاده از نیروهای انسانی سازمان‌یافته و منابع و امکانات متمرکز برای مقابله با بزهکاران فضای سایبر را سلب کرده است. بنابراین، مانند سایر حوزه‌های سیاست جنایی مقابله با جرائم سایبری، اقدام کیفری اثربخش در بعد ماهوی نیز مستلزم رویکرد خاصی است، که از آن به رویکرد افتراقی یاد کردیم. در ادامه سعی می‌شود الگوهایی گزینشی از رویکرد کیفری منظور

در حقوق جزای ماهوی از منظر تئوری‌های عمومی حقوق کیفری با تأکید بر حقوق کیفری ایران، مورد تجزیه و تحلیل قرار گیرد. شایان ذکر است این قواعد افتراقی در حوزه حقوق کیفری ماهوی حول محور جرم، مجرم و مجازات می‌چرخد که با توجه به گستردگی آن، در این مقاله سعی شده قواعد افتراقی حول محور ارکان متشکله جرم بررسی شود و سایر الزامات مانند قواعد افتراقی مربوط به مجرم و مجازات به فرصتی دیگر موکول شود.

۲. گونه‌های سیاست کیفری افتراقی ماهوی در حوزه عناصر تشکیل‌دهنده جرائم سایبری

سیاست کیفری افتراقی در حقوق ماهوی ناظر به عدول قانونگذار از اصول و قواعد شناخته‌شده‌ای است که نسبت به عموم جرائم اعمال می‌شود. برای بررسی سیاست کیفری افتراقی در حوزه جرم، لاجرم بایستی تحولات مربوط به عناصر تشکیل‌دهنده جرم در قلمرو جرائم سایبری مورد بررسی قرار گیرد. هر جرمی از سه رکن تشکیل شده است: الف) رکن قانونی؛ ب) رکن مادی؛ ج) رکن معنوی. ماهیت خاص و ویژگی‌های انحصاری جرائم سایبری سبب شد قانونگذاران در ارکان سه‌گانه تشکیل‌دهنده جرائم تحولاتی ایجاد کنند تا زمینه مقابله کارآمدتر با این حوزه از جرائم فراهم آید که در موارد لزوم این امر با عدول و نقض برخی اصول و تأسیسات حقوق کیفری سنتی، توأمان است.

۲-۱. راهبردهای ویژه در حیطه رکن قانونی

رکن قانونی به‌نظر بسیاری از حقوقدانان یکی از عناصر سه‌گانه جرم است که براساس آن، نوع تخلف صورت گرفته و مجازات مرتکب، باید در قانون پیش‌بینی شده باشد (اردبیلی، ۱۳۹۲: ۱۳۵). این سؤال به ذهن متبادر می‌شود که آیا این عنصر در همه جرائم صادق است؟ با کمی تعمق به این نتیجه می‌رسیم که رکن قانونی بایستی در همه جرائمی که عمداً یا سهواً حاصل می‌شود مصداق داشته باشد؛ «جرائم جزایی به‌طور دقیق و به‌صورت مواد قانونی توسط مقنن، تعیین‌شده و هر یک ارکان مخصوص به خود را دارد. بنابراین جرم جزایی عبارت از نقض متنی از متون خاص قانونی است» (شامبیاتی، ۱۳۹۱: ۲۱۷). ازاین‌رو،

هرقدر عمل انسان مخالف هنجارهای یک اجتماع باشد، تا زمانی که قانون به آن تصریح نکرده، جرم محسوب نمی‌شود. فایده اصل قانونی بودن جرم و مجازات، قابل پیش‌بینی شدن امور جامعه برای فرد و اجتماع است؛ افراد یک اجتماع با آگاهی از افعال مجاز و غیرمجاز سعی در تطبیق خود با این مواردِ امری خواهند کرد تا در معرض مجازات و کیفر قرار نگیرند (دزیانی، ۱۳۷۳: ۵۸). چنین اجتماعی که با قابلیت پیش‌بینی بالا در اعمال مجاز و ممنوعه، نظام قانونی خود را مدون کرده، می‌تواند امیدوار باشد که افرادِ جامعه قانون را بهتر رعایت کنند؛ در نتیجه قوانین و مقررات اعتبار بیشتری خواهند داشت. بنابراین رفتاری جرم محسوب می‌شود که به درجه‌ای از اهمیت رسیده باشد که جامعه خواهان مقابله کیفری با آن بوده و به‌صراحت در قانون جرم‌انگاری شود و در همان قانون به‌طور شفاف و مضیق رفتار مجرمانه تعریف شود. اما با پیدایش جرائم محیط سایبر با طرق نوینی از رفتارهای بزهکارانه فنی روبه‌رو شده‌ایم که حقوق کیفری ماهوی به‌ویژه در قلمرو رکن قانونی، پیش از گذشته در برخورد با این نوع از جرائم به‌لحاظ ویژگی‌های خاص فضای سایبر و نوعِ منحصربه‌فرد این جرائم، با چالش‌های عدیده‌ای روبه‌رو شده است که به‌ناچار از اصول پیش‌گفته ازجمله اصل قانونی بودن، اصل شفافیت قوانین کیفری، عناصر تشکیل‌دهنده جرائم، جرم‌انگاری انحرافات و ... که از ملزومات رعایت رکن قانونی محسوب می‌شوند، عدول می‌کند. بنابراین، نظام‌های قانونگذاری برای مواجهه هر چه کارآمدتر با این جرائم، اقدام به وضع قواعد افتراقی در قلمرو عنصر قانونی جرائم سایبری کردند که ذیلاً به تحلیل برخی از آنها خواهیم پرداخت.

۱-۱-۲. مفهومی کردن تعریف جرم سایبری

یکی از شیوه‌های بسیار حیاتی و ضروری درزمینه اتخاذ رویکرد افتراقی در قلمرو جرائم سایبری این است که با توجه به نوین بودن و پویایی فضای سایبر و متعاقب آن ظهور شیوه‌ها و جنبه‌های جدید جرائم در این فضا، سیستم قانونگذاری بایستی به سمت مفهومی شدن حرکت کند تا با ظهور مصادیق جدید با خلأ تقنینی مواجه نشویم. چراکه یکی از مشکلات عمده تعریف جرم سایبری تحول سریع شیوه‌های ارتکاب آن و ایجاد مصادیق

جدید است که شاید چتر تعاریف سابق نتواند آنها را بپوشاند. لذا در تعریف جرم سایبری باید اولاً، به‌گونه‌ای باشد که شامل تمام مصادیق سوءاستفاده از فضای سایبر باشد و ثانیاً، مصادیق احتمالی جدید را هم بتواند شامل شود و به‌این‌ترتیب عمر طولانی‌تری پیدا کند (مرهج الهیتی، ۲۰۰۴: ۱۵۳). به عبارتی، پیشرفت هر روزه صنعت انفورماتیک و توسعه حیرت‌انگیز فناوری اطلاعات ازیکسو و تنوع‌یابی اشکال سوءاستفاده اعم از مالی و غیرمالی از طریق رایانه و اینترنت ازسوی‌دیگر، این موضوع را پیش می‌کشد که جرائم سایبری باید دایره‌ای بس وسیع‌تر از موارد مشابه سنتی داشته باشد تا بتواند برای هر شکل از انواع سوءاستفاده‌های رایانه‌ای با تمسک به قانون، پاسخ کیفری داشته باشد و قاعدتاً جرم سایبری تعریفی گسترده‌تر از تعریف جرم سنتی، می‌طلبد. این نحو از تدوین رکن قانونی نیز به‌مراتب بهتر از موارد سنتی است. چراکه بهتر و راحت‌تر امکان انطباق عمل مجرمانه با عنصر قانونی جرم برای محاکم وجود دارد و به نحو شایسته‌تری تضمین‌کننده حقوق متهم و مانع از تفاسیر مختلف از قانون و وارد کردن عناصر و مصادیق مختلف در حیطه شمول قانون است. ازاین‌رو، در تعریف جرائم سایبر باید کلیت را مدنظر قرار داد و از ارائه تعریفی که با پیدایش مصادیق جدید قابلیت اجرایش را از دست می‌دهد، پرهیز کرد.

در حقوق کیفری سنتی معمولاً قانونگذار جهت تبیین رفتار مجرمانه موردنظر، به شیوه مصداقی اقدام به جرم‌انگاری می‌کند. به این بیان که به‌جای ارائه تعریفی دقیق و جامع از رفتار مجرمانه، آن را با مصادیق قابل فرض در جرم موردنظر تعریف می‌کند؛ در نتیجه در این شیوه همواره بین حقوقدانان اختلاف‌نظر پیش می‌آید که آیا فلان مصداق نیز جزو عنصر قانونی جرم مربوطه است یا خیر، اینکه آیا مصادیق مزبور در ماده احصایی هستند یا تمثیلی و از این قبیل ابهامات که به‌شدت با حقوق شهروندان نیز در تضاد است؛ چراکه همواره نمی‌دانند انجام یک رفتار خاص آیا عنصر قانونی مجرمانه دارد یا خیر؟ به‌طور مثال، قانونگذار در ماده (۵۲۳) قانون تعزیرات به جرم جعل و تزویر پرداخته است که با مداقه در آن ماده درمی‌یابیم قانونگذار تعریفی از جرم جعل ارائه نکرده و صرفاً به شمارش برخی از مصادیق جعل سنتی پرداخته است. همین رویکرد را قانونگذار در قانون تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاهبرداری مصوب ۱۳۶۷ اتخاذ کرده است. در ماده (۱) آن،

قانون به‌جای ارائه تعریفی از جرم کلاهبرداری به ارائه برخی مصادیق آن پرداخته است.

با عنایت به وقوع مشکلات احتمالی مذکور،کنوانسیون جرائم سایبر مصوب ۲۰۰۱، این مهم را مورد توجه قرار داده و با دوری گزیدن از جرم‌انگاری به شیوه مصداقی سعی داشته با عنایت به ویژگی‌های جرائم و فضای سایبر، قوانین مربوطه دچار کهنگی و غیرقابل استناد نشوند؛ لذا در جرائم مختلف سایبری شاهد به‌کارگیری عبارات به شیوه مفهومی در تقنین هستیم؛ به‌طور مثال در ماده (۷) کنوانسیون، فقط افعال چهارگانه «ورود، تغییر، محو و توقف داده‌های رایانه‌ای» را به‌صورت حصری برای تحقق جعل رایانه‌ای آورده است. این چالش‌ها که در نتیجه اوصاف و شرایط خاص جرائم ارتکابی در فضای سایبر به‌وجود می‌آید و در نتیجه ضرورت اتخاذ رویکردی متمایز و ویژه را در حوزه جرم‌انگاری توجیه می‌کند، در قانون جرائم رایانه‌ای مصوب ۱۳۸۸ نیز با اقتباس از کنوانسیون جرائم سایبر مورد توجه قرار گرفته است. قانونگذار در جرائم سایبری از رویه سابق خود در رکن قانونی جرائم مبنی‌بر ذکر نمونه‌هایی از مصادیق عنصر مادی و سپس بار کردن حکم مربوطه به آن فاصله گرفته است و با ذکر عناوین کلی برای عنصر مادی بزه همچون «تغییر یا ایجاد داده‌های قابل استناد» یا «تغییر داده‌ها یا علائم موجود»، سعی در تبیین بزه جعل رایانه‌ای موضوع ماده (۶) قانون مذکور را دارد. هرچند عناوین کلی است اما به‌نوعی عنصر مادی این جرم را صرفاً منحصر در این موارد دانسته است تا هر اقدامی که این عناوین کلی دربرگیرنده آن باشد عنوان بزه جعل رایانه‌ای به آن مترتب شود و خارج از حدود این عناوین نیز مشمول بزه مذکور نخواهد شد؛ و با رشد فناوری و بروز رفتارهای جدید نیز، قانون کارایی خود را از دست نمی‌دهد و قابلیت تطبیق با رفتارهای جدید بزهکارانه را دارد.

۲-۱-۲. استفاده از روش احاله یا ارجاع در جرم‌انگاری

حقوق کیفری امروزه تحت تأثیر سیاست جنایی متحول شده است. تحول عنصر قانونی نیز در همین راستا صورت گرفته است. اصل قانونی بودن در سراسر سده نوزدهم به‌عنوان حربه‌ای مؤثر برای دفاع از حقوق و آزادی‌های شهروندان در مقابل زیاده‌روی قوای مجریه و قضائیه به‌ویژه قضات کیفری محسوب می‌شد، لکن از پایان سده نوزدهم، به دلایل

مختلف تحولاتی در ماهیت این اصل به‌وجود آمده است. با توجه به فنی شدن حقوق جزا و گسترش رسالت حقوق جزا در ۳۰ سال اخیر که از حفظ ارزش‌های سنتی و اخلاقی به سمت حفظ ارزش‌های فنی و تخصصی حرکت کرده، این اصل نیز متحول شده است (نجفی ابرندآبادی، ۱۳۹۰: ۲۵). گسترش جرائم سایبری با توجه به نوع و شیوه ارتکاب آنها باعث فنی شدن حقوق کیفری گردیده است که این مسئله موجب شده تا شیوه احاله یا ارجاع در جرم‌انگاری در راستای به‌کارگیریِ رویکرد افتراقی برای فائق آمدن بر مشکلات لحاظ اصل قانونی بودن جرائم در معنای سنتیِ آن اِعمال شود یعنی هر جرمی به‌طور صریح در همان قانون کیفری بایستی مشخص باشد. به‌این‌ترتیب قانونگذار در قلمرو جرائم سایبری، به ارجاع به متن دیگری غیر از متن کیفری و خارج از مجموعه قوانین کیفری اکتفا می‌کند که نقض آن ارزش، از نظر کیفری دارای ضمانت اجرا خواهد بود. اتفاق مهمی که درخصوص جرائم سایبری افتاده این است که با عنایت به فنی بودن این جرائم، تفصیل این دسته جرائم از حوصله و تخصص قانونگذار خارج است. ازاین‌رو است که قانونگذار با آنکه اقدام به جرم‌انگاری می‌کند اما مصادیق آن را خودش تعریف نکرده و برعهده گروه یا یک وزارتخانه می‌گذارد؛ مثل کارگروه تعیین مصادیق محتوای مجرمانه[1] که زیر نظر دادستان کل کشور اقدام می‌کند. این گروه قانونگذار نیست و تشریفات ابلاغ قانون هم در مورد تصمیماتش صورت نمی‌گیرد.[2] ازاین‌رو، شاهد آنیم که اصل قانونی بودن متحول شده است به‌خصوص در مورد جرائم سایبری که واجد جنبه فنی هستند؛ زیرا این دست از جرائم مدام در حال تغییرند و قانونگذار تخصص لازم در مورد آنها ندارد. ازاین‌رو، تصمیم‌گیری درخصوص مصادیق مجرمانه را برعهده گروهی متخصص قرار می‌دهد و به‌نوعی این گروه اقدام به جرم‌انگاری تکمیلی می‌کند. به این بیان که این دسته از جرائم همواره با پیشرفت فناوری اطلاعات گونه‌های جدیدی به‌خود می‌گیرد و

---

۱. ماده (۲۲) قانون جرایم رایانه‌ای مصوب ۱۳۸۸.

۲. اصل قانونی بودن در حال تبدیل شدن به اصل آیین‌نامه‌ای بودن حرکت کرده است. قانون شکار و صید نیز مملو از ارجاع به آیین‌نامه است یا قانون اسلحه و مهمات که مصادیق اسلحه و مهمات را به عهده وزارت دفاع قرار داده است. بعد از جریانات ۱۳۸۸ وزارت دفاع آیین‌نامه جدیدی صادر کرد.

قانونگذار جهت عقب نماندن از این تحولاتِ سریع، سعی در مبارزه به روز با این تحولات را دارد. لذا به‌ناچار با سپردن تعیین مصادیق مجرمانه به کارگروه مذکور از یکسو خواسته تا از پروسه طولانی تصویب قانون جلوگیری کند و ازسوی‌دیگر به لحاظ فنی بودن جرائم سایبری، به ناچار نیاز به یک شناخت فنی وجود دارد؛ و این شناخت را برعهده یک کمیته فنی قرار داده است.

۳-۱-۲. کاستن از شرایط تحقق جرم

با توجه به سهولت ارتکاب جرم، فراوانی بزه‌دیدگان و خسارات گسترده احتمالی‌ای که جرم سایبری می‌تواند از خود به‌جا بگذارد، یکی از وجوه اتخاذ رویکرد افتراقی و البته سختگیرانه در قلمرو جرائم سایبری، کاهش رکن‌های تشکیل‌دهنده جرم است؛ زیرا هرچه شرایط تحقق جرم بیشتر باشد به همان نسبت دایره جرم کوچک‌تر و اثبات آن مشکل‌تر خواهد بود؛ این امر مقابله با اقدامات خطرناک و مجرمان جرائم سایبری را با محدودیت‌های بیشتری مواجه خواهد کرد (Dubber, 2001: 14). به‌طور مثال جرم کلاهبرداری سنتی، جرمی مرکب و مقید است. عناصر متعددی مانند استفاده از وسایل متقلبانه، فریب دیگری و بردن مال او برای تحقق جرم لازم است. در چنین جرمی از طرفی عناصر مادی متعددی باید به اثبات برسند و از طرف دیگر علم و اطلاع، سوءنیت عام و سوءنیت خاص مرتکب درخصوص عناصر مادی مذکور باید ثابت شود. عدم اثبات یا تردید در تحقق هریک از اجزای رکن مادی یا معنوی جرم مذکور، مانعی برای اثبات جرم بوده و به تعبیری مَفری برای گریز مرتکب از مجازات خواهد بود. ازاین‌رو، با وجود اصراری که قانونگذار در شدت بخشیدن به مبارزه با جرم کلاهبرداری در قانون تشدید مجازات مرتکبان ارتشاء، اختلاس و کلاهبرداری مصوب ۱۳۶۷ دارد، کثرت عناصر مذکور مانعی جدی برای مقابله با جرم کلاهبرداری محسوب می‌شود.

ماده (۱۳) قانون جرائم رایانه‌ای (ماده (۷۴۱) قانون مجازات اسلامی) به جرم کلاهبرداری رایانه‌ای اختصاص‌یافته است. مقایسه این جرم با کلاهبرداری سنتی بیانگر آن است که عناصر تشکیل‌دهنده جرم در اولی در مقایسه با همتای سنتی خود به‌صورت قابل

ملاحظه‌ای کاهش یافته است. به‌طور مثال در ماده مذکور، اثری از توسل به وسایل متقلبانه و فریب برای تحقق جرم کلاهبرداری رایانه‌ای دیده نمی‌شود. طبیعی است که در بعد عنصر روانی نیز اجزای جرم به همین نسبت کاهش می‌یابد. از طرف دیگر، نتیجه لازم برای تحقق جرم کلاهبرداری سنتی یک مصداق بیشتر ندارد و آن‌هم بردن مال دیگری است. درحالی‌که مصادیق نتیجه‌ای جرم کلاهبرداری سایبری توسعه قابل ملاحظه‌ای داشته است. این نتایج شامل مال، منفعت، خدمات یا امتیازات مالی برای خود و دیگران می‌شود؛ یعنی ازیکسو، عناصر تشکیل‌دهنده جرم کلاهبرداری سایبری کاهش یافته و ازسوی‌دیگر قانونگذار از محدود کردن نتیجه به بردن مال دیگری احتراز کرده و با توسعه مصادیق نتیجه، عملاً آن را به کسب هرگونه امتیاز، منفعت و خدمت گسترش داده است. چنین تحولی در سایه سیاست کیفری افتراقی و البته سختگیرانه قابل توجیه است؛ زیرا می‌تواند عملاً رفتارهای گسترده‌تر و مرتکبان بیشتری را شامل شود؛ لذا بزهکاران نمی‌توانند در سایه ضعفی که در حوزه سنتی جرم مذکور وجود داشت در محیط سایبر از عدالت کیفری فرار کرده و به کیفر نرسند.

۲-۲. راهبردهای ویژه در حیطه رکن مادی

دومین رکن از ارکان تشکیل‌دهنده هر جرمی، رکن مادی جرم است. رکن مادی در جرائم سایبری از حیث زمان و مکان ارتکاب نیز قابل‌توجه است. در جرائم سنتی، زمان ارتکاب جرم شامل قصد مجرمانه تهیه مقدمات شروع به جرم و تحقق نتیجه جرم یا عقیم ماندن جرم مطرح است؛ اما در جرائم سایبری در اکثر موارد پس از قصد مرتکب و تهیه مقدمات (کامپیوتر و اجزای آن برنامه‌ریزی یک عملیات تخریبی رایانه‌ای) شروع و عملیات اجرایی در کسری از ثانیه به‌وقوع می‌پیوندد. ازاین‌رو، جهت پیشگیری از نتایج زیانبار جرائم سایبری سیاست کیفری با سختگیری بیشتری نسبت به جرائم سنتی، سعی بر توسعه جرائم مطلق، پذیرش اعمال مقدماتی به‌عنوان جرم تام و وضع جرائم مانع، دارد. با عنایت به قانونگذاری‌های اخیر در عرصه داخلی و بین‌المللی در راستای مبارزه با جرائم سایبری به جهت شدت و اهمیت این جرائم، از این اصول کلی در قلمرو جرائم سنتی، در موارد متعددی عدول شده است که ذیلاً به بررسی آنها پرداخته می‌شود.

۱-۲-۲. جرم‌انگاری رفتارهای تمهیداتی به‌عنوان جرم مستقل

در حقوق کیفری سنتی، فرایند وقوع بزه از تصور عمل بزهکارانه و میل به انجام عمل آغاز و به تهیه وسایل، انجام اعمال مقدماتی، شروع به جرم و انجام عمل مجرمانه ختم می‌شود. در مرحله تهیه مقدمات، شخص از مرحله قصد و تصمیم به ارتکاب جرم خارج شده و برای نزدیک شدن به مقصود ارتکاب جرم، مقدمات کار را فراهم می‌کند. این اقدامات بنا به اصل قابل مجازات نیستند، زیرا تهیه مقدمات همیشه کاشف از نیت مجرمانه عامل نبوده و اغلب ممکن است عملیات مزبور به طور کامل مشروع و مجاز باشد. در نظام‌های کیفری به‌صورت بنیادین، اعمال مقدماتی جرم محسوب نمی‌شود.[۱] در نظام کیفری ایران حتی شروع به جرم هم علی‌الاصول جرم تلقی نمی‌شد.[۲] در شرایط استثنایی، به علت اهمیت جرم و آثار گسترده جرمِ خاص ممکن بود سیاست کیفری بر این قرار گیرد که شروع به جرم را جرم تلقی کند یا در شرایط حادتری اعمال مقدماتی را به‌عنوان شروع به جرم یا جرم تام تلقی کند.[۳] اما در مقابل، در جرائم سایبر به علت آثار زیانبار و گسترده آن، پیچیدگی و صعوبت کشف جرم، شناسایی مجرم و اثبات جرم، سیاستگذار کیفری موضع سخت‌گیرانه‌ای اتخاذ کرده و خواسته است جلو ارتکاب جرم را در منشأ بگیرد. به همین دلیل در راستای اعمال این رویکرد افتراقی، مقدمات بعیده جرم را نه فقط به‌عنوان شروع به جرم بلکه به‌عنوان جرم مستقل تعریف کرده است که ازجمله آن می‌توان به جرم «دسترسی غیرمجاز» اشاره کرد. در حقوق کیفری سنتی، دسترسی غیرمجاز با هیچ‌یک از بزه‌ها همسان نیست و ازاین‌رو، در زمره جرائمی است که با پیدایش رایانه نمود یافته و به‌عنوان برجسته‌ترین بزه رایانه‌ای ناب شناخته می‌شود که درآمد و بلکه مادر بیشتر جرائم رایانه‌ای[۴]

---

۱. ماده (۱۲۳) قانون مجازات اسلامی مصوب ۱۳۹۲.

۲. ماده (۴۱) قانون مجازات اسلامی مصوب ۱۳۷۰. همچنین رجوع کنید به: رأی وحدت رویه هیئت عمومی دیوانعالی کشور شماره ۶۳۵ سال ۱۳۷۶.

۳. هرچند قانونگذار در قانون مجازات اسلامی مصوب ۱۳۹۲ در ماده (۱۲۲) شروع به جرم را جرم‌انگاری کرد.

۴. طبق ماده (۱) قانون جرائم رایانه‌ای (ماده (۷۲۹) قانون مجازات اسلامی ـ بخش تعزیرات)، «هرکس به‌طور غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی که به‌وسیله تدابیر امنیتی حفاظت شده است دسترسی یابد، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون ریال تا بیست میلیون ریال یا هر دو محکوم خواهد شد».

است. در سنجش با بزه‌هایی مانند کلاهبرداری رایانه‌ای، اخلال در سیستم و تروریسم سایبری، دسترسی غیرمجاز به‌عنوان رفتاری مقدماتی به‌شمار می‌آید که هنوز با نتیجه که دربردارنده زیان دیگری است، فاصله دارد و از ریشه به‌دلیل چهره درآمدی و مقدماتی این بزه است که آن را دروازه جرائم رایانه‌ای می‌دانند. ازاین‌رو، قانونگذار خواسته با جرم‌انگاری اعمال مقدماتی جرائم رایانه‌ای از وقوع جرائم خطرناک و شدید بعدی پیشگیری و ابتدایی‌ترین رفتارهایی که به آثار مخرب گسترده منجر می‌شود را سرکوب کند.

یکی از جرائم رایانه‌ای ناشناخته و پرخطر امروزی را می‌توان سرقت هویت یاد کرد. جرم مذکور به‌عنوان یکی از اعمال مقدم و منشأ برای ارتکاب جرائم سایبری دیگر لحاظ می‌شود. در این شکل از جرائم سایبری، مجرم یک کپی تقریباً صددرصد شبیه یک وب‌سایت بنگاه تجاری، بانک یا شبکه‌های اجتماعی را ایجاد و سپس تلاش می‌کند تا کاربران را جهت افشاء جزئیات شخصی‌شان (نام کاربری، کلمه عبور و ...) از طریق یک فرم در سایتی جعلی فریب دهد که این عمل به مجرم اجازه می‌دهد با استفاده از این اطلاعات مقادیر بسیاری وجه به‌دست آورد. درواقع سرقت هویت عبارت است از معرفی کردن خود به‌جای دیگری با استفاده متقلبانه از اطلاعات شخصی دیگری (وایلدینگ، ۱۳۷۹: ۲۱). نکته قابل توجه این است که جعل هویت معمولاً هدف نهایی مرتکب نبوده و مقدمه‌ای برای ارتکاب جرائم دیگر نظیر کلاهبرداری، افشای داده‌ها، سرقت و ... است. در برخی نظام‌های حقوقی سرقت هویت جرم‌انگاری شده است. به‌عنوان مثال، در ایالات متحده آمریکا قانون فدرال سرقت مصوب ۱۹۹۸ عمل شخصی را که عالماً و بدون مجوز قانونی اقدام به انتقال یا استفاده از ابزارهای تشخیص هویت دیگری کند و قصد ارتکاب یا مشارکت یا معاونت در انجام یک عمل غیرقانونی داشته باشد که به نقض قوانین فدرال منجر می‌شود یا آنکه عمل مزبور به‌موجب قانون ایالتی یا محلی حاکم بر قضیه یک جنایت محسوب شود، جرم تلقی می‌کند (www.ftc.gov.bcp/conline/pubs/creditlidtheft/ htm=law). در حقوق کیفری ایران متأسفانه نص قانونی وجود ندارد که صریحاً سرقت هویت را به‌عنوان جرم مستقل تلقی کرده باشد. نکته‌ای که در اینجا ممکن است به ذهن خطور کند اینکه آیا سرقت هویت را می‌توان کلاهبرداری رایانه‌ای تلقی کرد؛ با نگاهی به

ماده (۱۳) قانون جرائم رایانه‌ای درخصوص کلاهبرداری رایانه‌ای ملاحظه می‌شود که اعمالی که جزء عنصر مادی تشکیل‌دهنده کلاهبرداری رایانه‌ای است عبارت است از وارد کردن، تغییر، محو، ایجاد یا متوقف کردن داده‌ها یا مختل کردن سیستم. درحالی‌که در سرقت هویت لزومی به وقوع رفتارهای فوق ندارد. همچنین سرقت هویت مقدم بر همه اینهاست و جزو اعمال مقدماتی برای کلاهبرداری و یا سایر جرائم سایبری می‌تواند تلقی شود. در نتیجه با توجه به اینکه سرقت هویت می‌تواند منشأ و موجد جرائم مختلفی شود، جرم‌انگاری آن در محیط مجازی از ضروریات این حوزه محسوب می‌شود. چراکه در قانون مذکور جای این جرم خالی است و همین فقدان عنوان مجرمانه و عدم لحاظ مجازات متناسب برای آن، وقوع و ارتکاب آن را افزایش می‌دهد.

۲-۲-۲. وضع جرائم مطلق

در این مرحله بزهکار وارد جریان اجرایی جرم شده و مرتکبِ عمل مجرمانه می‌شود. ارتکاب جرم وقتی تمام است که بزهکار تمامیِ شرایطی را که قانون برای تحقق و ارتکاب آن لازم دانسته انجام داده باشد. ازاین‌حیث، جرائم برمبنای عنصر مادی به دو گروه جرائم مقید[1] و مطلق یا رفتاری[2] تقسیم می‌شوند. جرم از این نظر مطلق نامیده می‌شود که وصف مجرمانه صرفاً به‌صورت یا ظاهر فعل تعلق گرفته و در توصیف مجازات اخذ نتیجه زیانبار منظور نشده است. برای مثال، به‌موجب قسمت اول ماده (۵۱۸) قانون مجازات اسلامی بخش تعزیرات، ساختن شبیه سکه‌های طلا یا نقره قابل مجازات است و لازم نیست سازنده سکه‌های قلب در عمل آنها را به مصرف رسانده یا از آنها سود برده باشد. یا وقتی قانونگذار مطلق افشای سؤالات امتحانی را جرم تلقی می‌کند (ماده واحده قانون افشای سؤالات امتحانی مصوب ۱۳۱۷)، به شیوه و طریق فعل نظر داشته و هیچ‌گاه نتیجه‌ای را که از این فعل حاصل می‌شود در توصیف مجرمانه ملحوظ نکرده است. ولی اگر چنانچه قانونگذار حصول نتیجه‌ای را جزو عناصر تشکیل‌دهنده جرم منظور کرده باشد مانند، قتل یا

1. Result Crime
2. Conduct Crime

سرقت، مادامی‌که به حیات کسی خاتمه داده نشده یا مال کسی از تملک او خارج نگردیده است جرم تحقق نمی‌یابد؛ لذا تحقق نتیجه جزء لاینفک جرم موردنظر بوده و بدون وجود نتیجه جرم محقق نمی‌شود؛ این قبیل جرائم، به جرائم مقید موسوم‌اند.

ازجمله دلایل ضرورت تعریف جرم به‌صورت مطلق در قلمرو جرائم سایبری، گزینش رویکرد عدم تسامح در مقابل جرائمی است که از حساسیت بیشتری برخوردار بوده و پیامدهای سوءِ گسترده‌تری دارند؛ جرائمی که در صورت تحقق نتایج مجرمانه آن می‌تواند امنیت ملی را متزلزل کند و گستره وسعت آثار زیانبار آن به‌شدت وسیع است. لذا قانونگذار درصدد است تا با جرم‌انگاری صرف ارتکاب رفتار ممنوعه صرف‌نظر از پدید آمدن هرگونه نتیجه‌ای خاص از رفتار موردنظر، خیلی زودتر به مقابله با رفتار خطرناک برآید و جلوی نتایج سوء و گسترده احتمالیِ بعدی را بگیرد. در قانون جرائم رایانه‌ای در راستای اتخاذ رویکردی افتراقی، گرایش آشکاری به تعریف جرائم به‌صورت مطلق نشان داده است. نمونه‌هایی از چنین رویکردی در مواد (۱) قانون مذکور با عنوان دسترسی غیرمجاز به داده‌های سیستم‌های رایانه‌ای، شنود غیرمجاز (ماده (۲))، نقض تدابیر امنیتی (ماده (۴)) و جعل رایانه‌ای (ماده (۶))، قابل مشاهده است. در موارد مذکور صرف دسترسی یا شنود غیرمجاز و یا نقض تدابیر امنیتی داده‌ها، فارغ از نتیجه احتمالی، استفاده مرتکب با ضررهای احتمالی، جرم تلقی شده است. حتی در مواردی قانونگذار به‌واسطه سهولت ارتکاب و افزایش میزان شیوع یک جرم سنتی در فضای سایبر، جرمی را که در حالت سنتی آن در زمره جرائم مقید بوده، در صورت ارتکاب در فضای سایبر، آن را در زمره جرائم مطلق قلمداد کرده است. به‌طور مثال جرم سرقت در محیط فیزیکی در زمره جرائم مقید است و تا زمانی که مال از حرز خارج نشود، مصداق ربایش پیدا نمی‌کند؛ اما قانونگذار با اتخاذ رویکرد افتراقی در فضای سایبر، ارتکاب جرم سرقت را از مقید بودن به مطلق شدن، تغییر داده است. وفق ماده (۱۲) قانون جرائم رایانه‌ای، درصورتی‌که مرتکب صرفاً از داده‌های متعلق به دیگری کپی‌برداری کند درحالی‌که عین داده‌ها در اختیار صاحب آن باشد، جرم سرقت رایانه‌ای محقق است و نیازی به کسب نتیجه موردنظر در سرقت سنتی یعنی خروج مال از حرز، نیست. البته بهتر بود قانونگذار در تبصره‌ای به ماده

مذکور، سرقت داده‌های دولتی (یا حاکمیتی) یا سرقت داده‌های سامانه‌هایی که برای ارائه خدمات ضروری عمومی به‌کار می‌روند یا سرقت‌هایی که قصد به خطر انداختن امنیت و آسایش عمومی را دارند، به‌عنوان عامل تشدید مجازات معرفی می‌کرد تا جنبه بازدارندگی کیفری ماده (۱۲) نیز افزون شود.

ازجمله رفتارهایی که می‌توان با جرم‌انگاری آن به‌صورت مطلق، جلوی پیامدهای سوء بعدی ناشی از ارتکاب جرائم سایبری را گرفت، جرم‌انگاری دور زدن فیلترینگ است که فقدان آن در قانون جرائم رایانه‌ای احساس می‌شود. به این بیان که، یک عمل خلاف رایانه‌ای به‌طور لزوم وارد کردن خسارت به یک تجهیز یا سیستم نیست بلکه گاه فقط دسترسی به بعضی اطلاعات حساس یا محرمانه می‌تواند جرم باشد؛ به‌تازگی نیز جرم‌انگاری استفاده از نرم‌افزارهایی به نام فیلترشکن (وی. پی. ان.) که باعث دور زدن سیستم فیلترینگ و دسترسی به محتوای تمام سایت‌های غیرمجاز می‌شود، مورد توجه قرار گرفته و در انتظار تصویب است. برای جلوگیری از ورود کاربران به محتوای مجرمانه در فضای مجازی به‌واسطه آثار سوئی که محتوای مجرمانه بر جامعه تحمیل می‌کند، از فیلترینگ استفاده می‌شود؛ اما در مقابل این اقدام، خدمات دسترسی ارتباطی مجازی یا «وی.پی.ان» فیلترینگ را دور می‌زند؛ به همین دلیل اخیراً طرحی در مجلس شورای اسلامی تحت بررسی است که به مبارزه با استفاده و فروش این ابزار بدون مجوز قانونی می‌پردازد. این مقررات تحت عنوان «الحاق یک بند به ماده (۲۵) قانون جرائم رایانه‌ای» تدوین شده است (http://rc.majlis.ir/fa/legal_draft/show/844651). در این طرح، تکثیر، فروش و استفاده از این خدمات یا دسترسی به‌طور غیرمجاز به سایت‌های اینترنتی فیلتر شده، ممنوع اعلام و برای انجام چنین اقدام‌هایی، حبس و جزای نقدی در نظر گرفته شده است.

۳-۲-۲. وضع جرائم مانع

هر یک از دو مفهوم جرم و انحراف، راه‌های مقابله خاصی دارد. مقابله با جرم غالب با توسل به ضمانت اجراهای کیفری انجام می‌گیرد که در قوانین پیش‌بینی می‌شود، درحالی‌که روش‌های مقابله با انحراف بنا به طبیعت رفتار منحرف، اصولاً خارج از چارچوب ضمانت

اجراهای کیفری است (نجفی ابرندآبادی و همکاران، ۱۳۸۳: ۲۴). ورود ضمانت اجراهای کیفری به قلمرو انحرافات با هدف جلوگیری از ارتکاب جرائم دیگر را باید در نظریات و اندیشه‌های مجازات‌گر ژرمی بنتام از اندیشمندان مکتب کلاسیک حقوق کیفری، جستجو کرد. بنتام به‌منظور از بین بردن زمینه‌های وقوع جرائم و تعدیل گرایش‌های خطرناک، توصیه‌هایی را به‌عنوان اقدامات مکمل کیفر مطرح می‌کرد. به‌نظر وی، اهمیت جرائم صرفاً با توجه به درجه فساد و تباهی که بر آنها مترتب است، ارزیابی نمی‌شود، بلکه با توجه به خطرهایی که به دنبال خواهند داشت، مورد سنجش قرار می‌گیرد (پرادل، ۱۳۸۱: ۶۶). به‌این‌ترتیب، بنتام عقیده به جرم دانستن انحرافاتی داشت که زمینه‌ساز جرائم محسوب می‌شوند تا به این وسیله هزینه‌های ارتکاب جرم افزایش‌یافته، معادله جرم به‌سوی عدم ارتکاب آن سوق داده شود.

در حوزه فضای سایبر رفتارهایی وجود دارد که در نگاه اول منحرفانه و فاقد وصف کیفری است اما به لحاظ زمینه‌سازی برای ارتکاب جرائم خطرناک‌تر بعدی، مقابله کیفری با آنها مورد پذیرش قرار گرفته است. این رویکرد از آن جهت افتراقی است که در حقوق کیفری سنتی اساساً رفتارهای منحرفانه، پاسخ‌دهی کیفری نمی‌شوند. ازجمله جرائم ارتکابی در فضای سایبر که می‌توان از منظر جرائم بازدارنده به آن توجه کرد، جرم «دسترسی غیرمجاز» است. هرچند دسترسی غیرمجاز، یکی از رفتارهای ناقض محرمانگی است و به‌دلیل شکستن حریم داده‌ها و اطلاعات دیگری، رفتاری غیراخلاقی است. بااین‌حال چهره اخلاقی دسترسی غیرمجاز چندان پررنگ نیست و اگر کسی از رایانه دیگری که گذرواژه نداشته، بهره ببرد و به داده‌ها و محتواها سر بکشد یا اینکه در حضور دارنده سامانه، به‌طور ناگهانی یا پنهانی به داده‌ها نگاه کند، بزهی انجام نداده است، هرچند رفتارش غیراخلاقی و منحرفانه است. بنابراین، به نظر می‌رسد چهره بازدارندگی دسترسی غیرمجاز بر چهره غیراخلاقی‌اش بچربد و از این منظر باید گفت دسترسی غیرمجاز در زمره بزه‌های بازدارنده یا مانع است.

بنابراین، ازآنجاکه جرائم سایبری در برخی موارد در زمره جرائم خطرناک و دارای خسارات گسترده، محسوب می‌شوند؛ ازاین‌رو، قانونگذار با اتخاذ رویکرد افتراقی خواسته تا با جرم‌انگاری مقدماتی‌ترین رفتارهای زمینه‌ساز ارتکاب جرائم خطرناک که فی‌الواقع در زمره

رفتارهای منحرفانه تلقی می‌شوند، از وقوع جرائم بزرگ‌تر و اصلی پیشگیری کند؛ امری که در جرائم سنتی با آن اصولاً مواجه نیستیم و اعمال انحرافی اصولاً فاقد وصف کیفری هستند.

۳-۲. راهبردهای ویژه در حیطه رکن روانی

در جرائم سنتی اصل بر عمدی بودن است و در جرائم عمدی نیز دو مقوله علم و قصد اجزاء رکن معنوی را تشکیل می‌دهند؛ ارتکاب عمل هم به خودی خود، دلیل وجود عنصر معنوی یا روانی نیست و در مواردی با وجود اینکه عملی صورت می‌گیرد، قانون مرتکب آن را به‌دلیل فقدان قصد مجرمانه یا فقدان مسئولیت جزایی قابل مجازات نمی‌داند. در جرائم سایبری به لحاظ ماهیت و اوصاف خاص این جرائم، رکن روانی لازم برای تحقق جرم برخلاف جرائم سنتی، همواره از گزاره لزوم عمدی و عالمانه بودن رفتار پیروی نمی‌کند؛ لذا با گسترش دامنه جرائم غیرعمدی و نیز پذیرش سوءنیت احتمالی در قلمرو جرائم سایبری مواجه‌ایم و ازسوی‌دیگر، در جرائم سنتی اصولاً جرائم سه عنصری هستند اما در جرائم سایبری با دو عنصری شدن جرائم یا به عبارتی با گسترش جرائم مادی صرف، روبرو می‌شویم که در ادامه به بررسی این تحولات در حوزه عنصر روانی می‌پردازیم.

۱-۳-۲. توسعه جرائم مادی صرف

در ارتکاب جرائم سنتی اصل بر عمدی بودن عمل مجرمانه است مگر اینکه مرتکب، بنا به دلایل و قرائن قابل قبول بتواند اثبات کند که در انجام رفتار ارتکابی سوءنیت مجرمانه نداشته است. این اصل در جرائم سایبری بنا به دلایلی دچار تحول شده و قانونگذاران در ارتکاب جرائم سایبری سعی در دو عنصری کردن جرم و حذف رکن روانی دارند که در جرائم سنتی از ارکان اصلی متشکله جرم تلقی می‌شود. مفروض بودن عنصر معنوی در ارتکاب مصادیقی از جرم سایبری به معنی مادی صرف بودن آن جرائم است و لذا به این جرائم عنوان «جرائم سایبری با مسئولیت مطلق» اطلاق می‌شود. ازجمله دلایلی که می‌توان جهت اتخاذ رویکرد افتراقی به سود پیش‌بینی جرائم با مسئولیت مطلق ارائه کرد این است که با بالا بردن سطح مراقبت، از جامعه در مقابل اعمال خطرناک حفاظت می‌کند

(Elliot and Quinn, 2000: 32). این ادعا به‌ویژه در مورد جرائم سایبری قابل توجیه و دفاع است. چراکه این جرائم لطمات و خسارات جبران‌ناپذیری در ابعاد گوناگونِ سیاسی، اجتماعی، اقتصادی و فرهنگی به جامعه وارد می‌کنند و فرض بر این است که مرتکبان این جرائم که به طور غالب صاحبان شرکت‌ها، یقه‌سفیدها و حِرف مختلف هستند، افرادی حرفه‌ای و متخصص بوده و نسبت به آثار اعمالی که در اثر تقصیر یا عدم تقصیر خود مرتکب می‌شوند، آگاهی دارند.

به‌بیان‌دیگر، حرفه‌ای و متخصص بودن صاحبان مشاغل با آگاه بودن آنها از آثار اعمالشان ملازمه دارد (نجفی ابرندآبادی، ۱۳۸۴: ۲۲۸۰). سازمان ملل متحد در اسناد مصوب خود در ارتکاب جرائم اقتصادی که یکی از مصادیق و حتی مهم‌ترین آن، ارتکاب از طریق فضای سایبر است، نه‌تنها احراز سوءنیت یا عنصر معنوی را در ارتکاب ضروری ندانسته و وجود آن را مفروض تلقی کرده است. این امر از ماده (۲۸) کنوانسیون مریدا که مقرر می‌دارد: «آگاهی، قصد یا نیت لازم به‌عنوان عنصر جرم احراز شده براساس کنوانسیون ممکن است از وضعیت واقعی عینی استنتاج شود»، قابل استنباط است. برعکس موارد مذکور، مقنن ایرانی وجود عنصر معنوی را از ارکان ضروری غالب جرائم به استثنای صدور چک پرداخت نشدنی، جرائم خلافی ازجمله پارک اتومبیل در جای توقف ممنوع یا عبور از چراغ قرمز دانسته است. درحالی‌که به‌نظر می‌رسد با توجه به خسارات سنگین و غیرقابل جبران، پیچیدگی، فنی و تکنیکی بودن جرائم سایبری که ملازمه با آگاهی و علم مرتکبان به آثار و تبعات فعل و ترک فعل‌های خود دارد، حداقل می‌توان عنصر معنوی را در مورد تعدادی از جرائم سایبری مانند جرائم سرویس‌دهندگان خدمات اینترنتی مفروض دانست. این امر علاوه بر پیشگیری از ارتکاب جرائم مورد بحث، زمینه را برای مبارزه هرچه کارآمدتر و در نتیجه صیانت از جامعه را در ابعاد گوناگون فراهم می‌کند.

۲-۳-۲. توسعه جرائم غیرعمدی

همان‌طور که ذکر شد، اصل بر عمدی بودن جرائم است و این امر نیاز به تصریح ندارد که در هر یک از موارد قانون جزایی، قانونگذار بیان از این موضوع داشته باشد که اگر

مرتکب با علم و عمد، همراه با آگاهی، به عمد، با سوءنیت، همراه با علم جرم را مرتکب شود. بلکه درصورتی که عنوان غیرعمدی را جرم‌انگاری کند باید به این امر تصریح داشته باشد. در جرم غیرعمدی، مرتکب به آن میزانی که لازم بوده است، فکر نکرده است و همین بی‌توجهی به سطح متوسط فکر جامعه، موجب شده است عمل واقع شود و این امر در قالب بی‌احتیاطی، غفلت، عدم مهارت و عدم رعایت نظامات دولتی و سایر مصادیق، نمود یافته است. ولی آیا حقوق کیفری می‌تواند اعمالی را که در حالت عمدی آن جرم‌انگاری شده است، در حالت غیرعمدی جرم‌انگاری کند؟ و آیا حقوق کیفری می‌تواند حالتی را که فقط صورت غیرعمدی آن مورد توجه باشد، بدون اینکه وضعیت عمدی آن جرم‌انگاری شده باشد را در چارچوب ابزار کیفری قرار دهد؟

جدای از سطح ضرر و شدید بودن آن و نیز توجه به معیارهای دیگر، یکی از تفاوت‌های ضمانت اجرای کیفری با دیگر ضمانت اجراها، توجه به تفاوت در وجود عنصر تقصیر کیفری است. مرتکب در عنوان کیفری، علاوه بر رابطه علیت مادی، از نظر روانی نیز به‌گونه‌ای تصمیم‌گیری کرده است که جامعه او را سزاوار سرزنش کیفری و برخوردی جزایی می‌بیند و علاوه بر جبران خسارت، لازم و ضروری می‌داند که او به‌دلیل نوع تصمیم‌گیری‌ای که کرده است نیز، مجازات شود. در همین راستا می‌توان گفت در بیشتر قوانین جزایی، در اغلب موارد غیر از جرائم علیه تمامیت جسمانی، حالت غیرعمدی آن در حوزه دخالت کیفری قرار نمی‌گیرد؛ سرقت بدون سوءنیت سرقت نیست و به همین دلیل است که علاوه‌بر علم به حکم، علم به موضوع و علم به حکم غیرکیفری که پایه حکم کیفری است، ضروری شمرده می‌شود؛ و در کنار این علم، وجود سوءنیت عام در همه جرائم و وجود سوءنیت خاص در جرائم مقید، ضروری خواهد بود.[1] باید یادآور شد که هر نوع جرم‌انگاری در حوزه جرائم غیرعمدی، حقوق کیفری و مرزهای حقوق مدنی و غیر آن را نادیده می‌گیرد؛ زیرا اگر بخواهیم حالت‌های غیرعمدی بسیاری از جرائم کیفری را جرم‌انگاری کنیم، به جرئت می‌توان گفت، بیشتر رفتارهای انسانی را با دشواری و عدم تسامح و رواداری همراه خواهد کرد.

---

۱. می‌توان گفت تنها جرم غیرعمدی که قصد فعل (سوءنیت عام) در آن شرط است، قتل شبه عمدی است که فرد قصد فعل دارد و قصد نتیجه ندارد.

در قلمرو جرائم سنتی در قانون مجازات اسلامی نیز، جرائم غیرعمد اغلب در مورد اعمال علیه تمامیت جسمانی فرد، پذیرفته شده است و علاوه بر دیه، مجازات حبس برای آن پیش‌بینی گردیده است و تفاوت میزان حبس در این موارد با مجازات اصلی جرائم عمدی مذکور، خود بیانگر میزان تفاوتی است که در واکنش‌های جامعه وجود دارد (فلاحی، ۱۳۹۲: ۳۳۴). ولی در بزه‌های سایبری با مواردی مواجه می‌شویم که قانونگذار نسبت به برخی رفتارهای غیرعمدی که تعرضی به تمامیت جسمانی افراد جامعه تلقی نمی‌شود، اقدام به جرم‌انگاری کرده است. به‌نظر می‌رسد مبنای اتخاذ رویکرد افتراقی در جرم‌انگاری جرائم غیرعمدی در این حوزه، به این جهت است که آن اعمال علاوه بر ضرر و خسارات گسترده، خطر غیرمعقولی را برای سایر اشخاص ایجاد می‌کنند. در کنوانسیون جرائم سایبر درخصوص فیلترینگ و استفاده از آن بسیار محافظه‌کارانه برخورد کرده است تا بتواند حتی رضایت کشورهای معتقد به آزادی مطلق بیان را نیز جلب کند، لیکن قانونگذار ایران با توجه به قوانین و اعتقادات اسلامی و لزوم حفظ شهروندان در برابر محتویات منحرف‌کننده، و همچنین حفظ حریم خصوصی و جلوگیری از نشر محتویات مجرمانه، صراحتاً بحث پالایش را در قانون جرائم رایانه‌ای گنجانده است و فرایند مربوطه به جرم‌انگاریِ خودداری ارائه‌کنندگان خدمات از دستور پالایش صادره از مراجع قانونی را در مواد (۲۱) و (۲۳) از قانون مزبور، وارد کرده است. این مواد از این جهت در راستای اتخاذ سیاست کیفری افتراقی سختگیرانه حرکت می‌کنند که اولاً، عنصر مادی جرم، خودداری از فیلتر کردن است که به‌صورت ترک فعل انجام می‌شود و ثانیاً، این رفتار به‌صورت غیرعمد نیز جرم تلقی شده و مرتکب مستوجب مجازات است؛ یعنی قانونگذار برخلاف شیوه مرسوم در جرائم سنتی، به جهت شدت و اهمیت خاص جرائم سایبری، تقصیر جزایی را کافی برای تحقق رکن روانی این قبیل از جرائم قرار داده تا از این مسیر احتمال وقوع جرائم سایبری را حتی‌الامکان کاهش داده و بتواند با اتخاذ این سیاست کیفری سختگیرانه از احتمال وقوع جرائم سایبری به لحاظ آثار زیانباری که همراه با این نوع جرائم است، جلوگیری کند.

۳-۳-۲. توسعه جرائم عمدی برمبنای سوءنیت احتمالی

هرگاه شخصی با هدف معین و به‌منظور حصول نتیجه قطعی مرتکب جرم شود و به همان نتیجه هم برسد، این اراده مجرمانه را سوءنیت منجز یا سوءنیت جازم گویند. در مقابل این اراده مجرمانه منجز، سوءنیت احتمالی قرار دارد و آن وضعیتی است که مباشر، قصد ارتکاب جرم را دارد و نتیجه عمل خویش را پیش‌بینی می‌کند، ولی به‌هیچ‌وجه خواستار حصول نتیجه زیانبار و حتی نتیجه‌ای از فعل خویش نیست (محسنی، ۱۳۷۵: ۲۴۲). به‌طور مثال، عمل راننده‌ای که با علم به نقص ترمز، وسیله نقلیه خود را به حرکت درآورد و در اثر تصادف با عابری، باعث فوت یا مجروح شدن او شود، جزء موارد سوءنیت احتمالی یا اتفاقی به‌شمار می‌رود. در سوءنیت احتمالی، مفروض این است که عامل تمام نتایج اعمال خود را پیش‌بینی کرده است، ولی نمی‌توان گفت قطع‌به‌یقین خواستار نتایج آن شده است (علی‌آبادی، ۱۳۷۱: ۶۴). سؤال این است که آیا درخصوص سوءنیت احتمالی حکم عمد قابل اجراست یا حکم غیر عمد؟

درخصوص جرائم ارتکابی در محیط واقعی نظر غالب بر این است که بنا به تفسیر مضیق قوانین جزایی و تفسیر به نفع متهم ایجاب می‌کند جز در موارد منصوص،[1] عمد احتمالی را در ردیف عمد قطعی قرار ندهیم و در موارد غیرمنصوص باید آن را در ردیف خطای کیفری برشماریم. مضاف بر اینکه نمی‌توان عمد قطعی و عمد احتمالی را مشمول یک حکم قرار داد؛ زیرا خطر مجرمی که با قصد و اراده قطعی به ارتکاب جرمی می‌پردازد، به مراتب بیش از کسی است که فقط احتمال آن را می‌دهد (قیاسی، ساریخانی و خسروشاهی، ۱۳۹۰: ۳۱۹). عدم پذیرش عمد احتمالی مورد تأیید قانونگذار نیز قرار گرفته و صراحتاً در ماده (۱۴۴) قانون مجازات اسلامی ۱۳۹۲، بر لزوم علم و قصد جازم مرتکب برای تحقق رفتار مجرمانه تأکید داشته است. اما در زمان حاضر که رایانه در همه ابعاد زندگانی بشر نقش اساسی و حیاتی ایفاء می‌کند و حفظ امنیت سیستم‌های رایانه‌ای به لحاظ مخاطرات زیانبار و گسترده آن ضرورت دارد و در این قبیل بی‌احتیاطی‌های حتی کوچک به لحاظ

---

۱. ر.ک: ماده (۶۸۹) قانون تعزیرات: «در تمام موارد مذکور در این فصل، هرگاه حریق و تخریب و سایر اقدامات انجام شده منتهی به قتل یا نقص عضو یا جراحت و صدمه به انسان شود، مرتکب علاوه‌بر مجازات‌های مذکور، حسب مورد به قصاص و پرداخت دیه و درهرحال به تأدیه خسارات وارده نیز محکوم خواهد شد».

ویژگی‌های خاص فضای سایبر ازجمله فراملی بودن، کنترل‌ناپذیری و پوشیدگی و ...، ممکن است خطرات و خسارات شگرف و بعضاً جبران‌ناپذیری به جامعه وارد شود، به‌نظر می‌آید در راستای اعمال رویکرد افتراقی و سختگیرانه، عمد احتمالی را بایستی تابع حکم عمد قطعی قرار داد. توسعه حکم سوءنیت احتمالی در جرائم سایبری به عمد قطعی، موجب خواهد شد تا از بی‌احتیاطی‌های فاحشی که آثار و خسارات جبران‌ناپذیری دارد، جلوگیری شود.

نمونه این سیاست کیفری افتراقی را می‌توان در ماده (۲۵) قانون جرائم رایانه‌ای (ماده (۷۵۳) قانون مجازات اسلامی) مشاهده کرد. قانونگذار در بند «ب» ماده مذکور مقرر داشته: «فروش یا انتشار یا در دسترس قرار دادن گذرواژه یا هر داده‌ای که امکان دسترسی غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی متعلق به دیگری را بدون رضایت او فراهم کند». هدف قانونگذار از این سختگیری کیفری و متعاقباً جرم‌انگاری رفتارهای موضوع بند مذکور، جلوگیری از بروز رفتارهای مجرمانه احتمالی بعدی است که ممکن است با آثار گسترده و زیانباری همراه باشد. لذا صِرف اینکه شخصی اقدام به فروش یا انتشار داده‌ای کند که امکان دسترسی غیرمجاز به سامانه دیگری وجود داشته باشد، مجرم تلقی می‌شود. به‌بیان‌دیگر، قانونگذار با اطلاق ماده مذکور، قصد داشته صرف‌نظر از عمد قطعی مورد نیاز، با ملاک قرار دادن معیار عینی در احراز عنصر روانی، جلوی بی‌احتیاطی‌های هرچند کوچک را در حوزه سایبر جهت جلوگیری از آثار مخرب آن، بگیرد و آن را مشمول حکم عمد قطعی کند؛ بدین‌صورت که در مواردی که به‌کارگیری داده‌ای، احتمال دسترسی غیرمجاز را برای دیگری فراهم می‌کند، نبایستی مورد فروش یا انتشار و یا در دسترس دیگری قرار گیرد و مرتکب نمی‌تواند به این دفاع که قصد قطعی فراهم کردن شرایط ارتکاب دسترسی غیرمجاز برای دیگری را نداشته و صرفاً احتمال ارتکاب وجود داشته، مبرا از مسئولیت کیفری باشد. بنابراین، ضروری است با توسعه حکم عمد به رفتارهایی که احتمال وقوع خسارات زیانبار آن توسط مرتکب وجود دارد، درصدد مقابله هر چه کارآمدتر و مؤثرتر با جرائم سایبری برآییم.

۳. جمع‌بندی، نتیجه‌گیری و پیشنهادها

تبیین واکنش‌های کیفری در قوانین جزایی سنتی، عموماً از اصول و مبانی مشترکی پیروی

می‌کند. در تعیین این واکنش‌ها تعریف بزه، ارکان تشکیل‌دهنده آن، مبانی مسئولیت کیفری و قواعد حاکم بر مجازات‌ها به‌گونه‌ای عمل می‌شود که کاربردی کمابیش یکسان در مورد انواع بزه و بزهکاری داشته باشد. سیاستگذاران حوزه کیفر تلاش می‌کنند برای تحقق عدالت و حفظ حقوق و آزادی‌های فردی قواعدی نسبتاً یکسان را برای مقابله با همه مصادیق بزه و بزهکاری به‌کار بندند. اما گاه ظهور و بروز مصالح و ارزش‌های نوین، ویژگی‌های خاص بزهکار و گستره بزه‌دیدگان یا آثار گسترده‌ای که گونه‌ای خاص از بزه ازجمله جرائم سایبری در جامعه دارد و نیز ناکارایی نظام عدالت کیفری سنتی، باعث می‌شود که قانونگذار در موارد استثنایی، معیارها، ضوابط و قوانین متمایز از معیارها، ضوابط و قوانینِ متعارف حاکم بر بزه وضع کرده یا به همین سبب آیین‌هایی متفاوت از شیوه‌هایی متداول دادرسی تعریف و تدوین کند. آنچه جرائم سایبری را از سایر جرائم جدا ساخته، ماهیت فنی و ویژگی‌های خاص این جرائم است که نیاز به اتخاذ رویکرد افتراقی در جرم‌انگاری این دسته از جرائم دارد. چراکه تکنولوژی جدید ازسویی ارتکاب جرائم کلاسیک را تسهیل کرده و از این رهگذر موجب دگرگونی توصیف و ارکان و شرایط عمل مجرمانه و نیز فنی شدن شیوه‌های ارتکاب جرم شده است و ازسوی‌دیگر موجب بروز اشکال جدیدِ جرائم شده که منافع و ارزش‌های جدیدی را مورد تجاوز قرار می‌دهد. ازاین‌رو، به دو جهت نیازمند سیاست کیفری افتراقی و متمایز از رویکرد معمول و کلاسیک احساس می‌شود: نخست به‌لحاظ نوین بودن موضوع جرم سایبری که اطلاعات است و دوم به‌لحاظ فنی بودن جرم سایبری که به دگرگونی ارکان و شرایط رفتار مجرمانه سایبری نسبت به سایر جرائم سنتی منجر شده است. البته حقوق کیفری ایران در حوزه ماهوی در راستای مقابله با این قبیل جرائم، تا حدودی در مسیر اتخاذ یک سیاست کیفری افتراقی گام برداشته است و در برخی موارد این رویکرد افتراقی را پذیرفته و در برخی موارد نیز به آنها توجهی نداشته؛ لذا این عملکرد نیازمند توسعه و اصلاح بیشتری است.

منابع و مآخذ

۱. اردبیلی، محمدعلی (۱۳۹۲). *حقوق جزای عمومی*، جلد نخست، چاپ سی‌ودوم، تهران، انتشارات میزان.

۲. اسحاقی، محمد (۱۳۷۸). «بزهکاری پیشرفته (قسمت دوم)»، فصلنامه *دانش انتظامی*، ش ۳ و ۴.

۳. پاکزاد، بتول (۱۳۸۴). «اقدام‌های سازمان‌های بین‌المللی منطقه‌ای درخصوص جرم‌های رایانه‌ای، تاریخچه، تعریف و طبقه‌بندی جرم‌های رایانه‌ای»، *مجموعه مقالات همایش بررسی جنبه‌های حقوقی فناوری اطلاعات*، چاپ اول، تهران، انتشارات سلسبیل.

۴. پرادل، ژان (۱۳۸۱). *تاریخ اندیشه‌های کیفری*، ترجمه علی‌حسین نجفی ابرندآبادی، تهران، نشر میزان.

۵. حسن‌بیگی، ابراهیم (۱۳۸۴). *حقوق و امنیت در فضای سایبر*، انتشارات مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر، تهران.

۶. خرم‌آبادی، عبدالصمد (۱۳۸۴). «جرائم فناوری اطلاعات»، رساله دکتری دانشکده حقوق دانشگاه تهران.

۷. دزیانی، محمدحسن (۱۳۷۳). «ابعاد جزایی کاربرد کامپیوتر و جرائم کامپیوتری» (قسمت اول)، خبرنامه *انفورماتیک*.

۸. زیبر، اولریش (۱۳۸۳). *جرائم رایانه‌ای*، ترجمه محمدعلی نوری، چاپ اول، تهران، انتشارات گنج دانش.

۹. سازمان ملل (۱۳۷۶). «نشریه بین‌المللی سیاست جنایی»، ترجمه دبیرخانه شورای عالی انفورماتیک، سازمان برنامه و بودجه کشور، ش ۴۳ و ۴۴.

۱۰. سلماسی‌زاده، محمود (۱۳۸۷). «جنگ اطلاعات و امنیت»، خبرنامه *انفورماتیک*، سازمان برنامه و بودجه کشور، ش ۸۰.

۱۱. شامبیاتی، هوشنگ (۱۳۹۱). *حقوق جزای عمومی*، جلد اول، چاپ هجدهم، تهران، انتشارات مجد.

۱۲. علی‌آبادی، عبدالحسین (۱۳۷۱). *حقوق جنایی*، جلد اول، چاپ سوم، تهران، انتشارات فردوسی.

۱۳. فلاحی، احمد (۱۳۹۲). «اصل ضرورت در جرم‌انگاری»، رساله دکتری، دانشگاه تهران پردیس فارابی.

۱۴. قیاسی، جلال‌الدین، عادل ساریخانی و قدرت‌الله خسروشاهی (۱۳۹۰). *حقوق جزای عمومی*، جلد دوم، چاپ دوم، قم، پژوهشگاه حوزه و دانشگاه.

۱۵. گرایلی، محمد باقر (۱۳۸۹). «بررسی جعل و تخریب و اخلال رایانه‌ای»، مجله *آموزه‌های حقوقی*، ش ۱۴.

۱۶. محسنی، مرتضی (۱۳۷۵). *دوره حقوق جزای عمومی*، جلد نخست، تهران، انتشارات گنج دانش.

۱۷. مرهج الهیتی، محمد حماد (۲۰۰۴). *التکنولوجیا الحدیثه و القانون الجنایی*، الطبعه الاولی، عمان، دارالثقافه للنشر و التوزیع.

۱۸. نجفی ابرندآبادی، علی‌حسین (۱۳۹۱-۱۳۹۰). *تقریرات سیاست جنایی*، گردآوری محسن مرادی، دانشکده حقوق دانشگاه قم.

۱۹. نجفی ابرندآبادی، علی‌حسین (۱۳۸۵-۱۳۸۴). «تقریرات درس درآمدی بر جرم‌شناسی بزهکاری اقتصادی و حقوق کیفری اقتصادی»، دوره کارشناسی ارشد دانشگاه شهید بهشتی.

۲۰. نجفی ابرندآبادی، علی‌حسین و محمدجعفر حبیب‌زاده و محمدعلی بابایی (۱۳۸۳). «جرائم مانع (جرائم بازدارنده)»، مجله *مدرس علوم انسانی*، ش ۳۷.

۲۱. وایلدینگ، ادوارد (۱۳۷۹). *جرائم رایانه‌ای*، ترجمه محمد هادی موزون جامی و محسن کریمی زیارانی، تهران، معاونت آموزشی ناجا.

22. Brenner, Susan W. (2005). Toward a Criminal Law for Cyber Space: Distributed Security, Vol. 10: 1, *Journal of Science and Technology Law*, at:www.cybercrimes.net.

23. Brenner, Susan W. and CCE Rico (1993). Other Complex Crime: Traus Formation of American Criminal Law, 2wm & Mary Billrts.J.

24. Campbell, D. (2000). "Echelon: Interception Capabilities Report", available at:www.cyberrights.org/interception/stoa_cover.htm.

25. Cooter, Robert and Thomas Ulen (2004). *Law and Economic*, Harper Collins Publisher.

26. Dorumodd, Einar and Per-Kristian Foss (2006). The Norwegian Government Action plan for Combating Economic Crime.

27. Dubber, Markus D. (2001). "Criminal Law Policing Possession: The War on Crime and the End of Criminal Law", *The Journal of Criminal Law & Criminology*, Vol. 91. No. 4.

28. Egger, Steven A. and Linkage Blindness (1990). A Systemic Myopia,in 8 Serial Murder: an Elusive Phenomenon.

29. Elliott, Catherine and Quinn (2000). *Criminal Law, Third Edition*, Pearson Education Limited, England.

30. http://rc.majlis.ir/fa/legal_draft/show/844651

31. http://www.cyberbannews.com

32. Ius In Formation- Vol. 6 Information Technology Y Crime, Edited by u,Sieber Car Heiman ver lag, 1994.

33. Ringwelski, M. (2001). Effects of Cyber Crime, Access on: www.ehow.com/ about_5052659_effects-cyber-crime.html.

34. Rizgar, Mohammed Kadir (2010). The Scope and the Nature of Computer Crimes Statutes, *German Law Journal*, Vol. 11, No.06.

35. Vaca, John (2002). Computer Forensics, Computer Crime Scene Investigation, Chorles River Media.

36. Wilson, Mark I. (2003). Real Places and Virtual Spaces, Network and Communication Studies, net com, Vol. 17, N. 3-4, Available at://recherché.univ.gov.

37. www.ftc.gov.bcp/conline/pubs/creditlidtheft/htm=law.