مجلهٔ دانش و توسعه (علمی - پژوهشی) سال هفدهم، شمارهٔ ۳۴، ویژه اسفند ۱۳۸۹

جرایم سایبر و رویکرد افتراقی حقوق کیفری

(با نگاهی به قانون مجازات اسلامی‌بخش جرایم رایانه‌ای)

عبدالرضا جوان جعفری *
استادیار گروه حقوق دانشگاه فردوسی مشهد

چکیده

فناوری اطلاعات، تمام ابعاد زندگی اجتماعی، اقتصادی، فرهنگی و از جمله حقوق کیفری را عمیقاً متأثر ساخته است. این تحول، حقوقدانان و سیاست‌گذاران حوزه‌های مربوطه را به تأمل وادار نموده است. تفاوت‌های جرایم سایبر با جرایم سنتی به گونه‌ای است که رویکرد کیفری متعارف و اصول و مبانی شناخته شده آن برای مقابله با این جرایم پاسخگو نیستند. فرامرزی بودن، سهولت ارتکاب جرم و ناشناختگی مجرمین از جمله خصایص این گونه جرایم‌اند. ویژگی‌های مذکور از یک سو ووابستگی‌های ساختارهای زندگی مدرن به تکنولوژی سایبر از یک سوی دیگر، تبیین یک رویکرد کیفری متفاوت را ضروری ساخته است. اثربخشی و کارآیی قوانینی که برای مقابله با جرایم دیجیتال تصویب می‌شوند، مستلزم نگاهی متفاوت به مقولاتی مانند تعریف جرم، ارکان جرم، مسئولیت کیفری و امثال آن است. موضوع اصلی این نوشتار بیان دلایل و ضرورت‌های وجودی رویکرد افتراقی قوانین کیفری در مبارزه با جرایم رایانه‌ای است. هرچند موضوع اصلی این مقاله تجزیه وتحلیل قوانین و مقررات مربوط به جرایم سایبری در ایران نیست، اما تلاش می‌شود با نگاهی به قانون مجازات اسلامی‌بخش جرایم رایانه‌ای میزان توجه این قانون به کاربست لوازم یک رویکرد افتراقی مورد تجزیه و تحلیل قرار گیرد.

واژهای کلیدی: جرایم سایبر، جرایم سنتی، رویکرد افتراقی

طبقه بندی JEL: G11, L20

---

* - (نویسنده مسئول): arjaafari@gmail.com

تاریخ دریافت: ۸۹/۴/۶ تاریخ پذیرش: ۸۹/۸/۱۱

Cyber Crime and Criminal Law Approach to the Differential (Looking at the Part Computer Crime Law Islamic)

Abdolreza Javan jafari
Assistant Professor of low,
***Ferdowsi University** of Mashhad*

Abstract

Information technology development has deeply affected all aspects of social, economic, cultural, life including criminal law. This development has forced lawyers and policy makers of these areas to reflect deeply. Differences between traditional and cyber crimes are such that long standing conventional criminal policy can no longer tackle them. Transnationality, easiness of occurrence, anonymity of culprits and their large scale effects partly show the characteristics of these offences. These features on one hand and dependence of the modern social life's structures on the other hand necessitate preparing a new criminal approach. Efficacy and efficiency of new acts against digital crimes require a new advance to categories such as definition of crime, elements of crime, criminal responsibility and so on. The main focus of this article is explanation of reasons and requirements of distinguished criminal policy against cyber crimes. Although analytical investigation of the Iranian criminal law in cyber crime is not the main aim of this writing, I tried to find out to what extent the differentiated criminal approach is adopted and applied by the Iranian criminal law.

Keywords: cyber crimes, traditional crimes, differentiated criminal approach

JEL: G11, L20

۱. مقدمه

توسعه‌ی پدیده جهانی فناوری اطلاعات و ارتباطات، تحولی شگرف در ابعاد مختلف حیات اقتصادی، اجتماعی، فرهنگی، امنیتی وسیاسی ایجاد نموده است. انقلاب الکترونیک تبدیل به مهم‌ترین پدیده تعیین‌کننده معاصر شده است. روزانه ده‌ها هزار رایانه ورود خود را به دنیای جدید اعلام می‌کنند. این گستره بیکران از یک سو فرصت‌های بی نظیری را فراهم ساخته و از سوی دیگر تهدیدهای جدی را متوجه بخش اعظم ساختارهای اجتماعی ساخته است.

این ویژگی دوگانه را در بسیاری از نوآوری‌ها و ابداعات بشری از جمله انقلاب صنعتی می‌توان مشاهده کرد. اما به نظر می‌رسد ابرساختار فناوری اطلاعات، دنیای جدیدی را خلق کرده، است. دنیایی مملو از نوآوری‌ها و پیچیدگی‌ها که قاعده و نرم پذیرفته شده‌ای ندارد (Grareth, et.al, 2005). این جهان متفاوت از جهان واقعی است. مالک خصوصی و دولتی ندارد. اینترنت

تابع آیین نامه‌ای جهانی نمی‌باشد، هیچ قانون‌گذار عمومی‌وجود ندارد، اگرچه تلاش‌هایی به منظور توسعه قانون‌گذاری در شماری از مراجع چند جانبه صورت می‌پذیرد. با وجود این امروز اینترنت اغلب به عنوان محیطی بی‌قانون، نامحدود، نامنظم، کنترل نشده و قابل دسترسی، دست کم به لحاظ تئوری برای همه توصیف شده است." (Steven, et.al, 2006) عدم وجود ظوابط دقیق در دنیای مجازی باعث شده است که از آن به عنوان غرب وحشی جدید[1] تعبیر شود. فناوری اطلاعات و ارتباطات نه تنها صنعت، اقتصاد، تجارت و دیگر عرصه‌ها را تحت تأثیر قرار داده است، بلکه حقوق هم از این تحولات بی‌بهره نبوده است. به فراخور این تغییرات بنیادین، طبعاً حقوقدانان نیز همانند متخصصین دیگر رشته‌ها باید برای هماهنگی با این فناوری و عقب نماندن از آن، به ارائه ضوابط، اصول و قواعد حقوقی جهت پیشگیری یا حل و فصل اختلافات ناشی از این تغییرات (Rezaee, 2009) اقدام نمایند.

این فضای جدید به گونه‌ای حقوق جزای سنتی را دستخوش تحولات بنیادین کرده است که تعریف از جرایم در محیط‌های مجازی انطباق چندانی با تعاریف کلاسیک نداشته و در بسیاری از موارد متفاوت است.(Hassan Baigi,2005)

نکته‌ی مهم در ارتباط با جرایم سایبری ویژگی‌های انحصاری آنها در مقایسه با جرایم سنتی است. سرعت، کثرت، سهولت ارتکاب، ارزان بودن، بی مرز بودن، ناشناختگی، اتوماتیک بودن و ... در جرایم دیجیتال موجب ظهور گونه‌ای متمایز از جرایم شده است. ویژگی‌های مذکور، سهولت سازماندهی و تهاجم از راه دور مجرمین سایبری از یک سو و وابستگی روزافزون ساختارهای اقتصادی، صنعتی، خدماتی، امنیتی و سیاسی به فضای سایبر از سوی دیگر، جامعه بشری را با تهدیدهای جدی جدیدی مواجه ساخته است. به گونه‌ای که گزارشات رسمی‌سازمان ملل هیچ حوزه‌ای از زندگی بشری را فارغ از تهدیدات فضای سایبر نمی‌بیند. (Kamal, 2005). تهاجمات سازمان یافته سایبر می‌تواند تمامی‌زیرساختارهای اجتماعی را دربرگرفته و حتی امنیت و حاکمیت ملی را هدف قرار دهند. تروریسم سایبری[2] و جنگ سایبری[3] امروزه مفاهیم شناخته

1- New Wild West
2- Cyber Terrorism
3- Cyber War

شده‌ای، هستند.

کشور ما نیز فارغ از تحولات مذکور نبوده است. جمعیت جوان و تحصیلکرده کشور، تعداد کاربران اینترنتی را به مرز ۳۰ میلیون نفر رسانده است. تعداد جرایم سایبری افزایش سالانه ۳۰٪ داشته و کشف جرایم با افزایش ۱۵۰٪ در سال ۱۳۸۸ مواجه بوده است (Omidi,2010). و افزایش تعداد پرونده‌ها در همان سال ۱۰۰٪ بوده است .

جرایمی‌با این وسعت و ویژگی‌های انحصاری، مستلزم استراتژی ویژه‌ای در ابعاد مختلف است. این استراتژی می‌تواند شامل اقدامات گسترده‌ای در ابعاد مختلف کنترل، مدیریت، پیشگیری و واکنش‌های کیفری شود. این نوشتار به تحقیق در یکی از ابعاد اقدامات مذکور یعنی گزینش رویکرد کیفری متمایز در حقوق کیفری ماهوی متمرکز شده است. به نظر نگارنده یکی از وجوه تمایز واکنش به جرایم سایبر، کیفیت تعریف جرایم، تعریف و توسعه مسئولیت کیفری و تعیین مجازات در قوانین کیفری ظاهر می‌شود، به گونه‌ای که قابلیت اجرایی، ارعابی و بازدارندگی بیشتری به واکنش‌های کیفری ببخشد.

در این مقاله تلاش می‌شود، ابتدا مفهوم رویکرد افتراقی اختصارا مورد بحث قرار گیرد. سپس دلایل و ضرورت‌های این رویکرد افتراقی از مسیر توصیف ویژگی‌ها و خصوصیات جرایم سایبر که به نظر نویسنده‌ی این سطور باعث تمایزات کمی‌و کیفی قابل ملاحظه‌ی جرایم سایبری از همتای سنتی خود شده است، با تفصیل بیشتری تبیین می‌شود. تمایزاتی که باعث می‌شود رویکرد سنتی حقوق کیفری پاسخگو نباشد اگرچه تجزیه و تحلیل قانون مجازات اسلامی‌در زمینه مبارزه با جرایم سایبر موضوع اصلی این مقاله نیست و هدف اصلی تبیین ضرورت وجود رویکرد کیفری متفاوت از منظر تئوری‌های حقوق جزا است، ولی تلاش می‌شود چگونگی اعمال این رویکرد جدید در نظام کیفری ایران، از طریق تجزیه وتحلیل قانون مجازات اسلامی‌در حوزه جرایم سایبر، مورد تحقیق قرار گیرد. بدین روش میزان انعکاس رویکرد مذکور در قانون مجازات اسلامی‌روشن خواهد گردید. در نهایت حاصل مباحث پیش گفته در قالب نتیجه گیری اختصارا ارائه می‌گردد.

۲. رویکرد کیفری افتراقی

تبیین واکنش‌های کیفری در قوانین جزایی عموماً از اصول و مبانی مشترکی پیروی می‌کند.

در تعیین این واکنش‌ها، تعریف بزه، ارکان تشکیل دهنده‌ی آن، مبانی مسئولیت کیفری و قواعد حاکم بر مجازات‌ها به گونه‌ای عمل می‌شود که کاربردی کما بیش یکسان درمورد انواع بزه و بزهکاری داشته باشد. مثلا همه جرایم از ارکان سه گانه برخوردار بوده و کیفیات مخففه و مشدده در همه جرایم به صورت کما بیش یکسان اعمال می‌شود. همین ویژگی‌های مشترک را در بعد شکلی یعنی آیین دادرسی کیفری نیز می‌توان مشاهده کرد. در این زمینه آئین‌های حاکم بر کشف بزه، تعقیب، محاکمه و اعمال مجازات علیه بزهکاران اشتراک بنیادین دارند. سیاست‌گذاران حوزه کیفر تلاش می‌کنند برای تحقق عدالت و حفظ حقوق و آزادی‌های فردی قواعدی یکسان را برای مقابله با همه مصادیق بزه و بزهکاری به کار بندند. مثلا قواعد مربوط به حقوق متهم، ادله اثبات بزه، جلب و احضار متهم، نحوه دادرسی و .... نرم‌هایی مشابهند.

اما گاهاً مصالح جامعه، ویژگی‌های خاص بزهکار و یا بزهدیدگان و یا آثار گسترده‌ای که گونه‌ای خاص از بزه در جامعه دارد، باعث می‌شود که قانون‌گذار در مواردی استثنایی نرم‌هایی متمایز از نرم‌های عام و کلی متعارف حاکم بر بزه وضع نموده و یا به همین سبب آیین‌هایی متفاوت از شیوه‌های متداول دادرسی تبیین نماید. الگوهایی از این گونه رویکرد کیفری افتراقی را در جرائم علیه امنیت در ابعاد شکلی و ماهوی می‌توان مشاهده کرد.

در این گونه‌ی خاص از بزه بر خلاف نرم‌های متعارف، گاه اعمال مقدماتی و یا حتی صرف اتخاذ تصمیم گروهی[1] برای ارتکاب بزه، جرم تام تلقی شده است. در حالی‌که موافق اصول بدیهی حقوق جزا تا زمانی که ذهنیت بزهکارانه تجسم عینی پیدا نکرده و به منصه عمل نرسد، بزهی اتفاق نمی‌افتد. در همین موارد تماس مستقیم بزه با امنیت و حاکمیت ملی و آثار گسترده احتمالی آن سبب گردیده است که اقداماتی که طبق مبانی و نرم‌های کلی حتی شروع به بزه نیز تلقی نمی‌شود، به عنوان بزه تام مورد پیگرد و اعمال واکنش‌های کیفری قرار گیرد.

به همین شیوه ارتباط نزدیک جرایم علیه امنیت با مسئله حاکمیت ملی و نظام عمومی، دغدغه قانون‌گذاران را در زمینه تضمینات دادرسی کاهش داده است (Majidi, 2005). ایجاد دادگاه‌های خاص برای رسیدگی به این گونه جرایم و شیوه‌های متفاوت دادرسی نمونه‌هایی از سیاست کیفری

۱- مواد ۶۱۵ و ۶۱۱ قانون مجازات اسلامی

شکلی برگزیده شده از ناحیه قانون‌گذار در برخورد با این گونه جرایم است. نمونه‌ی دیگر رویکرد کیفری افتراقی در نظام عدالت کیفری را می‌توان در حوزه مقررات مربوط به کودکان، به ویژه در زمینه‌ی شیوه‌های خاص دادرسی اطفال و نوجوانان بزهکار مشاهده کرد. فلسفه‌ی این تمایز در قوانین داخلی و اسناد بین‌المللی را می‌توان در آسیب پذیری‌های خاص شخصیتی این قشر در برابر اقدامات تعقیب و دادرسی کیفری متعارف جستجو نمود.

توجه به ویژگی‌ها و تمایزات بزه‌های فضای مجازی تبیین یک رویکرد افتراقی در مقایسه با بزه‌های ارتکابی دنیای واقعی امری قابل درک می‌سازد. بررسی اختصاری ویژگی‌های جرایم فضای مجازی ما را بدین حقیقت رهنمون می‌سازد که مدل‌های ارتکاب جرم در این فضا با مدل‌های جرایم سنتی تمایزات قابل توجهی دارند (Javan jafari, 2007). رویکرد کیفری سنتی موجود مربوط به زمانی است که تکنولوژی، دوران طفولیت خود را سپری می‌کرد. اما امروزه رشد و توسعه تکنولوژی امکان استفاده از نیروهای انسانی سازمان یافته و منابع و امکانات متمرکز برای مقابله با بزهکاران فضای دیجیتال را سلب کرده است. دنیای جدید با ساختاری متفاوت و محیط اجتماعی نو آفریده شده است که در آن استفاده از مدل نظامی‌سلسله مراتبی با بزه‌ها و بزهکاران را مشکل و یا غیر ممکن ساخته است. در مدل سنتی مذکور گزارشات مربوط به بزه‌ها به مرکز واحدی ارسال و از آنجا دستورات لازم برای مقابله با اهداف معین در محیط فیزیکی مشخص صادر می‌شود. بررسی تمایزات بزه‌های موجود در فضای سایبر نشان خواهد داد که مدل مذکور انعطاف لازم را برای کاربرد در محیط جدید ندارد.

۳. ویژگی‌های بزه‌های سایبر

پرسش بنیادین در باب جرایم رایانه‌ای این است که آیا تمایز جرایم مذکور با جرایم سنتی از نوع ماهیت است یا درجه؟ به بیان دیگر تفاوت‌ها از جنس کمیت‌اند یا کیفیت؟ آیا صرفاً فضای ارتکاب جرم، وسایل مورد استفاده، سرعت و حجم جرائم تغییر کرده است یا ماهیت این جرایم نیز دچار تحول شده است؟ آیا می‌توان این تحولات را ترکیبی از تغییرات کمی و کیفی دانست. در حالت اول یعنی پیش فرضی که در آن صرفاً وسیله و محیط ارتکاب جرم دچار دگرگونی شده است، با مهاجرت مدل‌های سنتی به فضای دیجیتال و با تغییراتی نه چندان گسترده در سیاست کیفری موجود، می‌توان چالش‌های موجود را مرتفع ساخت. اما اگر تمایزات، محصول تحولات

بنیادین و ماهوی و یا ترکیبی از طیف اول و دوم باشد، برای پاسخگویی به الزامات نوین دنیای مجازی تدوین رویکرد کیفری افتراقی گریز ناپذیر به نظر می‌رسد.

به نظر می‌رسد تحولات ناشی از تولد فضای سایبر، متمایز از دگرگونی‌هایی است که در اثر گسترش سایر فناوری‌های پیچیده و مدرن پدید آمده است. درست است که صنعت حمل و نقل، ارتباطات، جنگ افزار و سایر صنایع و تکنولوژی‌ها بزهکاری‌های خاص خود را تولید کرده‌اند، اما از آنجا که این دگرگونی‌ها عمدتا جنبه‌ی کمی داشته‌اند، نظام عدالت کیفری توانسته است با سرعت بیشتری خود را با الزامات ناشی از ساختارهای نوین هماهنگ سازد. یعنی با استفاده از اصول و مبانی موجود حقوق جزا در بعد شکلی و ماهوی در پی مقابله با جرایم ناشی از تحولات جامعه‌ی صنعتی برآمده و توفیق نسبی کسب نموده است. اما ویژگی‌ها و خصایص بزههای ارتکابی در فضای سایبر حامل این پیام است که حقوق جزا در ابعاد شکلی و ماهوی وارد مرحله جدیدی شده است، به طوری که تنها شرط مبارزه با این گونه جرایم، ارائه تحلیلی نو از نحوه ی ارتکاب بزه سایبری و تدوین رویکرد کیفری متناسب با آن است (Estaki et al, 2004).

در عصر حاضر، سخن صرفاً این نیست که تجهیزات کافی برای مقابله با بزهکاری‌های روزافزون سایبری وجود ندارد و یا اینکه "سرعت و شتاب موجود در رایانه‌ای نمودن و حجم فراوان اطلاعات و استفاده از شبکه، فرصت کافی توسعه سیستم‌های دفاعی در مقابل هجوم و پیشگیری از آن را به ما نداده است. (Ashori, 2007) بلکه حتی تسریع در آمادگی نظام قضایی موجود برای مقابله با موج نوین بزهکاری به صورت کامل پاسخگو نخواهد بود. ادعای این نوشتار آن است که تحقق اهداف مقابله با جرایم سایبرمستلزم تبیین گونه‌ای از رویکرد کیفری است که لزوماً با اصول و مبانی رویکرد کیفری متعارف همسانی ندارد. بیان ویژگی‌های جرایم سایبر بایستگی تدوین چنین رویکردی را روشن‌تر می‌سازد.

۳-۱. سرعت[1]

مفهوم متعارف زمان و مکان در دنیای مجازی دچار تحول شده است. یکی از فاکتورهای

1- Speed

کندی وقوع پدیده بزهکارانه در جهان واقعی بعد مکانی میان سه ضلع بزهکاری یعنی بزهکار، آماج بزه و مکان ارتکاب بزه است. ساختار فضای مجازی به گونه‌ای است که در آن قرابت مکان میان سه عنصر فوق ضرورتی ندارد. این وضعیت موجب صرفه جویی شگرفی از بعد زمان و هزینه برای بزهکاران گردیده و آنها را قادر ساخته است بدون وجود مانعی به نام مکان، جرایم متعددی را در سریع‌ترین زمان مرتکب شوند، هویتی را سرقت نمایند و یا پولی را از حسابی به حساب دیگر منتقل نمایند.

۳-۲. ناشناختگی[1]

ناشناختگی از اصول حاکم بر جرایم جهان مجازی است (Stuart, 2001). از یک سو اصولاً شناسایی کاربران ماشین متصل به شبکه امری پیچیده و پرهزینه است. از سوی دیگر استفاده از شیوه‌های سرقت مشخصات دیگر ماشین‌ها،[2] استتار آنلاین[3] و سایر مخفی کاری‌های موجود، امر شناسایی مرتکبین را به صورت معمول سخت و بعضا غیر ممکن ساخته است. این جرایم عمدتاً قبل از اطلاع نهادهای قانونی و حتی خود قربانی رخ داده و آثار جرایم و نرم افزارهای مورد استفاده، پس از ارتکاب توسط بزهکار سریعاً نابود می‌شوند و یا به صورت اتوماتیک از بین می‌روند.

۳-۳. حجم جرایم[4]

از زمره محدودیت‌های ارتکاب بزه در دنیای واقعی این است که ارتکاب بزه از نرم یک در برابر یک پیروی می‌کند. یعنی معمولاً برای وقوع بزه و ارتکاب آن علیه یک بزه دیده، حضور یک بزهکار لازم است. در بزه‌هایی مانند جعل، سرقت، قتل، اختلاس و ارتشا، بزهکار مجبور است برای آن برنامه ریزی نموده و پس از تهیه وسایل و مقدمات لازم با انجام عنصر مادی جرم و تحقق نتیجه، آن را تعقیب نماید.

1- Anonymity
2- IP spoofing
3- Online Camouflage
4- Large Scale

این محدودیت‌ها به نیروهای اجرای قانون و دستگاه عدالت کیفری کمک می‌کند که برنامه‌ها و منابع مالی و انسانی خود را بر روی بزه و بزهکار معین متمرکز نمایند. اما مقیاس بزه‌های ارتکابی در فضای سایبر بسیار وسیع است و به علت امکانات موجود و فقدان محدودیت‌ها، بزهکار از الگوی سریالی و شبکه‌ای استفاده می‌کند. لذا قربانی کردن هزاران نفر طی اقدامی‌واحد، فرضی واقعی در فضای سایبر است. این امر باعث می‌شود که حجم و آمار بزه در دنیای مجازی با دنیای واقعی قابل قیاس نباشد. آمار جنایی با توجه به زمینه‌های مذکور قابلیت رشد تصاعدی دارند. برخی پژوهش‌های صنعتی نشانگر آن است که در سال ۲۰۰۲ در امریکا بیش از ۹۰٪ بنگاه‌های صنعتی آماج حملات سایبری بوده‌اند و صدها میلیون دلار خسارت دیده‌اند (R.Vaca, 2002).

۳-۴. ارزان بودن بزه[1]

هزینه‌های سنگین مذکور در بندهای قبلی در حالی بر جامعه تحمیل می‌گردد که بزهکاران کمترین هزینه‌های ممکن را در ارتکاب بزه متحمل می‌شوند. این وضعیت فاکتور مضاعفی است که آمار جرایم را بالا برده و مقابله با آن را پیچیده‌تر و مشکل‌تر می‌سازد. مهم‌ترین وسیله ارتکاب بزه در فضای سایبر وجود یک دستگاه رایانه و خط تلفن برای اتصال به اینترنت است. ارزان بودن جرم محدودیت منابع مالی و انسانی را برای سیستم عدالت کیفری تشدید می‌کند (Norris, et.al, 2005). در سال ۲۰۰۲ یک فیلیپینی با ارسال ویروسی به نام "I love you" حدود ۱۰ میلیارد دلار خسارت وارد کرد و کامپیوترهای زیادی را در سراسر دنیا دچار اختلال نمود (Thomas, 2005).

۳-۵. عدم حضور در صحنه بزه[2]

در جرایم سنتی عمدتاً مجرم چاره‌ای جز حضور در صحنه ارتکاب بزه ندارد. این حضور قبل و همزمان با وقوع بزه ضرورت می‌یابد. پس از ارتکاب بزه نیز اقداماتی برای مخفی کردن و یا استفاده از آثار و نتایج حاصله از ارتکاب صورت می‌گیرد. این امر، یافتن سرنخ و تحقیق در باره شناسایی و تعقیب بزهکاران را تسهیل می‌کند. اما عدم حضور بزهکار در صحنه‌ی وقوع بزه سبب

1- Cheapness
2- Lack of Presence in the Crime Scene

می‌شود که شیوه‌های سنتی کشف بزه، تحقیق و شناسایی بزهکار قابلیت اجرا نداشته باشد. این وضعیت و ویژگی فراملی بزه سایبر، کار جمع آوری ادله اثبات بزه را با دشواریهای خاص همراه می‌سازد.

۳-۶. فراملی بودن[1]

وجود مرزهای بین‌المللی و شیوه‌های کنترل متعارف مانند ایست و بازرسی و استفاده از ابزارهای الکترونیکی از یک سو ارتکاب بزه در ورای مرزها را با موانع جدی مواجه ساخته و از سوی دیگر کمک مؤثری به کشف جرایم سنتی، به ویژه جرایم سازمان یافته ی فراملی می‌نماید. بزه سایبری اساساً در فضایی فارغ از مرزهای متعارف بین‌المللی واقع می‌شود. بزهکار بدون نیاز به عبور از مرزهای مذکور می‌تواند در هر نقطه‌ای از کره خاکی مستقر باشد.

در نتیجه‌ی چنین وضعیتی، اولاً: کشف جرم و شناسایی بزهکار با موانع عدیده‌ای روبرو است. ثانیاً: به دلیل گستره‌ی وسیع و پراکندگی حوزه ارتکاب جرم، در صورت کشف بزه و شناسایی بزهکار، پروسه‌ی جمع‌آوری مستندات قانونی، تعقیب و محاکمه بزهکار بسیار زمان بر و پرهزینه خواهد بود (Kamal, 2005). ثالثاً: در بسیاری موارد قانون حاکم و دادگاه صالح برای رسیدگی نظام عدالت کیفری را با چالش‌های جدی مواجه می‌سازد. رابعاً: فقدان قوانین لازم از یک سو و از سوی دیگر تعارض قوانین برخی از کشورها در کنار فقدان اسناد بین‌المللی لازم الاجرا و به ویژه با توجه به خصیصه فراملی بزه سایبری موانع جدی بر سر راه همکاری‌های قضایی و استرداد بزهکاران محسوب می‌شوند.

سرقت سایبری مشهور از سیتی بانک[2] در نیویورک توسط فردی به نام ولادیمیر لوین[3] ساکن در سن پترزبورگ روسیه، FBI را با مشکلات جدی مواجه ساخت. پلیس فدرال آمریکا مجبور شد از نظام قضایی هفت کشور برای بررسی سیستم‌های بانکی این کشور تقاضای مجوز قضایی کند. این وضعیت با تجربه ترین متخصصین سایبری پلیس فدرال را دچار دردسرهای جدی کرده

1- Transnational
2- City Bank
3- Vladimir Levin

بود. نهایتاً ولادیمیر لوین به سه سال حبس و پرداخت ۲۴ هزار دلار به بانک آمریکایی مذکور محکوم شد (Thomas, Opcit).

۳-۷. بالا بودن رقم سیاه[1]

بالا بودن رقم سیاه[2] در جرایم سایبری معلول دو علت است. از طرفی به دلایل پیش گفته اصولاً کشف بزههای سایبری بسیار مشکل‌تر از بزهکاری سنتی است. از سوی دیگر شرکت‌ها و مؤسسات معتبر تمایلی ندارند که با افشای این جرایم نا امن بودن فضای فعالیت‌های اقتصادی خود را افشا نمایند. چرا که این امر اعتبار این بنگاه‌های تجاری و صنعتی را که مهم‌ترین سرمایه‌ی آنها در جلب مشتری است، مخدوش می‌سازد. در نتیجه دو فاکتور مذکور می‌تواند افزایش قابل توجه رقم سیاه بزه در فضای مجازی باشد.

یکی از 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 مجازات است. در تحلیل اقتصادی از جرم و مجازات و در چارچوب تئوری انتخاب عقلایی[3] 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 et.al, 2004).

۳-۸ اتوماتیک بودن جرم[4]

مرکز امنیت تکنولوژیکی اطلاعات ایالت جورجیای امریکا (CTIC)[5] پس از نشست سالیانه خود در سال ۲۰۰۹ طی گزارشی اعلام کرد که در سال گذشته ۱۰٪ کامپیوترهای آنلاین به عنوان

1- Dark Figure of Crime

۲- عددی که نسبت بین جنایتکاران حقیقی و جنایتکاران قانونی یا قضایی را نشان می دهد در آمار جنایی رقم سیاه نامیده می شود. رک. کی نیا مهدی (1978) مبانی جرم شناسی، انتشارات دانشگاه تهران ص ۶۰-۱۵۹

3- Rational Choice

4- Automation

5- Georgia Tech Information Center

عامل بوتنت‌ها[1] (شبکه رباط‌ها) عمل کرده‌اند. به موجب این گزارش تعداد این ماشین‌های آنلاین در سال ۲۰۱۰ به ۱۵٪ می‌رسد[2]. شیوه کار این بوتنت‌ها به این ترتیب است که شما پیام جالبی را از دوستی، مثلاً از طریق facebook، دریافت کرده و روی آن کلیک می‌کنید. سپس از شما می‌خواهد که برای دیدن ویدئوی مورد علاقه خود نیازمند نصب flash player هستید و یا باید آن را به روز کنید. بعد از کلیک شما در واقع یک Malware روی ماشین شما ذخیره شده و طبق فرمان برنامه، کلیه اطلاعات شما را به صورت اتوماتیک برای طراحان برنامه می‌فرستد. در چنین روشی بزهکاران بدون نیاز به اقدام دیگری به صورت مستمر به شکلی اتوماتیک به سیستم اطلاعات شما دسترسی پیدا می‌کنند (Ibid). هکر می‌تواند این رباط‌ها را در کامپیوترهای متعدد وارد کرده و شبکه بوتنت‌ها را ایجاد نماید. این شبکه‌ها که در اختیار هکرها هستند، می‌توانند به صورت اتوماتیک حجم انبوهی از اطلاعات و فرامین را ارسال و دریافت نمایند (Kamal, (Opcit.

۳-۹. درونی بودن بزه[3]

در جرایم سنتی این امکان وجود دارد که جرایم از ناحیه افرادی که دسترسی به موضوع جرم دارند رخ دهد، مانند سرقتی که مستخدمان منازل مرتکب می‌شوند و یا اختلاسی که از ناحیه کارکنان یک سازمان دولتی انجام می‌شود. از آنجا که این اقدامات مجرمانه درونی از ناحیه افراد مورد اعتماد انجام می‌شود، آثار گسترده‌تری نسبت به اقداماتی که از ناحیه افراد بیگانه انجام می‌شود دارند، قانون‌گذار کیفری این وضعیت را یک کیفیت مشدده تلقی کرده و مجازات شدیدتری نسبت به آنها اعمال می‌کند. مانند آنچه در اختلاس در مقایسه با خیانت در امانت و سرقت مستخدمان در مقابل سرقت معمولی در قانون مجازات اسلامی‌دیده می‌شود.[4]

این مشکل در بزه‌های سایبری به صورت حادتری مشاهده می‌شود. یکی از مشکلات جرایم

1- Botnets
2- www.kaspersky.com/newszid, 2009
3- Insider Attack
۴- رک به: قانون مجازات اسلامی مواد ۶۵۶-۶۷۳ و قانون تشدید مجازات مرتکبین ارتشا و اختلاس و کلاهبرداری مصوب 1988 مجمع تشخیص مصلحت نظام

سایبری درونی بودن بسیاری از جرایم است. مستخدمان، پیمانکاران، مشاوران، شرکا و همکاران شرکت و مشاوران و پیمانکاران آنها، عاملان اصلی جرایم علیه یک شرکت یا سازمان هستند که تفکیک آنها از خارجی‌ها به سهولت امکانپذیر نیست (Kenneth, 2008).

در کنار ویژگی‌های فوق می‌توان به مشخصات دیگری مانند غیر ملموس بودن بزه‌های سایبری اشاره کرد. جرایم سنتی مانند سرقت اموال و یا اسناد امنیتی به علت عینی بودن، دیر یا زود کشف می‌شوند. اما برخی از بزه‌های سایبری ممکن است بسیار دیر کشف شده یا هرگز کشف نشوند. سرقت اطلاعات، جاسوسی و یا حتی سرقت‌ها و تخلفات جزیی سایبری که به مقدار زیادی رخ می‌دهند، ممکن است هرگز جلب توجه نکرده و کشف نگردند.

اما در کنار مختصات و ویژگی‌های پیش گفته که عمدتاً جنبه فنی و تخصصی دارند، یک سلسله عوامل فرهنگی و اجتماعی نیز می‌توانند از یک سو به عنوان عواملی در گسترش جرایم سایبری و از سوی دیگر به عنوان محدودیت‌هایی در مسیر مقابله و پیشگیری از جرایم سایبری مورد پژوهش قرار گیرند. فاکتورهایی مانند نوع بزهکاران سایبری، خواستگاه طبقاتی و اجتماعی آنها، عدم آشنایی کاربران با مخاطرات فضای سایبری و شیوه‌های مقابله با آنها و فقدان فشارها و کنترل‌های اجتماعی و ... می‌توانند در گسترش جرایم سایبری دخیل باشند. برای اختصار بیشتر در این بخش به یکی از عوامل فرهنگی و اجتماعی مذکور یعنی فقدان یا ضعف فشار و کنترل اجتماعی در جرایم سایبری پرداخته می‌شود.

۳-۱۰. ضعف یا فقدان کنترل اجتماعی[1]

قواعد مرتبط با جرایم سنتی یا عموماً ریشه در فرهنگ اخلاق جامعه داشته و یا بعضاً در طی زمان بخشی از فرهنگ جامعه شده‌اند. بنابراین، ارتکاب بزه علاوه بر نقض قوانین رسمی کشور، تعرض به ارزش‌ها و نرم‌های اجتماعی نیز محسوب می‌شوند. این نرم‌ها دوگونه کارکرد دارند؛ از یک سو با درونی شدن ارزش‌های اجتماعی، فرد هنگام مواجهه با بزه نوعی فشار درونی احساس می‌کند. این مکانیسم خودکنترلی[2] عاملی برای پیش گیری از جرم محسوب می‌شود. از سوی

1- Social Control
2- self-control

دیگر نگرانی از ننگ و رسوایی حاصل از دستگیری، محکومیت و مجازات، بزهکار بالقوه را شدیداً آزار می‌دهد (Salimi, 2004). یعنی افراد زیادی به این علت بزهکار نیستند که یا باورهای درونی آنها را کنترل می‌کند و یا نگرانی از قضاوت بد دیگران[1] مانع از تخلف و قانون‌شکنی می‌شود.

شرایط مذکور در مورد بسیاری از رفتارهای مزاحم در فضای سایبر به گونه‌ای دیگر است. برخی از رفتارهای آسیب رسان در این حوزه هنوز جرم انگاری نشده‌اند. برخی به علت فقدان سابقه‌ی لازم در فرهنگ اجتماعی رسوخ نکرده و ارتکاب این رفتارها موجب برانگیختگی افکار عمومی‌نمی‌شود. مثلاً برخی از بزه‌های سایبری مانند دسترسی غیرمجاز، تعرض به خلوت دیگران، سرقت اطلاعات، انواع هک کردن و ... هنوز بار ارزشی نگرفته و درونی نشده‌اند. بنابراین مکانیسم خودکنترلی فاقد کارکرد لازم در این حوزه است.

از سوی دیگر عدم حضور بزهکار در صحنه جرم، عدم مشاهده‌ی دیگران، پایین بودن احتمال دستگیری و مجازات، از کارآیی مکانیسم فشار و کنترل اجتماعی می‌کاهد. علاوه بر این‌ها از نگاه جامعه شناسی کیفری، فقدان بار ضد ارزشی یک رفتار انحرافی مانع جدی بر سر راه وضع مجازات‌های شدیدتر خواهد بود. یعنی شرایط فرهنگی، درون مایه لازم را برای تجویز مجازات‌های شدید نخواهد داشت. در چنین شرایطی مجازات‌های شدید از نگاه بزهکار، جامعه، قانون‌گذار و دستگاه عدالت کیفری نامتناسب و غیر عادلانه تلقی خواهد شد.

مباحث پیش گفته نشان از آن دارد که در ارتباط با جرایم سایبری سیستم عدالت کیفری، با شرایطی کاملاً متمایز مواجه است. از سویی سرعت، حجم و آثار زیانبار این جرایم بسیار گسترده‌تر از جرایم سنتی است. از سوی دیگر به علت غیر ملموس بودن، پدیده ناشناختگی، فقدان محدودیت‌های فیزیکی برای مجرمین، عدم ضرورت حضور فیزیکی مجرم در صحنه جرم، هزینه بالای کشف جرم و تعقیب مجرمین و ... ، دستگیری و مجازات بزهکاران حوزه سایبر را با محدودیت‌های جدی مواجه ساخته است. علاوه بر این‌ها به علت فقدان سابقه و نرم‌های تثبیت شده اجتماعی، چنان که ملاحظه شد، زمینه‌های لازم برای وضع مجازات‌های سنگین‌تر و ارعاب

1- social- control

مجرمین بالفعل فراهم نیست.

باید اضافه کرد که فقدان نرم‌های اجتماعی، هم کنترل درونی و هم کنترل بیرونی را با محدودیت‌هایی مواجه ساخته است. درونی کردن هنجارها و ایجاد روح وفاداری لازم نسبت به قواعد حوزه دیجیتال نیز، به دلیل بیگانه و ناآشنا بودن محیط، زمانی طولانی می‌طلبد و در کوتاه مدت اثر بخشی لازم را نخواهد داشت (Brenner, 2005). در سایر حوزه‌های پیش‌گیری و کنترل نیز محدودیت‌های قابل ملاحظه‌ای مشاهده می‌شود. مثلاً به دلایل استفاده از سیاست‌های معمول پلیس اجتماعی[1] هنوز کاربردی تعیین‌کننده ندارد.

بنابراین، مواجهه با جرایم فضای سایبر، راهبردها و برنامه ریزی‌های ویژه خود را می‌طلبد. به عنوان مثال می‌توان مجموعه‌ای از راهبردهای کنترل، مدیریت، پیشگیری و سایر اقدامات کنشی و واکنشی مربوط به حوزه سیاست جنایی را برای توفیق در این حوزه توصیه نمود، (javan Jafari,2005) که البته موضوع این نوشتار نیست. موضوع این مقاله تبیین رویکرد کیفری متناسب با جرایم سایبری در بعد ماهوی است. پیامد بحث‌های گذشته این است که مانند سایر حوزه‌های سیاست جنایی مقابله با جرایم سایبری، اقدام کیفری اثر بخش در بعد ماهوی نیز مستلزم رویکرد خاصی است، که از آن به رویکرد کیفری افتراقی یاد کردیم. اکنون زمان آن رسیده است که الگوهایی از رویکرد کیفری منظور در حوزه حقوق جزای ماهوی از نگاه تئوری‌های عمومی‌حقوق جزا مورد تحلیل قرار گیرد. در ضمن برای تبیین بیشتر بحث، تلاش خواهد شد کیفیت انعکاس این الگوها در قانون مجازات اسلامی‌بخش جرایم رایانه‌ای مورد توجه قرار گیرد.

۴. رویکرد کیفری افتراقی و انعکاس آن در قانون مجازات اسلامی‌بخش جرایم رایانه‌ای

منظور از رویکرد کیفری افتراقی در این حوزه کاربست رویکردی متمایز و البته سخت گیرانه در مواجهه با جرایم فضای سایبر، در مقایسه با جرایم سنتی است. منظور این نیست که این رویکردی کاملاً متفاوت بوده و همه راهکارها ابداعی و ویژه‌این جرایم هستند. مدعای این نوشتار این است که مدل واکنش کیفری اثربخش در این حوزه، کاربست گسترده‌تر مجموعه‌ای

1- community policing

ازتکنیکهای حقوقی است که یا در حوزه جرایم سنتی کاربردی ندارند و یا به گونه‌ای استثنایی به کار گرفته می‌شوند. در واقع برخی از تکنیک‌ها ابداعی بوده و برخی دیگر از تدابیر استثنایی و پراکنده موجود در جهان واقعی به صورت سیستماتیک و هدفمند در فضای سایبر مورد استفاده قرار می‌گیرند. عدم حمایت کیفری از بزهدیده‌ی سهل انگار، استفاده از مفاهیمی مانند مسئولیت نیابتی و مسئولیت مطلق، توسعه مسئولیت کیفری اشخاص حقوقی، جرم انگاری اعمال مقدماتی، شناسایی شروع به جرم به عنوان جرم تام، گسترش حوزه جرایم مطلق، شناسایی ترک فعل به عنوان عنصر مادی جرم، گسترش مفهوم معاونت، کاهش عناصر تشکیل دهنده جرم و امثال آن می‌توانند اجزایی از رویکرد کیفری افتراقی قوانین ماهوی در حوزه فضای مجازی باشند. این نوشتار جستاری در کیفیت استفاده از این مفاهیم و کاربست آن در حقوق کیفری، از جمله مقررات مربوط به جرایم رایانه‌ای است.

۴-۱. عدم حمایت از بزهدیده سهل انگار[1]

حقوق جزای سنتی چتر حمایتی خود را از بزهدیدگانی که مراقبت‌های لازم را برای پیشگیری از وقوع جرم به عمل نمی‌آورند، برنداشته است. مثلاً اگر فردی تدابیر پیشگیری وضعی را در حراست اموال خود معمول نداشته و اموال او به علت باز بودن درب منزل یا مغازه به سرقت رفته است، تفاوتی با کسی که این تدابیر را به اجرا گذاشته است، ندارد. یعنی عمل انجام شده کماکان قابل مجازات است. به همین ترتیب اگر بازبودن درب منزل او باعث سرقت از منزل همسایه گردد، در صورت فقدان تبانی قبلی هیچ مسئولیتی اعم از مدنی یا کیفری متوجه او نخواهد بود. ولی به دلیل حساسیت‌ها و افتراقات موجود درجرایم سایبری، قانون جزا ممکن است در حالت اول از بزهدیده حمایت نکند و یا در حالت دوم فرد سهل انگار را در مورد بزه‌های رخ داده به نوعی (کیفری-مدنی) مسئول تلقی نماید. یعنی استفاده از تدابیر ایمنی برای کاربران وظیفه تلقی شده و ترک وظیفه قانونی می‌تواند رکن مادی جرم واقع شده محسوب شود.

فرض اول در قانون مجازات اسلامی‌ماده ۷۲۹[1] پیش بینی شده است. در اولین ماده مبحث یکم

1- Negligent Victim

از فصل یکم بخش اول قانون مذکور آمده است: "هر کس به طور غیر مجاز به داده‌ها و سیستم‌های رایانه‌ای یا مخابراتی که به وسیله تدابیر ایمنی حفاظت شده است دسترسی یابد، به حبس از نود ویک روز تا یک سال یا جزای نقدی از پنج تا بیست میلیون ریال یا هر دو مجازات محکوم خواهد شد."

قانون‌گذار در ماده فوق در صورتی عمل مرتکب رابزهکارانه تلقی می‌کند که بزهدیده بالقوه تدابیر امنیتی لازم را به کار بسته باشد. امری که تصور آن در جرایم سنتی در موارد مشابه بعید به نظر می‌رسد. در واقع قانون‌گذار بخشی از هزینه پیشگیری از وقوع جرم را بر دوش افراد گذاشته و حمایت خود را منوط به انجام اقدامات پیشگیرانه کرده است (Javan Jafari,2010). در غیر این صورت نظام عدالت کیفری از آنها حمایت نخواهد کرد. البته فرض دوم مورد بحث، یعنی فراهم کردن زمینه‌های ارتکاب جرم علیه دیگران از طریق سهل انگاری و عدم رعایت تدابیر ایمنی هرچند از بعد نظری قابل طرح است ولی مورد توجه قانون‌گذار قرار نگرفته است.

۴-۲. تعریف اعمال مقدماتی به عنوان جرم تام[۲]

در حقوق کیفری سنتی, پیوستار 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 نظام‌های کیفری به صورت بنیادین، اعمال مقدماتی جرم محسوب نمی‌شوند. در نظام کیفری ما حتی شروع به جرم هم علی الاصول جرم نیست.[۳] در شرایط استثنایی، به علت اهمیت جرم و آثار گسترده جرم خاص ممکن است سیاست کیفری بر این قرار گیرد که شروع به جرم را جرم تلقی نماید و یا در شرایط حادتری اعمال مقدماتی را به عنوان شروع به جرم یا جرم تام تلقی نماید.

۱- قانون مجازات جرایم رایانه ای که طی ۵۴ ماده در سال 2009 به تصویب مجلس شورای اسلامی رسیده بود با نظر مجلس به ادامه قانون مجازات اسلامی اضافه گردید و مواد ۱ الی ۵۴ این قانون به عنوان مواد ۷۲۹ الی ۷۸۲ قانون مجازات اسلامی منظور گردید. روزنامه رسمی ۱۸۷۴۲-2009.

2- Preliminary Acts as Crime

۳- ماده ۴۱ قانون مجازات اسلامی و تبصره‌های آن .همچنین رجوع کنید به: رأی وحدت رویه هیئت عمومی دیوانعالی کشور شماره 635 سال 1999روزنامه رسمی شماره 15889-2000.

در جرایم سایبر به علت آثار گسترده آن، پیچیدگی و صعوبت کشف جرم، شناسایی مجرم و اثبات جرم، سیاست‌گذار کیفری موضع سختگیرانه‌ای اتخاذ نموده و خواسته است جرم را در نطفه خفه نماید. به همین دلیل مقدمات بعیده جرم را نه فقط به عنوان شروع به جرم بلکه به عنوان جرم مستقل تعریف نموده است. ماده ۷۳۲ قانون مجازات اسلامی‌مقرر می‌دارد:

"هرکس به قصد دسترسی به داده‌های سری موضوع ماده ۳ این قانون (داده‌های سری در حال انتقال یا ذخیره شده) تدابیر سیستم‌های رایانه‌ای یا مخابراتی را نقض کند به حبس از ۶ ماه تا ۲ سال یا جزای نقدی از ۴۰ میلیون ریال یا هر دو مجازات محکوم خواهد شد."

۴-۳. گسترش مسئولیت کیفری معاونتی[1]

تحقق معاونت در بزه شرایط متعددی دارد، از جمله این شرایط وجود وحدت قصد میان معاون و مباشر است. فرد در صورتی معاون بزه محسوب می‌شود که با آگاهی از قصد و نقشه بزهکار، با انجام عملی او را در تحقق بزه یاری نماید. یعنی مطابق مصادیق ماده ۴۳ قانون مجازات اسلامی‌او را به سوی ارتکاب بزه سوق داده یا ارتکاب بزه را از ناحیه او تسهیل نماید (Ardabili, 2002).

در واقع هیچ کس به دلیل ارتکاب بزه از ناحیه دیگری مسئول نخواهد بود مگر اینکه با آگاهی از قصد بزهکارانه، او را در راستای تحقق هدفش یاری نماید. از جمله مصادیق سیاست کیفری افتراقی در قانون جرایم رایانه‌ای تحمیل مسئولیت کیفری به فردی است که با بی احتیاطی یا بی مبالاتی موجبات وقوع بزه از ناحیه دیگران را فراهم می‌سازد. این رویکرد از دو جهت افتراقی است اولاً: معاونت غیر عمدی در بزه را محقق می‌داند. ثانیاً: ترک فعل را به عنوان عنصر مادی بزه تلقی نموده است. یعنی فرد بدون آگاهی از ارتکاب بزه از ناحیه دیگری و بدون انجام هرگونه فعل مثبتی، به خاطر عمل دیگری، مسئولیت کیفری را تحمل می‌نماید. ماده ۷۳۳ قانون مجازات اسلامی‌در این باب می‌گوید:

"چنانچه مأموران دولتی که مسئول حفظ داده‌های سری مقرر در ماده۳ (۷۳۱) [2] این قانون یا

1- Accessorial Criminal Liability

۲- لازم بود قانون‌گذار شماره مواد مورد اشاره در متن قانون را نیز اصلاح می‌نمود. به عنوان مثال ماده ۷۳۱ به جای ماده ۳ منظور می‌شد. در سایر موارد نگارنده شماره‌های داخل متن مواد قانونی را به شرح فوق اصلاح خواهد نمود.

سیستم‌های مربوط هستند و به آنها آموزش‌های لازم داده شده است، بر اثر بی احتیاطی، بی مبالاتی یا عدم رعایت تدابیر امنیتی موجب دسترسی اشخاص فاقد صلاحیت به داده‌ها، حامل داده‌ها یا سیستم‌های مذکور شوند، به حبس از نود ویک روز تا دو سال یا جزای نقدی از ۵ تا ۴۰ میلیون ریال یا هر دو مجازات و انفصال از خدمت از شش ماه تا دو سال محکوم خواهد شد."

درست است که محتوای این ماده به نوعی در ماده ۵۰۶ قانون مجازات اسلامی‌نیز آمده است ولی باید توجه داشت که اولاً: ماده مذکور نیز نوعی سیاست کیفری افتراقی در قبال جرایم علیه امنیت است. ثانیاً: در ماده ۵۰۶، مأمور دولت با بی احتیاطی اطلاعات را در اختیار دیگران قرار می‌دهد. در حالی‌که در ماده ۵ مورد بحث، دیگران از بی احتیاطی او استفاده کرده و اطلاعات طبقه‌بندی را به دست می‌آورند. ثالثاً: طرف دریافت کننده اطلاعات در ماده ۵۰۶ دشمن است، در حالی‌که در ماده ۵ مرتکب هرکسی می‌تواند باشد و نهایتاً مجازات‌های مندرج در ماده ۵ قانون جرایم رایانه‌ای شدیدتر از مجازات مندرج در ماده ۵۰۶ قانون مجازات اسلامی‌است. لذا تفاوت‌های دو ماده در نتیجه افتراقی بودن رویکرد برگزیده در قانون جرایم رایانه‌ای محرز است.

۴-۳. وضع جرایم مطلق[1]

جرایم بر مبنای عنصر مادی دو گروه جرایم مقید[2] و مطلق[3] تقسیم می‌شوند. در گروه اول، تحقق نتیجه جزء لاینفک جرم مورد نظر است و بدون وجود نتیجه جرم محقق نمی‌شود. جرایمی مانند قتل، سرقت، کلاهبرداری و اختلاس از این دسته‌اند. ولی جرایم گروه دوم، جرایمی‌هستند که در آنها تحقق نتیجه شرط تحقق جرم نیست و صرف انجام اعمال مادی مورد نظر قانون‌گذار برای شمول عنوان مجرمانه کفایت می‌کند. جرایم مندرج در موارد ۵۰۶ و ۵۰۷ و ۵۰۸ قانون مجازات اسلامی‌در بحث جرایم علیه امنیت از این گروه محسوب می‌شوند.

از جمله دلایل تعریف جرم به صورت مطلق، گزینش رویکرد عدم تسامح در مقابل جرایمی‌است که از حساسیت بیشتری برخوردار بوده و پیامدهای سوء گسترده‌تری دارند. در

1- Conduct Crime
2- result crime
3- conduct crime

قانون مجازات اسلامی‌بخش جرایم رایانه‌ای به دلایل تفصیلی مذکور در قسمت پیشین این نوشتار در راستای رویکردی افتراقی گرایش آشکاری به تعریف جرایم به صورت مطلق نشان داده است. نمونه‌هایی از چنین رویکردی در مواد (۷۲۹) دسترسی غیر مجاز به داده‌های سیستم‌های رایانه‌ای، (۷۳۰) شنود غیر مجاز، (۷۳۲) نقض تدابیر امنیتی داده‌ها و (۷۳۴) جعل رایانه‌ای قابل مشاهده است. در مواد مذکور صرف دسترسی یا شنود غیر مجاز و یا نقض تدابیر امنیتی داده‌ها، فارغ از نتایج احتمالی، استفاده مرتکب با ضررهای احتمالی جرم تلقی شده است.

۴-۵. کاهش عناصر تشکیل دهنده جرم[1]

یکی از وجوه اتخاذ رویکرد افتراقی و البته سختگیرانه کاهش عناصر تشکیل دهنده جرم است. زیرا هر چه تعداد عناصر تشکیل دهنده جرم بیشتر باشد به همان نسبت اثبات جرم مشکل تر و در نتیجه مقابله با مجرمین با محدودیت‌های بیشتری مواجه خواهد بود (Dubber, 2001). مثلاً جرم کلاهبرداری سنتی، جرمی مرکب و مقید است (MirmohammadSadeghi, 2006). عناصر متعددی مانند استفاده از وسایل متقلبانه، فریب دیگری و بردن مال او برای تحقق جرم لازم است. در چنین جرمی‌از طرفی عناصر مادی متعددی باید به اثبات برسند و از طرف دیگر علم و اطلاع، سوء نیت عام و سوء نیت خاص مرتکب در ارتباط با عناصر مادی مذکور باید ثابت گردد. عدم اثبات یا تردید در تحقق هر یک از اجزای رکن مادی یا معنوی جرم مذکور مانعی برای اثبات جرم بوده و به تعبیری مفری برای گریز مرتکب از مجازات خواهد بود. لذا علی‌رغم اصراری که قانون‌گذار در شدت بخشیدن به مبارزه با جرم کالاهبرداری در قانون تشدید مجازات مرتکبین ارتشا، اختلاس و کلاهبرداری[2] دارد، کثرت عناصر مذکور مانعی جدی برای مقابله با جرم کلاهبرداری محسوب می‌شود.

ماده ۷۴۱ قانون مجازات اسلامی‌به جرم کلاهبرداری رایانه‌ای اختصاص یافته است. مقایسه‌ی اجمالی این جرم با کلاهبرداری سنتی بیانگر آن است که عناصر تشکیل دهنده جرم در جرم اولی

1- Reducing Constituent Elements of Crimes

۲- قانون تشدید مجازات مرتکبین ارتشا، اختلاس و کلاهبرداری مصوب سال ۱۳۶۷ مجمع تشخیص مصلحت نظام

در مقایسه با همتای سنتی خود به صورت قابل ملاحظه‌ای کاهش یافته است. مثلاً در ماده مذکور اثری از توسل به وسایل متقلبانه و فریب برای تحقق جرم کلاهبرداری رایانه‌ای دیده نمی‌شود. طبیعی است که در بعد عنصر معنوی نیز اجزای جرم به همین نسبت کاهش می‌یابند.

از طرف دیگر نتیجه‌ی لازم برای تحقق جرم کلاهبرداری سنتی یک مصداق بیشتر ندارد و آن هم بردن مال دیگری است. در حالی که مصادیق نتیجه‌ای جرم کلاهبرداری سایبری توسعه‌ی قابل ملاحظه‌ای داشته است. این نتایج شامل مال، منفعت، خدمات یا امتیازات مالی برای خود و دیگران می‌شود. یعنی از یک سو عناصر تشکیل دهنده‌ی جرم کلاهبرداری سایبری کاهش یافته و از سوی دیگرقانون‌گذار از محدود کردن نتیجه به بردن مال دیگری احتراض نموده و با توسعه مصادیق نتیجه، عملاً آن را به کسب هرگونه امتیاز، منفعت و خدمت گسترش داده است. چنین تحولی در سایه‌ی سیاست کیفری افتراقی و سخت گیرانه قابل توجیه است. زیرا عملا می‌تواند رفتارهای گسترده‌تر و مرتکبین بیشتری را شامل شود.

همان‌گونه که در مقدمه اشاره شد، آنچه در این نوشتار مورد تحلیل قرار گرفت تمامی‌وجوه سیاست کیفری افتراقی مواجهه با جرایم سایبری را شامل نمی‌شود. این تحلیل هم از لحاظ دکترین و هم از نظرگاه قانونی ابعاد گسترده‌تری دارد. با تأمل بیشترابعاد دیگری مانند مسئولیت کیفری افراد حقوقی، مسئولیت کیفری نیابتی و تعریف جرم دارندگی صرف، از بعد تئوریک و قانونی در سایه‌ی رویکرد کیفری گزینشی در مواجهه با جرایم سایبری قابل مطالعه هستند. همانگونه که در مقدمه اشاره شد هدف از ارائه‌ی این مقاله طرح نظریه‌ی سیاست کیفری افتراقی در قبال جرایم دنیای مجازی است. پرداختن به سایر ابعاد این رویکرد به نوشتارهای بعدی موکول می‌شود.

۵. نتیجه

توسعه فناوری اطلاعات و انقلاب الکترونیک به عنوان پدیده تعیین کننده قرن حاضر، تمام ابعاد زندگی اجتماعی را در بر گرفته است. در حوزه حقوق و جرایم علی رغم تلاش‌های صورت گرفته، فضای سایبر هنوز محیطی کنترل نشده، نامنظم و بی قانون توصیف می‌گردد که تقریباً برای همگان قابل دسترسی است. در بعد کیفری، تمایزات کمی‌و کیفی جرایم دیجیتال در مقایسه با جرایم سنتی، کارآیی نظام کیفری متعارف را با چالش‌های جدی مواجه ساخته است؛ به گونه‌ای که اندیشمندان حوزه حقوق و سیاست‌گذاران حوزه‌های مربوطه را وادار به تأمل و اتخاذ تصمیم

نموده است. نکته‌ی بنیادین در حوزه حقوق جزا و سیاست کیفری تفاوت‌های کمی‌و کیفی است که جرایم سایبری با جرایم جهان واقعی دارد. سرعت، کثرت، سهولت ارتکاب، ارزان بودن، فرامرزی بودن، ناشناختگی مرتکب، اتوماتیک بودن جرایم از جمله این تمایزات محسوب می‌شوند. وابستگی روز افزون زیرساخت‌های اقتصادی، صنعتی، خدماتی و فرهنگی و ... از یک سو و آسیب پذیری این زیرساختها به علت وسعت گسترش جرایم سایبری و خطرات گسترده‌ای که این گسترش متوجه زیرساخت‌های مذکور نموده است، از سوی دیگر، مستلزم تدوین سیاست جنایی ویژه‌ای در ابعاد مختلف کنترل، مدیریت، پیشگیری و از جمله حقوق کیفری است.

رسالت نوشتار حاضر بررسی رویکرد افتراقی حقوق کیفری نسبت به جرایم سایبری از نگاه تئوری‌های عمومی‌حقوق جزا بوده است. تمرکز اصلی این پژوهش این بود که در کنار سایر استراتژی‌های خاصی که باید در قبال جرایم دنیای مجازی اتخاذ نمود، تبیین و تدوین رویکرد کیفری افتراقی در بعد ماهوی نیز ضروری است. برای اتخاذ یک سیاست کیفری کارآ و اثربخش به علت تمایزات ویژه‌ی این جرایم لازم است تعریف جرایم، مسئولیت کیفری و تعیین مجازات به گونه‌ای متفاوت انجام شود تا اثر بازدارندگی وپیشگیرانه آن قوی‌تر باشد. در این نوشتار تلاش شد تا برخی از ابعاد مهم رویکرد کیفری افتراقی مورد کنکاش و تحقیق قرار گیرد. عدم حمایت از قربانیان سهل انگار، تعریف اعمال مقدماتی به عنوان جرم تام، گسترش مفهوم مسئولیت کیفری معاونتی، تعریف جرایم به صورت مطلق از جمله محورهای رویکرد کیفری افتراقی در بعد ماهوی می‌باشند که در قانون مجازات اسلامی‌بخش جرایم رایانه‌ای نیز مورد توجه قرار گرفته است.

References:

1- Ahmad Kamal, (2005): "**The Law of Cyber-Space. An Invitation to the Table of Negotiations**". *Published by United Nations Institute for Training and Research.*

2- Ardabili Mohammad Ali., (2002): **"Public Criminal Law**", *first Vol. 3 Ed,Tehran Mizan Publication (in Persian)*

3- Ashori Mohammad., (2007): "**An Introduction to Internet and computer Crimes, New Aspects of Criminallity" Written by Boroman Bastani**, *Behanm Publication Tehran (in Persian)*

4- Brenner Sasan W., (2005): "**Toward a Criminal Law for Cyber Space: Distributed Security**", *vol.10:1. Journal of Science and Technology Law. www.cybercrimes.net.*

5- Coleman, C., & Moynihan, J., (1996): "**Understanding crime data: haunted by the dark figure**", *Open University Press*.
6- Cooter Robert and Thomas Ulen, (2004): "**Law and Economic**" *Harper Collins Publishers.*
7- David Icove J et al,.(1995) : " **Computer crimes: A Crimefighter's Hanbook** *translated by Estarki Akbar et al, Police Unoversity Deputy of Research,2004, Tehran* (in Persian)
8- Dubber Markus D., (2001): "**Criminal Law Policing Possession**: **The War on Crime And The End Of Criminal Law"**, *The Journal of Criminal Law & Criminolog,. Vol.91, N0.4.*
9- Gareth Norris et.al, (2005):" **Contemporary Comment: An Examination of Australian Internet Hate sites"**, *Bond University.*
10- Georgia Tech Information Center, (2009):" Emerging Cyber Threats Reports for"
11- Hasan Baigi Ebrahim, (2005): "**law and Security in Cyberspace**", *Cultural Institution of International Studies and Researches, Abrar Moaser* (in Persian)
12- Hosain Mirmohammadsadeghi (2009): **Offences Against Property**, 15th Ed. Mizan Publication. (in Persian)
13- Javan Jafari Abdolreza, (2009): " **Privitization of Crime Prevention in Iran**" , *The First National conference of Crime prevention, Police Deputy of Education* (in Persian)
14- Javan Jafari Abdolreza(2007): " **Cyber Crimes and New Challenges of Criminal policy***", Law Globalization Conference , Ferdowsi University of Mashhad* (in Persian)
15- Majidi Sayyed Mahmood (2005): **" Diferentiated Criminal Procedure to Crime Against Security and Criminal Policy of Iran and France**, *Pajohesh Quartly, No., 28* (in Persian)
16- Official Newspaper, (1999): No. 15889 (in Persian)
17- Omidi Mehrdad (2010): " **Iran ICT Newes"**
18- Kenneth C.Brancikl (2008). "**Insider Computer Fraud, An in-Depth Framework for Detecting and Definding Insider Attacks**", *Auerbach Publication.*
19- Moore, S. (1996): "**Investigating Crime and Deviance**". *Harpers Collins.*
20- Pilkington, Andy (1995): "**Measuring Crime**". *Sociology Review. November 1995.*
21- Rezaee Ali, (2009 : "**Electronic Commercial Law**", *Mizan Legal Foundatio*n
22- R. Vaca John (2002). Computer Forensics. Computer Crime Scene Investigation. Chorles River Media.
23- Salimi Ali,(2004): " **Crime and Criminology**" *Research Institution of Houzeh and University* (in Persian)
24- Steven Hick et a, l(2006): "**Human Rights and the Internet**", *Macmillan Press Ltd translated by Zamani Ghasem and Bahramlo Mahnaz, Khorsandi Publication,2006 Tehran* (in Persian)

25- Stuart Biegle (2001): " **Beyond our control? Confronting the Limits of Our Legal System in the Age of Cyber Space**". *The MIT Press. Cambridge. Massachusetts. London England.*
26- Thomas A. Johnson, (2005): "**Forensic Computer Crime Investigation"**, *Taylor and Francis Group.*
27- www.kaspersky.com/newszid=207575678.
28- www.Medianews.Ir 89/1/28.

Received: 27, jun , 2010
Accepted: 2 , Nov , 2010