فصلنامهٔ علمی دیدگاه‌های حقوق قضایی
مقالهٔ پژوهشی، دورهٔ ۲۵، شمارهٔ ۹۲، زمستان ۱۳۹۹، صفحات ۳۱۱ تا ۳۳۲
تاریخ دریافت: ۱۳۹۸/۰۲/۲۶ - تاریخ پذیرش: ۱۳۹۹/۱۲/۲۵

تحلیل جرم‌انگاری تولید و پخش نرم‌افزار و ابزارهای الکترونیکی صرفاً مجرمانه در سیاست کیفری ایران در پرتو اسناد فرامرزی

| **محمد یکرنگی*** | استادیار گروه جزا و جرم‌شناسی، دانشکدهٔ حقوق و علوم سیاسی، دانشگاه تهران، تهران، ایران
| **هادی مرسی** | دانشجوی دکتری حقوق جزا و جرم‌شناسی، دانشکدهٔ حقوق، دانشگاه میبد، میبد، ایران

چکیده

جرم‌انگاری و مجازات از مهم‌ترین شیوهٔ دولت‌ها برای مقابله با جرایم روبه‌رشد در فضای سایبر می‌باشد. با نظر به فضای مجازی از دیدگاه حقوق کیفری، می‌توان بیان نمود که این جرم‌انگاری در دو حوزه صورت گرفته است: نخست جرم‌انگاری رفتارهایی که اصالتاً باعث صدمه به دیگران و یا نقض اخلاق می‌شود و دستهٔ دوم رفتارهایی که مقدمهٔ جرایم فوق یا معاونت در آن‌ها می‌باشد. تولید، تهیه، توزیع و نگهداری هر نوع ابزار الکترونیکی که صرفاً به منظور ارتکاب جرایم رایانه‌ای به کار می‌رود، در زمرهٔ این دسته بوده که برخی مصادیق آن در بند الف مادهٔ ۷۵۳ قانون مجازات اسلامی جرم‌انگاری شده است. با وجود سادگی این بند، هنگام اعمال آن، مسائلی پیش می‌آید که نیازمند تدقیق می‌باشد مانند آنکه جهت‌گیری سیاست کیفری ایران در خصوص ابزارهایی که کارایی دوگانه دارند، مفهوم دقیق جرم رایانه‌ای منظور این بند، سوءنیت خاص این جرم و وضعیت نگهداری این ابزارهای مجرمانه چیست. نوشتار حاضر با مطالعهٔ کتابخانه‌ای و به روش توصیفی، تحلیلی و تطبیقی با مطالعهٔ اسناد فرامرزی مانند کنوانسیون شورای اروپا در زمینهٔ جرایم سایبری (بوداپست) ۲۰۰۱ و کنوانسیون عربی مقابله با جرایم تکنولوژی اطلاعات ۲۰۱۰ و استخراج وجوه اشتراک و افتراق آن‌ها

---

* نویسندهٔ مسئول؛ *Email:* Yekrangi@ut.ac.ir

و برپایهٔ اصول حاکم بر حقوق کیفری به تحلیل مادهٔ فوق پرداخته و درصدد یافتن پاسخ‌هایی است که ضمن دارا بودن بنیان نظری، بتواند مسائل عملی را نیز پاسخ‌گو باشد.

واژگان کلیدی: فضای سایبر، نرم‌افزار، جرم‌انگاری، جرم سایبری، ابزار الکترونیکی

مقدمه

فضای سایبر امروزه جزء جدایی‌ناپذیر زندگی انسان‌ها شده است. انسان‌هایی که در دنیای غیرسایبری زیست می‌کنند، هریک دارای هویت یا هویت‌های مستقل در فضای مجازی هستند. هویت‌هایی که پشت نام‌ها و عکس‌های مجازی پنهان شده است و نهایت امری که در این فضا واقعیت دارد، شمارهٔ IP[1] است که فرد را به دنیای سایبر متصل می‌کند. در این دنیای سایبری به‌موازات دنیای غیرسایبری هر امری ممکن است و بر همین اساس نیازمند کنترل.

این کنترل‌ها را می‌توان در یک تقسیم‌بندی کلی به دو دسته تقسیم نمود: اول، کنترل‌هایی که بر روی رفتار اشخاص صورت می‌گیرد و دوم، کنترل‌هایی که بر روی فضا صورت می‌گیرد. ایجاد محدودیت در دسترسی به برخی سایت‌ها در این دسته از کنترل‌ها قرار می‌گیرند. دستهٔ نخست کنترل‌های رفتاری خود در یک تقسیم‌بندی جزئی‌تر به دو دسته تقسیم می‌شوند: کنترل بر روی رفتارهای صدمه‌زننده و دوم، کنترل بر روی رفتارهای که به‌خودی‌خود صدمه‌زننده نیستند ولی می‌توانند زمینه‌ساز جرایم خسارت‌بار شوند. در نمونهٔ نخست رفتارهای صدمه‌زننده در فضای مجازی می‌توان به جاسوسی رایانه‌ای، تخریب رایانه‌ای، سرقت رایانه‌ای و کلاهبرداری رایانه‌ای اشاره نمود. دستهٔ دوم این رفتارها در واقع مقدمات این جرایم هستند که قانون‌گذار آن‌ها را به‌واسطهٔ ورود خسارت جرم‌انگاری نموده است. در واقع، این رفتارها شروع به این جرایم و یا حتی تهیهٔ مقدمات ویا معاونت در این بزه‌ها محسوب می‌شوند. به عبارتی، در این حوزه سیاست کیفری دامنهٔ خود را به رفتارهای ماهیتاً غیرصدمه‌زننده گسترش می‌دهد. مانند موردی که جوان ۲۳ سالهٔ انگلیسی در قبال دریافت پول، نحوهٔ اخذ اطلاعات از سامانه‌های رایانه‌ای را به شرکتی ارائه می‌کرد (طاهری، ۱۳۷۲: ۱۱۷).

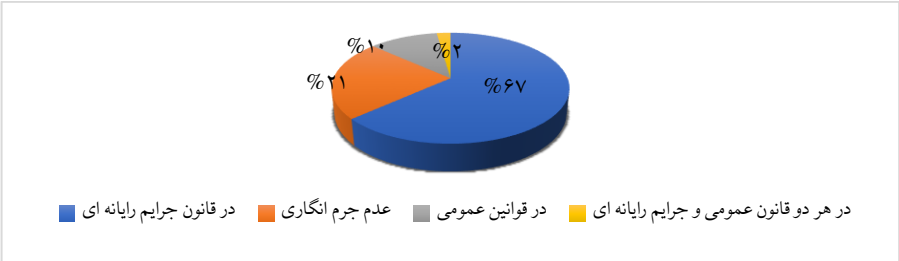
در حوزهٔ حقوق کیفری فناوری اطلاعات، از آنجا که کنترل رفتارهای مجرمانه دشوارتر و آثار ارتکاب جرم نیز به‌دلیل عدم وجود محدودیت‌های فیزیکی و مرزهای سیاسی گسترده‌تر است، کیفرِ صرف رفتارهای صدمه‌زننده بدون مجازات رفتارهای مقدماتی و معاونتی، نمی‌تواند کارایی لازم را در پیشگیری کیفری داشته باشد، لذا، قانون‌گذار اغلب کشورها و اسناد فرامرزی، دایرهٔ حقوق کیفری

---

1. Internet Protocol address

یک بر چسب عددی است که به یک اتصال قابل آدرس‌دهی در اینترنت اختصاص یافته است و فرد را به دنیای سایبر متصل می کند (نک: سینگر، ۱۳۹۴).

را بیش از جرایم عادی گسترش داده‌اند. به همین جهت، این حوزه با شمار بیشتری از جرایمی که پیشگیرانه و یا به اصطلاح مانع هستند، مواجه است. نمونهٔ بارز آن دسترسی غیرمجاز[1] می‌باشد، زیرا صرف ارتکاب آن اثر سوء یا منفی نسبت به داده‌ها و سامانه‌های رایانه‌ای نداشته و همان طور که در بند ۴۴ گزارش توجیهی کنوانسیون بوداپست اشاره شده است، این جرم به عنوان یک جرم مبنایی می‌باشد که امکان تحقق تهدیدهای دیگری از قبیل تخریب داده، اخلال در عملکرد سامانهٔ رایانه‌ای و غیره را که اثرات سوء و منفی بر روی داده‌ها و عملکرد سامانه می‌گذارند، افزایش می‌دهد. یکی دیگر از جرایمی که در این دسته قرار می‌گیرد، بزه تولید، انتشار و توزیع نرم‌افزارها، داده‌ها و یا هر نوع ابزار الکترونیکی است که تنها مصرف مجرمانه دارند. این امر، چنان‌که بیان خواهد شد در برخی اسناد فرامرزی ذکر شده است و در حقوق ایران نیز بیان شده است. این جرم ازجمله بزه‌هایی می‌باشد که هم‌پای جرم دسترسی غیرمجاز به سامانهٔ رایانه‌ای و شنود غیرمجاز، در کشورها جرم‌انگاری شده و شمار زیادی از کشورها در قوانین خود آن را قابل‌کیفر دانسته‌اند. چنان‌که طبق گزارش سازمان ملل، ۶۷ درصد کشورها این جرم را به طور خاص در قانون جرایم رایانه‌ای و ۱۰ درصد در قوانین عام، ۲ درصد در هر دو دسته قوانین ذکر کرده‌اند و حدود ۲۱ درصد کشورها این عمل را به طور مستقل جرم‌انگاری نکرده‌اند. نمودار زیر این امر را نشان می‌دهد (Malby & et al., 2013: 93).



---

۱. این امر در بند ۴۴ گزارش توجیهی کنوانسیون بوداپست که مقرر می‌دارد: دسترسی غیرقانونی شامل جرمی مبنایی می‌شود که تهدیدهای خطرناک و تعرض‌ها علیه امنیت (یعنی محرمانگی، تمامیت و دسترس‌پذیری) سیستم‌ها و داده‌های رایانه‌ای را در برمی‌گیرد. نیاز به حفاظت، منافع سازمان‌ها و افراد در مدیریت، اجرا و کنترل سیستم‌هایشان را بدون وجود مزاحمت و ممانعت بازتاب می‌دهد. صرف تعرض غیرمجاز، یعنی «هک کردن» ، «کرک کردن» یا «ورود به عنف به رایانه» اصولاً و فی‌نفسه باید غیرقانونی تلقی شود. این جرائم می‌توانند موانعی برای کاربران مشروع دستگاه‌ها و داده‌ها ایجاد کنند و تغییرها یا تخریب‌هایی را با هزینه‌های زیاد بازسازی به وجود آورند. چنین تعرض‌هایی می‌تواند باعث دسترسی به داده‌های محرمانه (نظیر گذرواژه‌ها، اطلاعات راجع به سامانه‌های هدف) و اسرار برای استفاده از سیستم بدون پرداخت پول یا حتی تشویق نفوذگرها به ارتکاب اشکال خطرناک‌تری از حملات مرتبط با رایانه، نظیر کلاهبرداری یا جعل مرتبط با رایانه شود» مورد تقنین قرار گرفته است. جهت مطالعهٔ ترجمه متن کنوانسیون و گزارش توجیهی آن (نک: جلالی فراهانی، امیرحسین، ۱۳۹۵).

شمار بالای کشورهایی که این رفتار را جرم دانسته‌اند، نشان از اهمیت این جرم دارد. دلیل این اهمیت آن است که نقش سامانه‌ها در این جرم نه جانبی و یا توسعه‌دهنده بلکه آغازگر و اصلی می‌باشد (کردعلیوند و میرزایی، ۱۳۹۷: ۱۹۵). ایران نیز در زمرهٔ کشورهایی است که این امر را در بند الف مادهٔ ۷۵۳ قانون مجازات اسلامی (مادهٔ ۲۵ قانون جرایم رایانه‌ای)[1] پیش‌بینی نموده است.

با وجود این ماده، بند مذکور هنگام کاربرد در عمل با مسائلی مواجه است که نیازمند تأمل می‌باشد. برای مثال جهت‌گیری قانون‌گذار کیفری ایران در خصوص داده‌ها و یا نرم‌افزارهایی که ماهیت دوگانه داشته و یا نسبت به تولید نرم‌افزارهای صرفاً مجرمانه برای نگهداری و نه استفاده مشخص نمی‌باشد. همچنین مفهوم حقوق کیفری ایران در زمینهٔ حدودوثغور جرایم رایانه‌ای و نیاز به وجود سوءنیت خاص مبهم می‌باشد.

جهت تحلیل مسائل مذکور مطالعهٔ تطبیقی می‌تواند راهگشا باشد، چراکه جرایم رایانه‌ای به‌دلیل آنکه از ضرورت‌های امروز ایجاد شده‌اند و از طرفی گسترهٔ محدود مانند جرایم سنتی ندارند، اغلب در کشورها دارای مقرره‌های مشابه می‌باشند و اسناد فرامرزی نیز برای ایجاد این یکپارچگی تدوین شده‌اند. لذا، در راستای این تحلیل ضروری است که این جرم‌انگاری در اسناد منطقه‌ای بررسی و برخی قیود مذکور در آن‌ها ارزیابی شود و با توجه به این مطالعهٔ تطبیقی اولاً خلأهای موجود در قانون ایران شناسایی و ثانیاً تا حد ممکن قانون ایران به‌گونه‌ای عادلانه و کارا تفسیر شود. در همین راستا، جهت تطبیق مؤثر، مقالهٔ حاضر به صورت موضوعی پیش رفته و ابتدا به موضوع این جرم و سپس به رفتارهای موجد بزه و سوءنیت لازم برای ارتکاب جرم می‌پردازد.

۱. موضوع بزه مرتبط با وسایل غیرقانونی

از منظر حقوق تطبیقی عبارات متفاوتی برای این ابزارها و در نتیجه این جرم استعمال شده است. برخی اسناد مانند گزارش سازمان ملل از عبارت «سوء بهره از وسایل رایانه‌ای»[2] بهره برده (Malby & et al., 2013: 93) و برخی دیگر از اسناد مانند کنوانسیون بوداپست ۲۰۰۱، گزارش HIPCAR برای یکسان‌سازی قوانین در حوزهٔ کارائیب (HIPCAR, 2012: 20) و سند موسوم به «مدل قانونی برای

---

۱. طبق بند الف مادهٔ ۷۵۳ قانون مجازات اسلامی، «هر شخصی که مرتکب اعمال زیر شود، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون (۵/۰۰۰/۰۰۰) ریال تا بیست میلیون (۲۰/۰۰۰/۰۰۰) ریال یا هر دو مجازات محکوم خواهدشد:

الف) تولید یا انتشار یا توزیع و در دسترس قرار دادن یا معاملهٔ داده‌ها یا نرم افزارها یا هر نوع ابزار الکترونیکی که صرفاً به منظور ارتکاب جرائم رایانه‌ای به کار می‌رود.»

2. computer misuse tools

جرایم رایانه‌ای و جرایم مرتبط با رایانه»[1] که برای یکسان‌سازی قوانین کشورهای مشترک‌المنافع تدوین شده است از عبارت «وسایل غیرقانونی»[2] و برخی کتب از عبارت «سوء بهره از وسایل»[3] (Clough, 2010: 120) استفاده کرده‌اند. در حقوق ایران برای این جرم عنوانی انتخاب نشده است و قانون‌گذار در صدر مادهٔ ۷۵۳ قانون مجازات اسلامی با عبارت «سایر جرایم»، به این بزه پرداخته است. با این حال، به نظر می‌رسد از نظر واژه‌گزینی عبارت «بزه مرتبط با وسایل غیرقانونی» مناسب‌تر باشد؛ زیرا چنان‌که بیان خواهد شد این وسایل، برای ارتکاب جرم ایجاد می‌شوند و نه آنکه برای امر دیگر ایجاد شده و از آن‌ها سوءبهره شده باشد؛ به همین جهت، عبارت سوءبهره که ناظر به مواردی است که وسیلهٔ هر دو بهره مثبت و منفی را دارا می‌باشد، با توجه به موضوع این جرم نمی‌تواند گویا باشد.

فارغ از این چالش لفظی، تحلیل موضوع این جرم اهمیت بسزایی دارد. در حقوق کیفری هنگامی که از موضوع جرم بحث می‌شود به طور عمده سه مفهوم می‌تواند اراده شود: نخست، موضوع در معنای ارزش مورد حمایت. برای مثال هنگامی که از موضوع جرایم ضدامنیت و یا علیه مالکیت بحث می‌شود، مقصود از موضوع جرم، ارزش مورد حمایت این بزه‌ها یعنی امنیت و مالکیت مشروع است. دوم، موضوع در معنای امری که متعلَق رفتار قرار می‌گیرد و یا به عبارتی، رفتار بر روی آن صورت می‌گیرد. برای مثال موضوع جرم سرقت در این معنا، مال متعلق به غیر است، زیرا رفتار ربودن نسبت به آن صورت گرفته است و سوم، موضوع در معنای گسترده مدنظر بوده و تمامی شرایط لازم برای جرم را دربرمی‌گیرد. چنان‌که مادهٔ ۱۴۴ قانون مجازات اسلامی هنگامی که از علم به موضوع بحث می‌نماید، این معنا را اراده می‌کند. در متن حاضر از این سه رویکرد، رویکرد دوم مدنظر می‌باشد. بدین معنا که در بزه بند الف مادهٔ ۷۵۳ قانون مجازات اسلامی چه‌چیزی می‌تواند متعلق رفتار باشد.

تمامی اسناد مذکور در فوق، به‌رغم نام‌گذاری‌های متفاوت، «devices» (وسایل) را موضوع این جرم دانسته ولیکن آن را تعریف ننموده و بعضاً تنها مصادیق آن‌ها را بیان نموده‌اند. کنوانسیون بوداپست در بند الف-۱ مادهٔ ۶ بیان می‌دارد: «هر یک از اعضا باید به‌گونه‌ای اقدام به وضع قوانین و سایر تدابیر کنند که در صورت لزوم بر اساس حقوق داخلی خود هر گونه اقدام عمدی و بدون حق[4] زیر را جرم‌انگاری کنند: الف) تولید، فروش، تهیه[5] برای استفاده، وارد کردن، توزیع یا به هر نحو در

1. Model Law on Computer and Computer Related Crime; Thecommonwealth.org. (2019). [online] Available at: http://thecommonwealth.org/sites/default/files/key_reform_pdfs/P15370_11_ROL_Model_Law_Computer_Related_Crime.pdf [Accessed 1 May 2019].
2. Illegal devices
3. misuse of device
4. without right
5. production, sale, procurement

دسترس قرار دادن:۱- یک دستگاه[1]، شامل برنامه رایانه‌ای[2] که اساساً به منظور ارتکاب هر یک از جرایم مندرج در مواد ۲ تا ۵ طراحی یا سازگار شده است.» لذا، طبق این کنوانسیون موضوع این جرم، دستگاه است. این سند برای رفع ابهام و عدم تفسیر مضیق، «برنامهٔ رایانه‌ای» را نیز شامل «دستگاه» دانسته است. اتحادیهٔ اروپا در بند ۷۲ گزارش توجیهی این کنوانسیون، برنامهٔ رایانه را این‌گونه تعریف نموده است:«به برنامه‌هایی گفته می‌شود که برای مثال به منظور تغییر یا حتی تخریب داده‌ها یا مختل کردن عملیات سیستم‌ها، نظیر برنامه‌های ویروسی یا برنامه هایی که به منظور دسترسی به سیستم‌های رایانه‌ای طراحی یا سازگار شده اند به کار می‌رود.» به نظر می‌رسد با توجه به این تعریف، واژهٔ «بدافزار»[3] واژه‌ای مناسب‌تر باشد؛ زیرا از یک‌سو، بدافزارها ابزارهای بدنیتی می‌باشند که به صورت مخفیانه وارد سامانه‌های رایانه‌ای می‌گردند و اعمال مخرب خاص خود را بر روی داده‌ها و سامانه‌های رایانه‌ای به‌منصهٔ ظهور می‌رسانند و منجر به تغییر و تخریب داده‌های رایانه‌ای و یا تضعیف عملکرد سامانه‌ای رایانه‌ای می‌گردند و از سوی دیگر، بر تمامی نرم‌افزارها و سخت‌افزارهای مخرب عنوان «بدافزار» صدق می‌نماید (داوری دولت‌آبادی، ۱۳۹۳: ۶). از طرفی این ابزارها باید به منظور ارتکاب جرایم دسترسی غیرمجاز، شنود غیرمجاز، مختل کردن داده، مختل کردن سامانه به کار رود.

همچنین کنوانسیون عربی مقابله با جرایم تکنولوژی اطلاعات ۲۰۱۰[4]، در بند الف-۱ مادهٔ ۹ بیان می‌دارد: «تولید، فروش، وارد کردن، توزیع یا تهیه: ۱- هر وسیله[5] یا برنامه[6] که به منظور ارتکاب جرایم مذکور در مواد ۶-۸ طراحی شده و یا تغییر یافته باشد.» این کنوانسیون نیز وسیله را تعریف ننموده است ولیکن در بند ۵ ماده ۲ برنامه اطلاعاتی را این‌گونه تعریف کرده است: «دسته‌ای از دستورالعمل‌ها یا فرمان‌ها که می‌تواند به وسیله تکنولوژی اطلاعات اجرا شود و برای دستیابی به منظور خاص باشد.» از طرفی این ابزار باید برای ارتکاب سه جرم دسترسی غیرمجاز، شنود غیرمجاز و جرایم علیه تمامیت داده تولید یا تغییر داده شده باشد. بنابراین این کنوانسیون‌ها در دو امر مشترک می‌باشند: اول، ابزار و برنامه‌های رایانه‌ای را در بر می‌گیرد. لذا شامل سخت‌افزارها و نرم‌افزارهایی که برای ارتکاب جرم به کار می‌رود نیز می‌شود. دوم، تنها برای جرایم رایانه‌ای خاص است.

---

1. device
2. Computer program
3. Malicious software
4. Arab Convention on Combating Information Technology Offences 2010
5. tools
6. programme

در قانون ایران، در خصوص موضوع جرم، مادهٔ ۷۵۳ قانون مجازات اسلامی «داده‌ها یا نرم‌افزارها یا هر نوع ابزار الکترونیکی» را بیان نموده است. در خصوص عبارت نرم‌افزار و ابزار الکترونیکی قانون ایران هم‌سو با اسناد فرامرزی می‌باشد. لیکن ذکر عبارتِ «داده»، در این خصوص کمی مبهم می‌باشد. تنها سند فرامرزی که عبارت داده را همراه وسیله و برنامهٔ رایانه‌ای بیان نمود. مادهٔ III-۲۲ پیش‌نویس کنوانسیون اتحادیهٔ آفریقا در خصوص ایجاد چهارچوب قانونی سازنده در خصوص امنیت سایبری آفریقا[1] است و سایر اسناد در این خصوص مطلبی بیان ننموده‌اند. لذا، بررسی اینکه آیا ضرورتی به ذکر داده در این بند بوده یا خیر ضروری می‌باشد.

داده‌ها مواد خامی هستند که قبل از اینکه به اطلاعات تبدیل شوند، نیازمند طی مراحل و فرایندهایی هستند. به عبارت دیگر، داده‌ها می‌توانند به صورت عدد، متن، گرافیک یا صوت باشند. آنچه دارای اهمیت می‌باشد آن است که داده‌ها جهت پردازش باید به صورتی درآیند که توسط سامانهٔ رایانه‌ای قابلیت پردازش داشته باشند. طبق بند الف مادهٔ ۲ قانون تجارت الکترونیک ایران داده‌پیام این‌گونه تعریف شده است: «هرنمادی از واقعه، اطلاعات یا مفهوم است که با وسایل الکترونیکی، نوری و یا فناوری‌های جدید اطلاعات تولید، ارسال، دریافت،ذخیره یا پردازش می‌شود.» کنوانسیون بوداپست نیز تعریف مشابهی از داده در بند ب مادهٔ ۱ بیان داشته و مقرر نموده است: «هرگونه نماد حقایق، اطلاعات یا مفاهیم به شکلی مناسب برای پردازش در یک سیستم رایانه ای، شامل برنامه‌ای که برای کارکرد یک سیستم رایانه‌ای مناسب است.» بنابر این تعاریف، برنامه‌ها که شامل نرم‌افزارها می‌شود نیز با داده فعالیت می‌کند؛ لذا، نرم‌افزارها و ابزار الکترونیکی چنان‌که در تعریف کنوانسیون عربی مقابله با جرایم تکنولوژی اطلاعات ۲۰۱۰ ذکر شده است، توسط دستورالعمل‌ها و فرمان‌ها عمل می‌کنند که این موارد خود داده محسوب می‌شوند. بنابراین تصور نرم‌افزار بدون داده از نظر فنی محال می‌باشد.[2] به همین جهت ممکن است در بادی امر، به نظر رسد عبارت داده، در مادهٔ مذکور زاید می‌باشد. با این حال، به نظر می‌رسد، کدهای مخربی که برنامه‌نویسان از آن‌ها برای تولید بدافزارها استفاده می‌کنند را می‌توان تحت عنوان داده‌های مخرب قرار داد، علت اول اینکه این داده‌ها منجر به تولید یک بدافزار

---

1. Draft African Union Convention on the Establishment of A Legal Framework Conducive to Cyber Security in Africa

۲. تعریف نرم‌افزار از دیدگاه علوم فناوری و اطلاعات چنین می‌باشد: «نرم افزار کامپیوتری، محصولی است که مهندس نرم افزار طراحی می‌کند و می‌سازد. شامل برنامه‌هایی می‌شود که در کامپیوتری به هر اندازه و با هر معماری، قابل اجرا هستند، مستنداتی دارد که شامل فرم‌های واقعی و مجازی می‌شود و داده‌هایی دارد که ترکیبی از ارقام و حروف است و البته می‌تواند شامل اشکال نمایشی از قبیل اطلاعات تصویری و ویدئویی و صوتی می‌باشد» (نک: پرسمن، ۱۳۹۳: ۱۳).

می‌شوند و دوم اینکه تا زمانی در محیط برنامه‌نویسی قرار نگیرند، فاقد عملیات اجرایی می‌باشند و صرفاً به صورت مجموعه‌ای از حروف و کاراکترها می‌باشند. به عنوان مثال در بسیاری از سایت‌ها کدهای مخربی وجود داشته که با وارد نمون آنان در محیطی مانند (notepad) و ذخیرهٔ آن با پسوندهایی مانند «INF» یا «BAT» یک بدافزار ساخته خواهد شد. بنابراین، صرف این داده‌ها می‌تواند موضوع این جرم باشد و از این منظر حقوق ایران صحیح عمل نموده است. از طرفی، نمونهٔ بارز نرم‌افزارهای شامل این ماده می‌توان به بمب منطقی[۱]، اسب تراوا[۲]، ویروس‌ها[۳]، کرم‌ها[٤] و غیره اشاره نمود که بر تمامی آنان عنوان بدافزار صدق می‌کند (جهت مطالعهٔ بیشتر نک: آیوک، ۱۳۹۱: ۲۷-۲۳). بدافزارها در یک تقسیم‌بندی کلی به دو دسته تقسیم می‌شوند: بدافزارهای مستقل که بدون نیاز به برنامه‌های دیگر فعال می‌شوند مانند کرم‌ها و تروجان‌ها و بدافزارهای نیازمند میزبان که نیاز به آن دارند به برنامهٔ دیگری چسبیده و همراه آن‌ها اجرا شوند، مانند ویروس‌ها و غیره. (آیرک، ۱۳۹۱: ۶) مادهٔ ۷۵۳ قانون مجازات اسلامی هر دو دستهٔ این بدافزارها را در بر می‌گیرد. همچنین در این خصوص میان بدافزارهایی که بلافاصله اجرا می‌شوند، مانند ویروس‌ها و کرم‌ها و تروجان‌ها و بدافزارهایی که نیازمند راه‌انداز یا ماشه دارند مانند بمب منطقی، تفاوتی وجود ندارد.

---

۱. یک بمب منطقی خودش را منتشر نمی‌کند، اما بر روی یک سیستم نصب شده و منتظر می‌ماند تا یک رویداد خارجی مانند ورودی داده، رسیدن به یک تاریخ خاص، ایجاد، حذف یا حتی تغییر یک فایل خاص حادث گردد تا منجر به آسیب رساندن به سیستم رایانه‌ای گردد. نک:

Rehman, Rizwan, G. C. Hazarika, and Gunadeep Chetia. (2011), "Malware threats and mitigation strategies: a survey". Journal of Theoretical and Applied Information Technology, vol. 29.2, 69-73.

۲. یک نوع بدافزار که به شکل قطعاتی از کدهای نرم‌افزاری ظاهر می‌شود و برای اهداف مفید در نظر گرفته شده است. این کار دستورات مورد نظر را برای کاربران اجرا می‌کند اما مخفیانه یک سری اقدامات در کنار آن اجرا می‌کند. نک:

Egele, Manuel, et al.(2012), "A survey on automated dynamic malware-analysis techniques and tools". ACM computing surveys (CSUR), vol.44.2.

۳. ویروس رایانه‌ای کد مخرب رایانه‌ای است که توانایی کپی‌سازی از خود و گسترش نمونه‌های مختلف از خود را به داخل کدهای قابل اجرای دیگر یا اسناد رایانه‌ای، شبکه و نرم‌افزارهای رایانه‌ای داراست..

٤. کرم‌ها برخلاف ویروس‌ها برنامه‌های متکی به خود هستند و بدون نیاز به سایر برنامه‌ها فعالیت دارند؛ کرم‌ها به راحتی تکثیر یافته و رایانه‌های متصل به شبکه را آلوده می‌نماید، لذا نمی‌تواند در خارج از شبکه برای مثال از طریق یک دیسکت گسترش پیدا کند. آن‌ها در یک رایانه مقیم می‌شوند و فضای رایانه را اشغال می‌کنند تا آنکه رایانه کند شود و یا از کار بیافتد (نک: آنجلیز، ۱۳۸۳: ۳۶). بنابراین «کرم یک عامل خودمختار است که از طریق خودش تکثیر می‌شود در حالی که ویروس خود را به نرم‌افزارها می‌چسباند و با اجرای آن نرم‌افزار تکثیر می‌شود.» (نک: ضیایی‌پرور، ۱۳۸۳: ۱۹۷).

در کنار داده‌ها یا نرم‌افزارها، ابزارهای الکترونیکی موضوع سوم این بزه می‌باشد. این ابزارها از تسلیحات پالس الکترومغناطیسی[1] تأثیر می‌پذیرند و می‌توان با استفاده از آنان در فرایند ارسال و انتقال سیگنال‌ها اختلال ایجاد کرد و یا اینکه سیگنال‌های متصاعد شده از ابزارهای الکترونیکی را شنود نمود (مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر، ۱۳۹۱: ۲۲۳). همچنین ابزارهای الکترونیکی قادر خواهند بود با ایجاد تشعشعات متغیر جهت جذب انعکاس و پخش امواج الکترومغناطیسی سبب تغییر در اطلاعات دریافتی از طریق سیستم‌های الکترونیکی مربوطه گردند که در اصطلاح اقدام انجام شده را «فریب الکترونیکی» می‌نامند.[2]

مشهورترین اثر مخرب ناشی از ابزارهای الکترونیکی نویزها یا همان پارازیت‌ها می‌باشند. پارازیت‌ها سیگنال‌های الکتریکی ناخواسته‌ای می‌باشند که به صورت طبیعی یا توسط مدارهای الکتریکی کیفیت سیگنال‌ها و کارایی کانال ارتباطی میان آنان را کاهش می‌دهند که به دو دستهٔ کلی پارازیت‌های عمدی[3] و غیرعمدی[4] تقسیم می‌گردند.

وجود قید (هر نوع) در مادهٔ ۷۵۳ قانون مجازات اسلامی، قرینه‌ای بر صحت این مدعاست که هر دستگاه سخت‌افزاری توانایی ایجاد پارازیت یا فریب الکترونیکی و... داشته باشد در شمول این بند قرار خواهد گرفت.

۲. مفهوم «کاربرد انحصاری» ابزار صرفاً مجرمانه

قید مهمی که بند الف مادهٔ ۷۵۳ قانون مجازات اسلامی به این ابزارها وارد نموده آن است که ضروری است ابزارها «صرفاً» به منظور «ارتکاب جرایم رایانه‌ای» به کار رود. مادهٔ ۷۵۳ قانون مجازات اسلامی از آنجا که در فصل هفتم این قانون ذکر شده و قانون‌گذار تمامی جرایم ماهوی را در فصل‌های اول تا پنجم ذکر نموده است، این سؤال را مطرح می‌سازد که آیا مقصود از «جرایم رایانه‌ای» مذکور در این بند، همهٔ این جرایم اعم از جرایم رایانه‌ای محض و جرایم مرتبط با رایانه

---

1. Electoromagnetics Puls

2. http://pptdl.ir/downloads.aspx?code=71833171401378318411, p.6.

۳. پارازیت‌های عمدی به سه دسته تقسیم می‌گردند: یک، پارازیت نقطه‌ای که در آن نیروی مؤثر مولد فرستنده را روی یک فرکانس گیرنده متمرکز می‌گردد دو، پارازیت سدی که در آن نیروی مولد فرستنده در باند وسیع فرکانس‌های گیرنده پخش می‌گردد سوم، پارازیت متغیر. نک:

http://pptdl.ir/downloads.aspx?code=71833171401378318411, p.8.

٤. پارازیت‌های غیرعمدی به دو دسته تقسیم می‌گردند: یک، پارازیت طبیعی مانند رعد و برق و اختلالات جوی و ایجاد پدیده فادینگ دو، پارازیت مصنوعی مانند القا تشعشعات و جرقه‌ها و میدان‌های ناشی از موتورهای احتراقی، کارخانجات برق و غیره. نک:

http://pptdl.ir/downloads.aspx?code=71833171401378318411, p.7.

است و یا تنها جرایم رایانه‌ای محض را شامل خواهد شد که در فصول اول و دوم قانون جرایم رایانه‌ای ذکر شده است. هر دو شق دارای وجه است. دلیل گرایش به نظر نخست را می‌توان از طریق تفسیر یکپارچه برداشت نمود. مادهٔ ۷۴۷ قانون مجازات اسلامی (۱۹ قانون جرایم رایانه‌ای) در مقام بیان مسئولیت کیفری اشخاص حقوقی بیان می‌دارد: «در موارد زیر، چنانچه جرایم رایانه‌ای به نام شخص حقوقی و در راستای منافع آن ارتکاب یابد، شخص حقوقی دارای مسئولیت کیفری خواهد بود». در این ماده «جرایم رایانه‌ای» بدون شبهه تمامی جرایم مذکور در آن قانون، ازجمله کلاهبرداری رایانه‌ای و پخش محتوای مستهجن را در بر می‌گیرد و شبهه در خصوص سرایت این ماده به سایر جرایم رایانه‌ای خارج از این قانون مانند جرایم مذکور در قانون نحوهٔ مجازات کسانی که در امور سمعی و بصری فعالیت غیرمجاز می‌کنند، است. بنابراین عبارت «جرایم رایانه‌ای» مذکور در مادهٔ ۷۴۷ قانون مجازات اسلامی نسبت به شمول تمامی جرایم مذکور در قانون جرایم رایانه‌ای عام است و طبق اصل تبعیت قانون‌گذار از منطق و اینکه این عقلانیت مقنن مستلزم آن است که یک واژه را در یک قانون در دو معنا به کار نبرد، عبارت جرایم رایانه‌ای مادهٔ ۷۵۳ قانون مجازات اسلامی نیز در معنای عام که شامل همهٔ جرایم مذکور در آن قانون می‌شود به کار رفته است.

از طرفی دیگر، در مقابل نظر نخست دیدگاه دیگری مبنی بر اینکه این ابزارها تنها ناظر به جرایم رایانه‌ای محض است، وجود دارد با این استدلال که اول، کنوانسیون‌های بین‌المللی که راهبری تدوین این قانون را داشته‌اند این جرم را منحصر به جرایم رایانه‌ای محض نموده‌اند و دوم، از نظر فنی نیز این نرم‌افزارها و ابزارها زمانی می‌توانند برای ارتکاب جرم به کار روند که موضوع جرم داده و یا سامانه باشد. در حالی که در جرایم مرتبط با رایانه موضوع جرم مال یا منفعت و یا محتوا و... می‌باشد؛ زیرا هر نرم‌افزاری که بتواند محتوای غیرقانونی را پخش کند می‌تواند محتوای قانونی را نیز پخش نماید. لذا، این جرایم توسط رایانه ارتکاب می‌یابد. به همین جهت به نظر می‌رسد طبق این نظر، مقصود از جرایم رایانه‌ای در این بند، جرایمی می‌باشد که در آن داده و سامانهٔ موضوع جرم هستند و شامل دسترسی و شنود غیرمجاز، تخریب و اخلال در داده و سامانه و ممانعت از دسترسی به آن‌ها و جعل رایانه‌ای، سرقت رایانه‌ای و استفادهٔ غیرمجاز از پهنای باند بین‌المللی می‌باشد.[۱]

با این حال، در مقام گزینش بین این دو نظر می‌توان بیان داشت که اسناد فراملی، پیشنهادهای حداقلی برای جرم‌انگاری ارائه می‌نمایند ولیکن کشورها در صورت لزوم، می‌توانند با توجه به‌دلیل خود،

---

۱. جاسوسی رایانه‌ای اگر چه در مادهٔ ۷۳۱ قانون مجازات اسلامی ذکر شده است، لیکن چون ماهیت رفتاری آن دسترسی غیرمجاز و شنود غیرمجاز است و تنها دادهٔ آن دارای ویژگی سری است و تفاوت ماهوی با دو جرم فوق ندارد، در این متن ذکر نشده است.

این جرم‌انگاری‌ها را توسعه دهند؛ چنان‌که در این اسناد پورنوگرافی منحصر به افراد زیر ۱۸ سال شده است، لیکن ایران این جرم‌انگاری را در مادهٔ ۷۴۲ قانون مجازات اسلامی گسترش داده و هر نوع توزیع و پخش محتوای مستهجن را جرم‌انگاری نموده است. در این مورد نیز به نظر می‌رسد با توجه به سیاق عبارات به کار رفته در بند الف مادهٔ ۷۵۳ قانون مجازات اسلامی و تفسیر منسجم قانون، می‌توان بیان نمود استدلال‌های گروه نخست اقوی بوده و این ماده تمامی جرایم رایانه‌ای را در بر می‌گیرد.

قید دوم که در بند الف مادهٔ ۷۵۳ قانون مجازات اسلامی به کار رفته است قید «صرفاً» می‌باشد. ذکر این قید که نوعی تخصیص را شامل می‌شود، باعث می‌شود ابزارهایی که تنها و تنها برای ارتکاب جرم تولید یا منتشر نمی‌شوند، از شمول ماده خارج گردند، لازم به ذکر است «تشخیص اینکه نرم‌افزار یا ابزار خاصی اختصاصاً در ارتکاب جرایم رایانه‌ای کاربرد دارد یا خیر، با اخذ نظر کارشناسان و خبرگان امور رایانه‌ای صورت می‌گیرد.» (محمدنسل، ۱۳۹۵: ۱۸۰). در واقع این قید ابزارهای الکترونیکی و نرم‌افزارها و برنامه‌های دومنظوره را خارج می‌نماید. بنابراین، در صورتی که نرم‌افزاری تولید شود که صرفاً امکان دانلود محتوای مستهجن از این سایت‌ها را داشته باشد، می‌تواند موضوع این بند قرار گیرد. در مقابل‌نرم‌افزاری مانند مرورگر که توسط آن علاوه بر امکان دانلود محتوای مستهجن، امکان دانلود مطالب آموزشی و علمی و فرهنگی وجود دارد به‌واسطهٔ وجود قید «صرفاً مجرمانه» از شمول این بند خارج می‌باشد.

این امر در زمان تصویب کنوانسیون بوداپست نیز مطرح بود و کنوانسیون در یک عبارت کلی‌تر از واژهٔ «اساساً»[1] بهره برد و در گزارش توجیهی خود بیان داشت: «کنوانسیون به عنوان یک تعهد جمعی متعارف، حوزه خود را به دستگاه‌هایی محدود کرده که نوعاً به قصد ارتکاب جرم طراحی یا سازگار شده باشند. این شرط معمولاً به تنهایی دستگاه‌های دومنظوره را خارج می‌سازد.» لذا، هرچند این کنوانسیون منعطف‌تر برخورد نموده است ولیکن ذکر عبارت «عموماً» یا »اساساً» یا «نوعاً» در قانون کیفر نمی‌تواند صورت پذیرد. زیرا مفهوم آن بسیار سیال شده و نمی‌توان مرز مشخصی برای ابزارها و یا نرم‌افزارهایی که کاربرد دوگانه دارند، تعیین نمود. ضمن آنکه مشخص نمی‌باشد در صورت بهره از واژهٔ عموماً یا نوعاً، معیار احراز نوع افراد جامعه است و یا متخصصین حوزهٔ سایبر.

از طرفی دیگر، قید «صرفاً»، باعث می‌شود حوزهٔ این جرم بسیار محدود شده و در مواردی که حتی کوچک‌ترین کاربرد غیرمجرمانه‌ای برای این ابزارها شناسایی شود، از حوزهٔ این بزه خارج شود. بنابراین، این امر مفرّی برای مجرمین خواهد شد. زیرا آنان هنگام طراحی و تولید یک نرم‌افزار یا برنامهٔ مجرمانه یک کاربرد مثبت به آن می‌افزایند تا از این ماده رهایی یابند. مانند آنکه نرم‌افزاری در

---

1. primarily

جهت تخریب یا سرقت داده‌ها تولید نموده و کابرد دیگری مانند نشان دادن ساعت یا تعیین وقت و یا تبدیل تاریخ شمسی به قمری برای آن تعریف کرده تا نرم‌افزار طراحی شده صرفاً مجرمانه تلقی نگردد. برای رهایی از این امر، به نظر می‌رسد قید صرفاً را می‌توان ناظر به «قصد مرتکب در ترکیب با ویژگی وسیله یا برنامهٔ رایانه‌ای» و یا «هدف اصلی تولید آن» دانست. بدین معنا که اگر هدف از تولید برنامه یا نرم‌افزار صرفاً مجرمانه بوده، هرچند در عمل برای پوشش، کاربردهای دیگر برای آن تعریف کرده باشد، می‌توان آن برنامه یا نرم‌افزار را شامل این بند دانست. به نظر می‌رسد عبارت گزارش توجیهی کنوانسیون بوداپست مبنی بر اینکه «تنها معیار شخصی، قصد ارتکاب جرم رایانه‌ای است که اعمال مجازات را قطعیت می‌بخشد» همین امر است. با این حال، زمانی که نتوان کارکرد مجرمانه را بر کارکرد غیرمجرمانه به طور یقینی ترجیح داد، نمی‌توان شخص را محکوم به این جرم نمود. به همین جهت، مواردی مانند مرورگرها که توسط آن علاوه بر امکان دانلود محتوای مستهجن، امکان دانلود مطالب آموزشی و علمی و فرهنگی وجود دارد به‌واسطهٔ وجود قید «صرفاً مجرمانه» از شمول این بند خارج می‌باشد.

۳. عنصر مادی و روانی بزه مرتبط با وسایل غیرقانونی

هیچ جرمی بدون ارتکاب رفتار ممکن نمی‌باشد. در واقع رفتار که در حقوق انگلستان از آن به بدنهٔ جرم یا عنصر فیزیکی جرم یاد می‌نمایند (Jefferson, 2009, 91; Molan, 2005: 474) بزه حاضر نیز با توجه به رفتارهایی که محقق آن می‌باشد، می‌تواند دو قسمت گردد: نخست، تولید و انتشار و توزیع که از آن در این نوشتار به عنوان رفتارهای فعال در بزه مرتبط با وسایل غیرقانونی یاد می‌شود و دوم، نگهداری که از آن به عنوان رفتار منفعل این جرم یاد می‌شود. علت نام‌گذاری آن است که در سه رفتار تولید، انتشار و توزیع فرد عملی را انجام می‌دهد و نقش وی فعالانه است ولی در نگهداری صرفاً در یک وضعیت قرار دارد و رفتار وی فعال نبوده و منفعل می‌باشد که هر دو رفتار در بندهای آتی مورد تدقیق قرار خواهد گرفت.

۱-۳. رفتارهای فعال در بزه مرتبط با وسایل غیرقانونی و رکن روانی مرتبط با آن

جرم وسایل غیرقانونی، جرمی فعلی است بدین معنا که با ترک فعل قابل‌تحقق نمی‌باشد. برای تحقق این جرم، کنوانسیون بوداپست سه فعل را به‌طور خاص مشخص نموده است که عبارتند از: «تولید»، «فروش»، «تهیه». کنوانسیون عربی مقابله با جرایم تکنولوژی اطلاعات ۲۰۱۰ نیز پنج فعل را پیش‌بینی نموده که عبارتند از: «تولید»، «فروش»، «وارد کردن»، «توزیع» یا «تهیه». قانون جرایم رایانه‌ای در بند الف مادهٔ ۷۵۳ قانون مجازات اسلامی نیز تولید یا انتشار یا توزیع و در دسترس قرار دادن یا معاملهٔ این ابزارها را به عنوان جرم مستقل جرم‌انگاری نموده است و مرتکبان آن به عنوان

مباشر جرم مجازات می‌گردند. در توجیه جرم‌انگاری بند الف مادهٔ ۷۵۳ قانون مجازات اسلامی بیان شده است: «همان طور که در حقوق سنتی جرایمی وجود دارند که از آن‌ها به‌عنوان جرایم مانع یاد می‌کنیم، در حقوق کیفری رایانه‌ای نیز با چنین جرایمی مواجه هستیم. به عنوان مثال در قانون مجازات اسلامی جرمی همانند ساختن کلید و وسایلی که در سرقت به کار می‌روند و همچنین حمل اسلحه به طور مستقل جرم‌انگاری شده‌اند، چراکه این قبیل اقدامات می‌توانند مقدمهٔ جرایم دیگری همچون سرقت و قتل باشند؛ فلسفهٔ جرم‌انگاری اعمال تولیدکنندگان برنامه‌های مخرب نیز به همین شکل است زیرا اعمالی این چنینی می‌تواند مقدمه‌ای باشد برای جرایم سنگین‌تر مانند تخریب رایانه‌ای» (نادرخانی، ۱۳۹۰: ۵۶-۵۶).

بدیهی است منظور از تولید در بند الف مادهٔ ۷۵۳ قانون مجازات اسلامی، ساخت و طراحی هر نوع بدافزار می‌باشد (عزیزی، ۱۳۹۴: ۱۸۸). نکته‌ای که لازم است بدان توجه داشت آن است که امروزه کاربران قادرند با نرم‌افزارهایی که توسط دیگران جهت ساخت و طراحی بدفزارها تولید می‌گردند، یک بدافزار جدیدی را تولید نماید. مانند حالتی که نرم‌افزاری تولید می‌شود که تنها با ورود یک کد یا یک فایل نوعی بدافزار دیگر از این بدافزار نخست تولید می‌گردد. به نظر می‌رسد در این‌گونه موارد رفتار سازندهٔ نرم‌افزار و رفتار کاربرانی که توسط آن نرم‌افزار بدافزاری را تولید می‌کنند، تحت رفتارهای معاونتی بند الف مادهٔ ۷۵۳ قانون مجازات اسلامی قرار می‌گیرند و نمی‌توان اولی را معاون در جرم ارتکابی مادهٔ ۷۵۳ قانون مجازات اسلامی دومی دانست. زیرا هر دو رفتار مشمول بند نخست این ماده می‌شوند.

با بررسی اسناد فرامرزی در زمینهٔ رکن روانی مشخص می‌گردد در حوزهٔ سایبری دو گرایش در خصوص این جرم وجود دارد: گرایش اول این جرم را بزه عمدی دانسته و ارتکاب آن به صورت غیرعمد را ممکن نمی‌داند. این گرایش غالب بوده و در کنوانسیون‌های فوق‌الذکر از این گرایش پیروی شده است. در گرایش دوم، این جرم به صورت عمد و یا غیرعمد قابل‌تحقق است. برخی اسناد مانند سند موسوم به «مدل قانونی برای جرایم رایانه‌ای و جرایم مرتبط با رایانه»[1] برای یکسان‌سازی قوانین کشورهای مشترک‌المنافع این امر را پیش‌بینی کرده‌اند. طبق بند الف-۱-۹ این سند «شخص مرتکب جرم خواهد شد اگر آن شخص: الف) قاصدانه یا از روی بی‌احتیاطی، بدون عذر یا توجیه قانونی، برای استفاده، وارد کردن، صادر کردن، توزیع یا غیر از این موارد در دسترس قرار دادن مبادرت به

1. Model Law on Computer and Computer Related Crime; Thecommonwealth.org. (2019). [online] Available at: http://thecommonwealth.org/sites/default/files/key_reform_pdfs/P15370_11_ROL_Model_Law_Computer_Related_Crime.pdf [Accessed 1 May 2019].

تولید، فروش، تهیه موارد ذیل نماید: ۱- ابزاری شامل برنامه رایانه‌ای که به منظور ارتکاب جرایم مواد ۵، ۶، ۷ یا ۸ طراحی یا تغییر داده شده است.»

گرایش نخست خود دو دسته می‌شود: اول، تنها رفتار را فارغ از اینکه به چه قصدی باشد جرم‌انگاری نموده است. مانند کنوانسیون عربی مقابله با جرایم تکنولوژی اطلاعات ۲۰۱۰ دوم، صرف ارتکاب رفتار با سوءنیت عام جرم نمی‌باشد بلکه سوءنیت خاص نیز لازم است مانند کنوانسیون بوداپست ۲۰۰۱.

قانون‌گذار ایران از میان این موارد جرم را عمدی و بدون سوءنیت خاص پیش‌بینی نموده است. در مقام تحلیل این گرایش به نظر می‌رسد از نظر عمدی بودن قانون جرایم رایانه‌ای صحیح عمل نموده است. زیرا در سیستم‌های تابع حقوق نوشته اصل بر عمدی بودن جرایم می‌باشد و به عبارتی اشخاص علی‌الاصول تنها برای رفتارهایی که عالمانه و قاصدانه مرتکب شده‌اند، کیفر خواهند شد. در حقوق کیفری ایران نیز پیش‌بینی جرایم غیرعمد با عنصر تقصیر جزایی در تعزیرات، برای جرایم بسیار مهم می‌باشد مانند جاسوسی و یا جرایمی که به تمامیت جسمانی افراد صدمه می‌زند و علی‌الاصول پیش‌بینی عنصر روانی تقصیر برای جرمی که خود بزه مانع جرایم سایبری عدول بلاوجه از اصل کلی می‌باشد. بر این اساس، مادهٔ ۷۵۳ قانون مجازات اسلامی با عمدی دانستن بزه، راه صوابی را پیموده است.

لیکن از نقطه‌نظر پیش‌بینی سوءنیت خاص، موضوع کمی پیچیده‌تر می‌باشد. قاعدهٔ کلی در حقوق کیفری آن است که جرایم مقید نیازمند سوءنیت خاص بوده و جرایم مطلق طبق اصل کلی نیازمند این سوءنیت برای تحقق نمی‌باشند و از آنجا که این جرم، مطلق می‌باشد، نیاز به سوءنیت خاص نمی‌باشد. لیکن، قانون در بسیاری از موارد به ویژه در جرایم مطلقی که جنبهٔ پیشگیرانه دارد، انگیزه و یا سوءنیت خاص را برای مضیق نمودن محدودهٔ جرم‌انگاری پیش‌بینی کرده است. در خصوص بند الف مادهٔ ۷۵۳ قانون مجازات اسلامی درصورتی‌که جرم را بدون سوءنیت خاص تلقی نماییم، این نتیجه حاصل می‌شود که شخص به صرف تولید یک نرم‌افزار صرفاً مجرمانه، حتی اگر برای تفنن باشد، قابل‌تعقیب کیفری خواهد بود. برای مثال در صورتی که فردی مرتکب جرمی شده و مقام قضایی دستور توقیف یا تفتیش سامانهٔ رایانه‌ای را طبق مادهٔ ۶۷۱ قانون آیین دادرسی کیفری صادر نماید و در حین تفتیش ناگهان به نرم‌افزاری این چنینی برخورد شود، می‌توان سریعاً به مقام قضایی اطلاع داد و فرآیند تحقیق و تعقیب و محاکمه انجام خواهد شد. در حالی که این امر غیرمعقول خواهد بود. زیرا این امر گسترش خلاف اصل حقوق جزا به اقدامات بعیدهٔ جرم خواهد بود و مقنن باید توجیه مناسبی برای گسترش تا این اندازه موسع حقوق کیفری داشته باشد. در حالی‌که

هیچ یک ار نظریه‌های جرم‌انگاری اعم از اصل ضرر، پدرسالاری، اخلاق‌گرایی قانونی نمی‌تواند توجیه‌گر این جرم‌انگاری موسع باشد. به همین دلیل، کنوانسیون بوداپست سوءنیت خاصی را برای این جرم پیش‌بینی نموده است که عبارت است از اینکه تولید، فروش و تهیه برای استفاده، وارد کردن، توزیع یا به هر نحو در دسترس قرار دادن این ابزارها باشد. لذا با این قید، صرف تولید و تهیه جرم نمی‌باشد مگر آنکه به قصد استفاده یا توزیع یا در دسترس قرار دادن باشد. به همین دلیل مناسب است قانون‌گذار ایران نیز سوءنیت خاص را پیش‌بینی کرده و بیان دارد: «تولید و تهیهٔ داده‌ها یا نرم‌افزارها یا هر نوع ابزار الکترونیکی که صرفاً به منظور ارتکاب جرایم رایانه‌ای به کار می‌رود به منظور استفاده، توزیع، انتشار و در دسترس قراردادن.» در تبیین مفهوم توزیع و در دسترس قرار دادن، بند ۷۲ گزارش توجیهی کنوانسیون بوداپست بیان می‌دارد: «منظور از توزیع ارسال فعالانه داده‌ها به دیگران است، در حالی که در دسترس قرار دادن، به قرار دادن بر خط دستگاه‌ها جهت استفاده دیگران اطلاق می‌شود.» در مادهٔ ۷۵۳ قانون مجازات اسلامی، نیز می‌توان توزیع را به معنای ارسال فعالانه و مشخص این ابزارها و در دسترس قرار دادن را به معنای پخش برخط و عمومی بدون آنکه مخاطب مشخصی مد نظر باشد، در نظر گرفت.

۲-۳. رفتار منفعل در بزه مرتبط با وسایل غیرقانونی و رکن روانی مرتبط با آن

علاوه بر رفتارهای فوق که در بند الف مادهٔ ۷۵۳ قانون مجازات اسلامی ذکر شده است، برخی کنوانسیون‌ها از رفتار «نگهداری» هم یاد کرده‌اند. لیکن این رفتار را از موارد فوق جدا نموده‌اند. برای مثال کنوانسیون بوداپست ۲۰۰۱ در بند ۱-ب مادهٔ ۶ به این جرم پرداخته و بیان می‌دارد: «نگهداری هر یک از موارد مندرج در بندهای الف۱ یا ۲ فوق، با قصد استفاده از آن‌ها جهت ارتکاب هر یک از جرایم مقرر در مواد ۲ تا ۵. اعضا می‌توانند به‌موجب قانون تعداد چنین ابزارهایی را که فرد پیش از تحمیل مسئولیت کیفری باید در تصرف داشته باشد، تعیین نمایند» همچنین کنوانسیون عربی مقابله با جرایم تکنولوژی اطلاعات ۲۰۱۰ نیز در بند ۲ مادهٔ ۹، «تملک هر وسیله یا برنامه‌ای که در دو پاراگراف فوق بیان شد، با هدف بهره از آن‌ها برای ارتکاب هر جرمی که در مواد ۶ تا ۸ بیان شده است.» را قابل‌جرم‌انگاری دانسته است. تفاوت این جرم‌انگاری با موارد فوق که باعث شده این اسناد این رفتار را از آن موارد جدا نمایند آن است که ماهیت رفتارهای تولید، توزیع، انتشار یا در دسترس قراردادن دارای ماهیتی فعال و معاونتی است. در واقع فرد با انجام رفتارهای فوق در جرم دیگری معاونت می‌نماید که قانون‌گذار آن را به عنوان جرم مستقل ذکر نموده است. لیکن در این بند فرد این ابزارها را به قصد ارتکاب جرم سایبری در آینده توسط خود نگهداری می‌نماید. بنابراین ماهیت این رفتار مفعل و تهیهٔ مقدمات برای جرم آتی است که این اسناد آن را با شرایطی جرم‌انگاری کرده‌اند.

قانون ایران صرف نگهداری یا تملک نرم‌افزارها یا ابزارهایی را که صرفاً برای ارتکاب جرم رایانه‌ای به کار می‌روند، جرم‌انگاری ننموده است، در حالی‌که مناسب بود در صورتی که معاونت در جرم سایبری ارتکاب شده توسط دیگری را که به شکل تهیهٔ مقدمات ظهور یافته، به عنوان جرم مستقل پیش‌بینی می‌نماید، تهیهٔ مقدمات برای جرم ارتکابی توسط خود را نیز جرم‌انگاری نماید. به همین دلیل است که کنوانسیون بوداپست در بند ۳ مادهٔ ۶، اجازهٔ اعمال حق شرط را نسبت به بند الف-۱ قسمت ۱ مادهٔ ۶ یعنی همان تولید، خرید و تهیهٔ وسایل و نرم‌افزارهایی را که برای ارتکاب جرم رایانه‌ای طراحی شده یا تغییر داده شده است، داده ولیکن از حق شرط نسبت به بند ۲ که شامل نگهداری این وسایل می‌شود، سخنی به میان نیاورده است و این خود نشان اهمیت والاتر این جرم نسبت به جرم قبلی است. به همین جهت به نظر می‌رسد قانون‌گذار ایران نیز در صورتی که قصد برخورد منطقی با جرایم رایانه‌ای را دارد، باید رویهٔ یکسان را پیش گیرد و در صورتی که مواردی را که معاونت است، جرم‌انگاری می‌نماید، به جرم‌انگاری نگهداری نیز اقدام نماید. البته در این خصوص دو نکته حائز اهمیت است:

اول، چنان‌که کنوانسیون بوداپست و کنوانسیون عربی مقابله با جرایم تکنولوژی اطلاعات ۲۰۱۰ مقرر نموده‌اند، پیش‌بینی نگهداری، «به منظور ارتکاب جرم» ضروری است. بنابراین جرم‌انگاری صرف نگهداری به‌دلیل آنکه با هیچ اصل جرم‌انگاری قابل‌توجیه نیست، در این اسناد پیشنهاد نشده است. دوم، از آنجا که قصد ناظر به حالت ذهنی و درونی شخص می‌باشد و اثبات آن تعلیق به محال است، کنوانسیون بوداپست در راستای عینی نمودن این اثبات به کشورها اجازه داده است که تعدادی از این ابزار را مشخص نموده و نگهداری این تعداد را قرینه‌ای برای قصد ارتکاب جرم در آینده محسوب نمایند.

۴. مسئولیت ارائه‌دهندگان خدمات اینترنتی در قبال عدم حذف ابزارهای مجرمانه

ارائه‌دهندگان خدمات اینترنتی، اشخاصی هستند که در دو حوزهٔ میزبانی و دسترسی امکان دسترسی افراد را به وب فراهم می‌نمایند. ارائه‌دهندگان خدمات میزبانی، مبادرت به ارائهٔ فضایی در فضای مجازی برای افراد کرده تا بتوانند در آن وب‌سایت، کانال و یا صفحه‌ای را برای خود ایجاد نمایند. برای مثال در صورتی که دانشگاه، صفحه را برای یکی از اساتید اختصاص داده تا وی بتواند داده‌های علمی و مطالب خود را در آن بارگذاری نماید، دانشگاه ارائه‌دهندهٔ خدمات میزبانی محسوب می‌شود. از سوی دیگر، ارائه‌دهندهٔ خدمات دسترسی، امکان اتصال فرد به اینترنت را فراهم می‌آورد. به عبارتی حجم اینترنتی که به شبکهٔ زیرساخت وارد می‌شود، در میان شرکت‌های ارائه‌دهندهٔ خدمات دسترسی تقسیم شده و آن‌ها این حجم را بین کاربران خود تقسیم می‌نمایند. این دو نهاد

طبق مواد ۷۴۹ و ۷۵۱ قانون مجازات اسلامی نسبت به محتوایی که توسط سامانه یا اینترنت دسترسی داده شده توسط آن‌ها ارائه می‌شود، وظایفی دارند. این وظیفه به طور خاص ناظر به پالایش محتوای مجرمانه به محض دریافت دستور کارگروه (کمیته) تعیین مصادیق می‌باشد. طبق مادهٔ ۷۴۹ این قانون، ارائه‌دهندگان خدمات دسترسی موظفند طبق ضوابط فنی و فهرست مقرر از سوی کارگروه (کمیته) تعیین مصادیق موضوع مادهٔ ذیل محتوای مجرمانه که در چهارچوب قانون تنظیم شده است اعم از محتوای ناشی از جرایم رایانه‌ای و محتوایی که برای ارتکاب جرایم رایانه‌ای به کار می‌رود را پالایش (فیلتر) کنند. و طبق مادهٔ ۷۵۱، ارائه‌دهندگان خدمات میزبانی موظفند به محض دریافت دستور کارگروه (کمیته) تعیین مصادیق مذکور در مادهٔ فوق یا مقام قضایی رسیدگی‌کننده به پرونده مبنی بر وجود محتوای مجرمانه در سامانه‌های رایانه‌ای خود از ادامهٔ دسترسی به آن ممانعت به عمل آورند. حال پرسش آن است، در صورتی‌که این دو از وجود ابزارهایی که صرفاً برای جرایم رایانه‌ای به کار می‌رود آگاه شوند، آیا موظف به پالایش و ممانعت از دسترسی کاربران به آن سامانه می‌باشند؟ به عبارتی با توجه به متن مادهٔ ۷۵۳ قانون مجازات اسلامی که در دسترس قرار دادن این داده را جرم‌انگاری کرده است، آیا نهادهای ارائه‌دهندهٔ این خدمات به‌واسطهٔ عدم پالایش و ممانعت از دسترسی مسئولیت کیفری خواهند داشت؟ به نظر می‌رسد پاسخ منفی خواهد بود. زیرا حق دسترسی آزاد مردم به اطلاعات و دانش چنان‌که در مقدمهٔ «مقررات و ضوابط شبکه‌های اطلاع‌رسانی رایانه‌ای»، ابلاغی ۱۳۸۰/۹/۱۲ و «آیین‌نامهٔ ساماندهی فعالیت پایگاه‌های اطلاع‌رسانی (سایت‌های) اینترنتی ایرانی» مصوب ۱۳۸۵/۵/۱۹ آمده جزء حقوق هر شهروند می‌باشد و از آنجا که تحدید حقوق شهروندان جز در مواردی که قانون اجازهٔ این امر را نداده باشد، ممکن نیست. ارائه‌دهندگان خدمات اینترنتی نمی‌توانند حتی در مواجهه با این داده‌های مجرمانه رأساً مبادرت به پالایش و یا ممانعت از دسترسی کاربران بنمایند. زیرا در این صورت این اشخاص اقدامی قضایی را بنا به صلاحدید خود انجام داده‌اند. با این حال، قانون مجازات اسلامی در تبصرهٔ مادهٔ ۷۵۱ مقرر داشته است: «ارائه‌دهندگان خدمات میزبانی موظفند به محض آگاهی از وجود محتوای مجرمانه مراتب را به کارگروه (کمیته) تعیین مصادیق اطلاع دهند.» این تبصره دارای دو نکتهٔ مهم می‌باشد: اول آنکه این وظیفه تنها بر ارائه‌دهندگان خدمات میزبانی بار شده است و ارائه‌دهندگان خدمات دسترسی چنین وظیفهٔ قانونی‌ای را ندارد. لذا، حتی در صورت مواجهه با انتقال داده‌های مجرمانه توسط اینترنتی که توسط آن‌ها ارائه شده است، موظف به گزارش نمی‌باشند. این امر از آن جهت صحیح است که ارائه‌دهندگان این خدمات با توجه به اصل محرمانگی و حق بر خلوت، قانوناً نمی‌توانند کاربران خود را کنترل نمایند و در نتیجه امکان گزارش انتقال داده‌های مجرمانه نیز سالبه

به انتفاء موضوع می‌باشد. مسئلهٔ دوم در خصوص این تبصره ضمانت‌اجرای آن می‌باشد. تبصرهٔ مذکور اگرچه برای ارائه‌دهندگان خدمات میزبانی وظیفهٔ گزارش را پیش‌بینی نموده است، لیکن برای این امر ضمانت‌اجرایی پیش‌بینی نکرده است. حال، پرسش آن است که در صورت آگاهی از اینکه نرم‌افزارهای صرفاً مجرمانه در سامانه‌ای قرار داده شده است و ارائه‌دهندهٔ خدمات میزبانی آن را به کمیتهٔ تعیین مصادیق مجرمانه گزارش نکند، آیا وی را می‌توان مشمول بند الف مادهٔ ۷۵۳ قانون مجازات اسلامی دانست؟ با توجه به سیاق عبارت به کار رفته در ماده و نظر به رفتارهایی که پیش و پس از این عبارت در بند الف مادهٔ ۷۵۳ بیان شده است، می‌توان به این امر پاسخ منفی داد. زیرا تمامی رفتارهای مذکور در این تبصره فعلی می‌باشند، مانند تولید، انتشار، توزیع و معامله و این قرینه‌ای است که این جرم تنها با فعل قابل‌تحقق است.

دلیل دوم، مبنی بر عدم امکان کیفر این ارائه‌دهندگان خدمات جهت عدم پالایش و ممانعت از دسترسی، تفکیک وظایف اجرایی از قضایی می‌باشد. تحدید حق شهروندان امری قضایی می‌باشد که نمی‌توان آن را به شهروندان عمومی دولت تفویض نمود. به عبارتی، این ارائه‌دهندگان از نظر مبنایی نباید بتوانند به صلاحدید خود سامانه‌ای را تنها به این دلیل که به گمان آنان ابزارهای مجرمانه در آن در دسترس قرار گرفته، پالایش نمایند. در صورت پذیرش این امر، تحمیل مسئولیت کیفری بر آنان نه تنها از نظر قانونی در مقام وضع صحیح نمی‌باشد، بلکه در وضعیت حقوقی فعلی نیز مقنن، به طور صحیح این وظیفه را بر آنان تحمیل ننموده است و به همین جهت نمی‌توان حتی در صورت برخورد با این محتوا و عدم ممانعت یا پالایش آنان را کیفر نمود.

با این حال، در صورتی که دستور مقام قضایی و یا کارگروه پالایش محتوای مجرمانه مبنی بر پالایش یا ممانعت از دسترسی صادر شد و این ارائه‌دهندگان عمداً و یا از روی تقصیر مبادرت به عدم پالایش یا ممانعت از دسترسی نمایند، طبق مواد ۷۴۹ و ۷۵۱ قانون مجازات اسلامی مسئولیت کیفری خواهند داشت.

نتیجه

امروزه فضای مجازی جزئی واقعی از زندگی انسان‌ها شده است. مراودات در این فضا اگر بیش از فضای واقعی نباشد، از آن کمتر نخواهد بود. روزانه تعداد زیادی از افراد وارد این فضا شده و امور خود را به انجام می‌رسانند و این پیوستگی بین انسان‌ها با فضای مجازی را روزبه‌روز افزایش داده است. به همین دلیل، این فضا، محیط مناسبی برای مجرمان نیز گردیده تا بتوانند آنچه را در فضای واقعی نمی‌وانند انجام دهند در این فضا به‌منصهٔ ظهور رسانند. از طرفی، دولت‌ها نیز با وقوف به این امر و با پیشنهاد اسناد فرامرزی، نه تنها رفتارهای صدمه‌زننده بلکه مقدمات این رفتارها را در فضای

مجازی جرم‌انگاری کرده و به مقابله با آن پرداخته‌اند. بند الف مادهٔ ۷۵۳ قانون مجازات اسلامی که در اسناد فرامرزی متعددی مشابه آن وجود دارد، نیز در این راستا تصویب شده است. لیکن ابهاماتی در خصوص اعمال این ماده وجود داشته که این مقاله با بررسی این ابهامات و با رویکرد تطبیقی به نتیجه‌های زیر دست یافته است:

اگرچه این ماده به جرایم رایانه‌ای اشاره کرده است و در اغلب اسناد فرامرزی این جرایم تنها منحصراً به جرایم رایانه‌ای محض شده‌اند، لیکن از آنجا که قانون جرایم رایانه‌ای در سایر مواردی که از واژهٔ «جرایم رایانه‌ای» بهره برده است (مانند مادهٔ ۷۴۷)، ارادهٔ اعم نموده و جرایم رایانه‌ای محض و جرایم مرتبط با رایانه را مدنظر قرار داده است، به نظر می‌رسد این ماده نیز هر دو دستهٔ جرایم را در برمی‌گیرد. از طرفی این امر مخالف این اسناد نیز نمی‌باشد زیرا آن‌ها اجازهٔ توسعه و یا ضیق این جرم‌انگاری را به کشورها اعطا کرده‌اند.

در خصوص ابزارهایی با کاربرد دوگانهٔ مجرمانه و غیر آن، به رغم ذکر عبارت «صرفاً» در این ماده، هرچند این لفظ از نظر معنا افادهٔ حصر می‌کند با این حال، تفسیر کاربردی حقوق کیفری اقتضای آن را دارد که این لفظ در معنای «غالب» تفسیر شود و در این امر قصد مرتکب از تولید و انتشار آن نیز مدنظر قرار گیرد.

از منظر عنصر روانی نیز در بین کشورها و اسناد اختلاف‌نظر در خصوص عمدی بودن این جرم وجود دارد، به‌گونه‌ای که برخی اسناد و کشورها ارتکاب این جرم به صورت غیرعمد را نیز ممکن دانسته‌اند. مانند لایحهٔ قانون جرایم رایانه‌ای و جرایم مرتبط با رایانهٔ اسپانیا. با این حال، با توجه به اصل کلی عمدی بودن در حقوق ایران مقنن ارتکاب آن را تنها به صورت عمدی ممکن دانسته است که با توجه به آنکه این جرم، بزه مانع محسوب می‌شود، عدم گسترش دامنهٔ آن صحیح‌تر بوده و از این منظر رویکرد مقنن صحیح می‌باشد. با این‌حال، بر اساس این مبنا، به نظر می‌رسد پیش‌بینی سوءنیت خاص برای این جرم ضروری است، زیرا در صورت عدم پیش‌بینی این امر، هرگونه تولید هرچند به قصد نشان دادن علم رایانه‌ای و با احراز عدم وجود قصد انتشار یا بهره شامل این جرم می‌شود که با اصول جرم‌انگاری هماهنگ نمی‌باشد و بر این اساس، مناسب‌تر است بند الف مادهٔ ۷۵۳ قانون مجازات اسلامی با کنوانسیون‌هایی که سوءنیت خاص را پیش‌بینی کرده‌اند، مانند کنوانسیون بوداپست ۲۰۰۱، هماهنگ شود.

از نظر رفتار مادی در بند الف مادهٔ ۷۵۳ از نگهداری ذکری به میان نیامده است، لیکن در برخی از اسناد مانند کنوانسیون بوداپست ۲۰۰۱ و کنوانسیون عربی مقابله با جرایم تکنولوژی اطلاعات ۲۰۱۰ این رفتار ذکر شده است. جرم‌انگاری این رفتار به نظر ضروری می‌باشد، زیرا این رفتار، جرم

مانع می‌باشد و مقنن می‌تواند هر رفتار مقدماتی که برای پیشگیری از جرایم رایانه‌ای مناسب باشد را جرم‌انگاری نماید. با این حال، مقنن مبسوط‌الید نمی‌باشد و ضروری است برای تضییق جرم‌انگاری نگهداری قید محدودکننده ذکر شود که عبارت است از عنصر روانی قصد توزیع یا بهره از این ابزارها. به عبارتی درصورت نگهداری به قصد توزیع مناسب است این رفتار جرم‌انگاری گردد که خلأ مادهٔ ۷۵۳ از این منظر رفع شود.

در نهایت، با توجه به آنکه این جرایم در بستر فضای ارتباطات صورت می‌گیرد که ارائه‌دهندگان خدمات میزبانی و یا خدمات دسترسی آن‌ها را ارائه می‌دهند، شایان ذکر است این ارائه‌دهندگان حتی با وجود برخورد با ابزارهای صرفاً مجرمانه در فضایی که میزبانی آن را دارا می‌باشند و یا پخش از طریق بستری که ارائه کرده‌اند، راساً حق مداخله ندارند[1] و ضروری است آن را از طریق کمیتهٔ پالایش و یا سایر طرق قانونی پیگیری نمایند. با این حال، عدم پیگیری آن‌ها در این مورد نمی‌تواند مشمول رفتارهای بند الف مادهٔ ۷۵۳ شود و نهایتاً می‌توان با احراز عنصر روانی، آن‌ها را معاون این جرم دانست. لذا، در مجموع می‌توان بیان داشت قانون ایران به‌جهت عمدی دانستن این جرم و ذکر عبارت دادهٔ مجرمانه در شمار موضوعات جرم نسبت به اسناد فرامرزی دارای برتری بوده ولیکن به‌جهت عدم ذکر سوءنیت خاص، عدم تصریح به نگهداری در شمار رفتارهای مجرمانه و محدود کردن جرم به وسایلی که صرفاً برای ارتکاب جرم کاربرد دارند، نیازمند اصلاح می‌باشد.

---

۱. نکتهٔ شایان توجه در جرایم رایانه‌ای آن است که فضای مجازی در این جرایم بستر ارتکاب جرم می‌باشند و نه وسیلهٔ ارتکاب جرم و از این جهت بین این جرایم و بزه‌های مطبوعاتی که در آن مطبوعات وسیله است تفاوت وجود دارد (توحیدی و امیرلی، ۱۳۹۷).

منابع

فارسی

- آنجلیز، جینادی (۱۳۸۳)، **جرایم سایبر**، ترجمه عبدالصمد خرم‌آبادی و سعید حافظی، تهران: نشر شورای عالی اطلاع‌رسانی تهران.
- آیوک، جان (۱۳۹۱)، **ویروس‌ها و بدافزارهای کامپیوتری**، ترجمه بابک بشری راد وآرش حبیبی لشکری، چاپ نخست، تهران: انتشارات ناقوس.
- پرسمن، راجر اس (۱۳۹۳)، **مهندسی نرم افزار**، ترجمه عین الله جعفرنژاد قمی و ابراهیم عامل محرابی، تهران: انتشارات دانش نگار.
- توحیدی، جلال و حسین امیرلی (۱۳۹۷)، «بایسته‌های کیفرگزینی در رویارویی با جرایم سایبری با تأکید بر رویه قضایی»، **مجله حقوقی دادگستری**، شماره ۱۰۱.
- جلالی فراهانی، امیرحسین (۱۳۹۵)، **کنوانسیون جرایم سایبر و پروتکل الحاقی آن**، چاپ دوم، تهران: نشر خرسندی.
- داوری دولت آبادی، مجید (۱۳۹۳)، **بدافزارها و راهکارهای مقابله با آن**، چاپ اول، تهران: نشر پندارپارس.
- سینگر، فریدام (۱۳۹۴)، **امنیت سایبری و جنگ سایبری**، چاپ اول، ترجمهٔ علی‌اصغر جعفری لاری، تهران: نشر پندار پارس.
- ضیایی‌پرور، حمید (۱۳۸۳)، **جنگ نرم ۱ (ویژه جنگ رایانه‌ای)**، چاپ اول، تهران: نشر مؤسسه فرهنگی و مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران.
- طاهری، محسن (۱۳۷۲)، «جرم و رایانه»، **مجله حقوقی دادگستری**، شماره ۹.
- عالی پور، حسن (۱۳۹۳)، **حقوق کیفری فناوری و اطلاعات**، چاپ سوم، تهران: نشر خرسندی.
- عزیزی، امیرمهدی (۱۳۹۴)، **حقوق کیفری جرایم رایانه ای**، چاپ دوم، تهران: نشر مجد.
- مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر (۱۳۹۱)، **امنیت و جنگ سایبری (۲) (ویژه سلاح‌ها، جنگجویان و حملات سایبری)**، چاپ اول، تهران: نشر مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر.
- نادرخانی، نیما (۱۳۹۰)، «ابزارهای مورد استفاده مجرمان و خرابکاران رایانه ای»، **فصلنامه علمی ترویجی کاراگاه**، شماره۱۴.

انگلیسی

- Clough, Jonathan. (2010). **Principles of Cybercrime**. Cambridge University Press.
- Egele, M., Scholte, T., Kirda, E., & Kruegel, C. (2012). "A survey on automated dynamic malware-analysis techniques and tools". **ACM computing surveys (CSUR)**. 44 (2), 6.
- HIPCAR. (2012). **Cybercrime/e-Crimes: Model Policy Guidelines & Legislative Texts**, Itu.int. (2019). [online] Available at: https://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/in-country_assistance/Grenada/HIPCAR-

Grenada_Cybercrime_Report_Final_Draft_April2012.pdf [Accessed 1 May 2019].

- Jefferson, Michael. (2009). **Criminal Law**. Pearson (longman) publisher.
- Mollan, Mike. (2008). **Cases and Materials on Criminal Law**. Routlege. Cavandish group.
- Rehman, Rizwan, G. C. Hazarika, and Gunadeep Chetia. (2011). "Malware threats and mitigation strategies: a survey". **Journal of Theoretical and Applied Information Technology**. vol. 29.2.
- Malby, S., Mace, R., Holterhof, A., Brown, C., Kascherus, S., & Ignatuschtschenko, E. (2013). **Comprehensive study on cybercrime**. United Nations Office on Drugs and Crime. Tech. Rep