

## مطالعه‌ی تطبیقی جرایم سایبری در ایران و حقوق بین‌الملل

بیثا دشتی<sup>۱</sup>

دکتر مریم افشاری<sup>۲</sup>

تاریخ پذیرش: ۱۳۹۸/۰۸/۲۷

تاریخ دریافت: ۱۳۹۷/۰۹/۱۱

### چکیده

هرگونه تغییر و تحول در دنیای کنونی، خواه ناخواه آثار و پیامدهایی به همراه خواهد داشت. به گونه‌ای که با اختراع وسیله‌ای جدید همواره امکان سوء استفاده از آن‌ها وجود دارد. در این راستا علم حقوق هر آن‌چه را که کوچک‌ترین خدشه‌ای به این توازن وارد نماید، تحت پوشش قرار داده و در رفع یا پیشگیری از آثار نامطلوب سعی می‌نماید. فضای سایبر نیز از این قاعده مستثنی نبوده و آثاری به صورت مثبت و منفی در زندگی بشر وارد نموده است که ضرورت مطالعه‌ی آن را انکارناپذیر می‌نمایاند. متعاقب این کار با این امر سیاستگذاران جنایی، حقوقدانان و جرم‌شناسان به این فضا ورود پیدا کرده و با تعریف جرایم سایبری، پیش‌بینی مجازات‌های متناسب با آن و ارائه و انجام تدابیر امنیتی و پیشگیرانه نسبت به مخاطرات این فضا و آموزش و آگاه‌سازی افراد از پیامدهای مخرب فضای سایبر، وظایف اساسی خود را در این زمینه انجام می‌دهند که بررسی کیفیت و ابعاد این کارکرد امری ضروری است. در این مقاله ماهیت فضای سایبر و ابزارهای ارتباطی، تعریف، تاریخچه، ویژگی و طبقه‌بندی آن مورد بررسی قرار می‌گیرد. خطرات احتمالی و جهانی شدن مقابله با جرایم سایبری از نکاتی بود که به عنوان نتیجه بحث مطرح شد. همچنین پیشنهاداتی به عنوان مدل مورد استفاده برای سیاست‌گذاران جنایی کشور جهت مقابله و پیشگیری

---

<sup>۱</sup> دانشجوی کارشناسی ارشد دانشکده‌ی حقوق دانشگاه آزاد اسلامی واحد دماوند (نویسنده - مسئول)

bita\_dashti@yahoo.com

<sup>۲</sup> دانشیار دانشکده‌ی حقوق دانشگاه آزاد اسلامی واحد دماوند - afshari2005m@yahoo.com

از جرایم سایبری ارائه شده که امید است مورد توجه حقوقدانان، جرم شناسان و کاربران عزیز قرار گیرد.

**کلیدواژگان:** رایانه، جرایم سایبری، اطلاعات رایانه‌ای، حقوق بین‌الملل، حقوق ایران

## مقدمه

بی تردید هر کاری ابزاری می‌خواهد و ابزار تحقق یک جامعه ی مدرن، فناوری اطلاعات و ارتباطات است. هدف از اختراع رایانه، تسریع و تسهیل پردازش اطلاعات بود که به‌خوبی به‌ثمر نشست و مخابرات نیز به‌عنوان مهم‌ترین ابزار ارتباطی، در نشر این اطلاعات پردازش شده نقش به‌سزایی ایفا کرده است. از حدود نیم قرن اخیر، به‌تدریج با کشف قابلیت های شگرف ناشی از تلفیق این دو فناوری، انقلابی در عرصه ی فناوری اطلاعات و ارتباطات رقم خورد. اوج این انقلاب را می‌توان در ظهور شبکه‌های اطلاع‌رسانی رایانه‌ای جهانی دانست که از دهه نود میلادی به بعد، تحولی بنیادین را در این حوزه رقم زده‌اند. این شبکه‌ها که خود از بسیاری سیستم‌های رایانه‌ای متصل به یکدیگر تشکیل شده‌اند، به مدد فناوری‌های پیشرفته مخابراتی با یکدیگر ارتباط برقرار کرده و فضایی با ویژگی‌های کاملاً متمایز از دنیای فیزیکی به‌وجود آورده‌اند که عده‌ای آن را فضای مجازی<sup>۱</sup> نامیده‌اند و عده‌ای هم عنوان فضای سایبر<sup>۲</sup> را برای آن برگزیده‌اند.<sup>۳</sup> فضای سایبری علاوه بر امکاناتی که برای رشد و توسعه در اختیار بشر قرار داده، فرصت‌هایی نیز برای مجرمان ایجاد کرده است. از این روست که امروزه سخن از وجه سیاه اینترنت به‌میان می‌آید از جمله ویژگی های این فضا آن است که مجرمان می‌توانند راحت‌تر مرتکب جرم شده و جرایم بیشتری مرتکب شوند و آماج مجرمانه متکثرتری را هدف بگیرند. این ویژگی‌های فضای سایبری باعث شده است که مقرراتی در خصوص پاسخ‌دهی کیفری برای مجرمان چه در حقوق ایران و چه در حقوق بین‌الملل وضع شود و این مقاله درصدد این است که بتواند به سوالات زیر پاسخ دهد.

جرایم سایبری در ایران و حقوق بین‌الملل از منظر حقوقی چگونه مطابقت دارند؟

قدرت بازدارندگی مجازات های کنونی نسبت به جرایم سایبری به چه صورتی می‌باشد؟

جرایم سایبری در چه فضاهایی قابل اعمال است؟

---

<sup>۱</sup> Virtual Space

<sup>۲</sup> Cyber Space

<sup>۳</sup> اصطلاح فضای سایبر، برای اولین بار در سال ۱۹۸۲ در یک داستان علمی-تخیلی به کار رفت و در سال ۱۹۹۰ پروفیسور جان پری بارلو به هنگام صحبت در یک کنفرانس آنلاین، از آن استفاده کرد و آن را بر سر زبان‌ها انداخت.

این مقاله براساس روش توصیفی\_تحلیلی نوشته شده است که پس از بررسی و واکاوی قانون جرایم رایانه‌ای ایران و کنوانسیون بین‌المللی جرایم سایبری، به توصیف و تحلیل جرایم سایبری در حقوق ایران و حقوق بین‌الملل پرداخته شده و لازم به ذکر است که در تنظیم پژوهش پیش رو از روش اسنادی و کتابخانه‌ای استفاده شده است.

## یافته‌های تحقیق

### تعریف جرم سایبری

اولین مشکل در ارائه‌ی تعریف، ماهیت جرم سایبری است. در مورد تعریف و ماهیت جرایم، الگوی یکسانی مورد تبعیت قرار نگرفته است (زندى، ۱۳۸۹: ۱۵). برای درک مفهوم جرم سایبر و تفاوت آن با سایر جرایم رایانه‌ای، درک تعریف محیط سایبر و ویژگی‌های آن ضروری است. سایبر از لحاظ لغوی در فرهنگ‌های مختلف به معنی مجازی و غیرملموس است. بدون وجود تعریفی از جرم سایبر در فرهنگ‌لغت‌ها، قانون‌گذاران و مجریان قانون در سراسر جهان جرم سایبر را درک کرده‌اند. وقتی آن را می‌بینند، می‌شناسند. انتشار ویروس‌ها و کرم‌های رایانه‌ای، انجام حملات الکترونیکی و به‌طور کلی هرگونه فعالیتی که سبب ایجاد اختلال در شبکه‌های رایانه‌ای و امور مبتنی بر آن شود، جرایم سایبری نامیده می‌شوند. جرایم سایبری را در معنی جامع می‌توان به هرگونه فعالیتی که به‌منظور انجام تبهکاری در شبکه‌های رایانه‌ای به‌خدمت می‌گیرد، اطلاق نمود. بر اساس تعریف فوق اقداماتی چون حمله‌ی الکترونیکی به زیرساخت‌های حیاتی و ملی کشورها، کلاهبرداری، پولشویی الکترونیکی، استفاده جنایتکارانه از اینترنت، جعل آی‌دی<sup>۱</sup> و حتی استفاده از رایانه و مفاهیم فناوری اطلاعات در جریان جنایات غیر سایبری مصداق‌هایی از جرایم سایبری است. در کل می‌توان گفت که جرم سایبری زیرمجموعه جرم رایانه‌ای است (حسینی خواه، ۱۳۹۰: ۲۳).

<sup>۱</sup> ID

## ویژگی های جرایم سایبری

### ۱- جرایم کلاسیک با توصیف سایبری

۱-۲-۱ جرایمی در این دسته قرار می گیرند که جرایم سنتی تلقی می شوند؛ اما در حال حاضر به علت پیشرفت فناوری، با وسایل طبقه بندی جرایم سایبری جرایم سایبری را در چهار دسته یا طبقه ی کلی می توان جای داد. از جمله این جرایم می توان به کلاهبرداری سایبری، جعل سایبری، تخریب سایبری، جاسوسی سایبری و... اشاره نمود.

### جرایم علیه محرمانه بودن داده ها و سیستم ها

هر نمادی از موضوع ها، مفاهیم یا دستورالعمل ها از جمله متن، صوت یا تصویر را که برای برقراری ارتباط میان سیستم های رایانه ای یا پردازش توسط شخص یا سیستم رایانه ای به کار گرفته شده و به وسیله ی سیستم رایانه ای ایجاد می گردد، داده ی محتوا گویند. از جمله جرایمی که در این دسته جای می گیرند می توان به شنود غیر مجاز داده های مخابراتی در یک ارتباط خصوصی یا داده های سری اشاره کرد که واجد ارزش برای امنیت داخلی و خارجی کشور می باشند.

### جرایم علیه صحت و تمامیت داده ها و سیستم ها

تغییر، ایجاد، محو یا متوقف کردن رایانه ای و مخابراتی به قصد تقلب، غیر قابل استفاده کردن، تخریب یا اختلال در داده ها یا امواج الکترو مغناطیسی، ممانعت از دستیابی اشخاص مجاز به داده ها با تغییر رمز ورود و یا رمز نگاری از جمله جرایمی هستند که در این دسته قرار می گیرند.

## جرایم مرتبط با محتوا

این دسته جرایمی را تحت شمول خود قرار می‌دهد که در آن‌ها، رایانه به عنوان ابزار و وسیله توسط مجرم برای ارتکاب جرم به کار گرفته می‌شود و صرفاً فناوری اطلاعات، زمینه‌ی ارتکاب آن‌ها را فراهم می‌سازد. برای مثال، انتشار محتویات مستهجن از قبیل نمایش اندام جنسی زن و مرد یا نمایش آمیزش جنسی انسان، تبلیغ یا تحریک یا تشویق به انحرافات جنسی یا خودکشی از طریق سیستم رایانه‌ای یا مخابراتی در این دسته قرار می‌گیرند (سایت [www.CyberCrimes.com](http://www.CyberCrimes.com)).

## راهکارهای احتمالی در مقابله و پیشگیری از جرایم رایانه‌ای

وظیفه نظام حاکم است که با توجه به روند تحولات جهانی ابزار قانونی و اجرایی لازم را برای مقابله و پیشگیری از جرایم مهیا نماید. تجربه‌ی کشورهایی که حداقل یک دهه از عمر قانون‌گذاری و نهادهای اجرایی مقابله با جرایم رایانه‌ای آن‌ها می‌گذرد بیانگر این امر مهم است که:

- (۱) سعی کرده‌اند تعادلی بین نیازهای جامعه و ضمانت اجرای لازم برای مجریان قانون به وجود آورند.

- (۲) نه تنها سه نهاد اصلی یعنی قانون‌گذار نظام قضایی و پلیس؛ بلکه سازمان‌ها و وزارت‌خانه‌های متعددی دست به دست یکدیگر داده‌اند تا طرح مبارزه با جرایم را از طریق آموزش عمومی و مقابله با مجرمان به اجرا در آورند (فهیمی، ۱۳۸۰: ۱۳۶).

## مشکلات مقابله با جرایم سایبری بین‌المللی

### اصول صلاحیت کیفری مربوط به مجرمان بین‌المللی

جرایم سایبری فراتر از مرزهای جغرافیایی اتفاق می‌افتد و در نتیجه محل اصلی ارتکاب جرم و کشور آسیب‌دیده ممکن است متفاوت باشند؛ برای مثال اگر شخص (الف) با ملیت فیلیپین،

ویروسی در فیلیپین منتشر کند و این ویروس به شرکتی در ایالات متحده آسیب بزند، این مسئله پیش می آید که این فرد باید طبق قانون کدام کشور مجازات شود.

اصول صلاحیت کیفری اعمال مجرمانه بین المللی به چند دسته اقلیمی، صلاحیت شخصی منفعل، حمایت گرایی و شخصی گرایی تقسیم شده اند؛ براساس مثال بالا به شرح هر کدام از این اصول پرداخته شده است.

### اصل اقلیمی

این اصل به معنی اعمال قانون ملی به تمام جرایم مرتکب شده در قلمروی یک کشور صرف نظر از ملیت مجرمان گفته می شود. با توجه به این اصل وقتی فرد (الف) در فیلیپین مرتکب جرمی می شود برای مجازات این شخص باید قانون کشور فیلیپین اعمال شود با این حال براساس اصل حضور همه جانبه اگر این جرم در آمریکا هم اتفاق افتاده باشد چه بسا اجرای قانون در اختیار و صلاحیت این کشور باشد اگر فیلیپین هیچ قانونی برای مجازات این جرم نداشته باشد پس در نتیجه این عمل در فیلیپین جرم محسوب نمی شود. در نتیجه می توان گفت حوزه ی قضایی این جرم به فیلیپین محدود نمی شود.

### اصل صلاحیت شخصی

اصل صلاحیت شخصی فعال صرف نشر از محل ارتکاب جرم به اعمال قانون کشور فرد مجرم اطلاق می شود براساس این اصل اگر چه جرم شخص (الف) در آمریکا صورت گرفته باشد و خود فرد دارای ملیت فیلیپینی باشد فقط فیلیپین صلاحیت رسیدگی به این جرم را دارد نه آمریکا. در صورتی که فیلیپین هیچ قانونی برای رسیدگی به این جرم نداشته باشد این عمل جرم محسوب نشده و به اصل مشروعیت ارجاع داده می شود.

## اصل صلاحیت شخصی منفعل

این اصل می‌گوید که دادگاه کشور قربانی صلاحیت رسیدگی به این جرم را دارد؛ با توجه به این اصل کشور قربانی، همان آمریکا است که دارای صلاحیت داوری است نه فیلیپین. با این حال این اصل در سطح بین‌المللی مورد استفاده قرار نگرفته و هیچ معاهده‌ای براساس آن وجود ندارد. حمایت‌گرایی

سیستم حمایت‌گرایی به این معنی است که صرف‌نظر از کشوری که مرتکب جرم شده و کشور قربانی قانون، کشور مورد نظر به هر کدام از اعمال مجرمانه که حقوق آن کشور را نقض کرده است اعمال شود؛ براساس این اصل شرکتی که در آمریکا است و اقدام مجرمانه (الف) باعث به خطر افتادن حقوق آن شده است، به حوزه‌ی قضایی فدرال مربوط می‌شود؛ با این حال جرایم مربوط به ملی، تحت قانون هر دو کشور قرار می‌گیرند که حوزه‌ی قضایی فدرال در پشتیبانی و حمایت از آن‌ها مختار است.

## جهان‌گرایی

جهان‌گرایی، استفاده از کشور برای یک عمل خاص مجرمانه (دزدی دریایی، جنگ و...) صرف‌نظر از کشور محل وقوع جرم و جنایت و مجرم و قربانی است؛ در این حالت اعمال مجرمانه معین در چهارچوب جهانی‌گرایی شامل دزدی دریایی و جنگ، جرم علیه بشریت است که توسط عوامل بین‌المللی تشخیص داده می‌شود؛ بنابراین براساس این قانون، آمریکا سازوکار رسیدگی به این جرایم را ندارد.

## قطعنامه‌های اتحادیه‌ی بین‌المللی ارتباطات

اتحادیه‌ی بین‌المللی ارتباطات چندین قطعنامه مرتبط با موضوع جرایم سایبری را در حالی صادر نموده است که مستقیماً و با مقررات و قوانین کیفری مشخص به مسئله نمی‌پردازند. از جمله مهم‌ترین این قطعنامه عبارتند از:



- قطعنامه ی شماره ی ۱۳۰، صادره در کنفرانس مستقل اتحادیه در گوادالاجارای مکزیک در سال ۲۰۱۰ با موضوع تقویت نقش اتحادیه ی بین المللی ارتباطات در ایجاد اطمینان و امنیت در استفاده از فناوری های ارتباطاتی و اطلاعاتی.

توضیح این که وظیفه ی اتحادیه در ایجاد ظرفیت های لازم، در کنفرانسی که در سال ۲۰۱۰ در گوادالاجارا در مکزیک برگزار و به صدور قطعنامه شماره ی ۱۳۰ منجر شد، مورد تأکید قرار گرفت. براساس این قطعنامه، اتحادیه ی بین المللی ارتباطات وظیفه دارد با کشورهای عضو و به ویژه کشورهای در حال توسعه در اتخاذ تدابیر قابل اجرا و مناسب مرتبط با محافظت در برابر تهدیدات سایبری، همکاری و مساعدت نماید. که این همکاری و مساعدت شامل فعالیت های ظرفیت ساز در توسعه و پیشرفت راهبردهای ملی، قوانین و اجرای آنها، ساختارهای سازمانی (به طور مثال هشدار، نظارت و عکس العمل) می باشد (Gercke, 2014: 133). به علاوه اتحادیه ی بین المللی ارتباطات تعدادی کنفرانس منطقه ای را که به طور ویژه به مسئله جرایم سایبری می پردازند را برگزار نمود.<sup>۲</sup>

- قطعنامه ی شماره ی ۱۴۹، صادره در کنفرانس مستقل اتحادیه در آنتالیای ترکیه در سال ۲۰۰۶؛ با موضوع بررسی و مطالعه ی تعاریف و ترمینولوژی در حوزه ی ایجاد اطمینان و امنیت در استفاده از فناوری های ارتباطاتی و اطلاعات<sup>۳</sup>.

- قطعنامه ی شماره ی ۵۰، صادره در مجمع جهانی استانداردسازی ارتباطات<sup>۴</sup> در سال ۲۰۰۸ در ژوهانسبورگ آفریقای جنوبی<sup>۵</sup> درباره ی امنیت سایبری.

---

<sup>1</sup> ITU Resolution 130 (Rev. Guadalajara, 2010).

<sup>۲</sup> از جمله: کنفرانس ۲۰۰۹ سانتا دوینگو نوامبر سال - ۲۰۰۹، جمهوری دومینیک؛ کنفرانس ۲۰۰۹ حیدرآباد نوامبر - ۲۰۰۹، هند؛ کنفرانس ۲۰۰۹ تونس ژوئن - ۲۰۰۹، تونس؛ کنفرانس ۲۰۰۹ ژنو می - ۲۰۰۹، ژنو.

<sup>3</sup> Resolution 149 (Antalya, 2006) – Study of definitions and terminology relating to building confidence and security in the use of information and communication technologies.

<sup>4</sup> World Telecommunication Standardization Assembly

<sup>5</sup> ITU Resoulution 50 (Johannesburg, 2008).

- قطعنامه‌ی شماره‌ی ۵۲، صادره در مجمع جهانی استانداردسازی ارتباطات در سال ۲۰۰۸ در ژوهانسبورگ آفریقای جنوبی؛ با موضوع مواجهه و مبارزه با هرزنامه‌ها.<sup>۱</sup>
- قطعنامه‌ی شماره‌ی ۵۸، صادره در مجمع جهانی استانداردسازی ارتباطات در سال ۲۰۰۸ در ژوهانسبورگ آفریقای جنوبی؛ در مورد تشویق کشورها به ویژه کشورهای در حال توسعه به تشکیل گروه‌های عکس‌العمل سریع رایانه‌ای.<sup>۲</sup>
- قطعنامه‌ی شماره‌ی ۴۵، صادره در کنفرانس توسعه‌ی جهانی ارتباطات<sup>۳</sup> در سال ۲۰۰۶ در دوحه قطر؛ راجع به سازوکارهای افزایش همکاری در امنیت سایبری شامل مبارزه با هرزنامه‌ها.<sup>۴</sup>
- علاوه بر این از حیث همکاری‌های دوجانبه در سال ۲۰۱۱ اتحادیه‌ی بین‌المللی ارتباطات تفاهم‌نامه‌ای را در زمینه‌ی جرایم سایبری با «اداره مبارزه با مواد مخدر و جرایم» سازمان ملل متحد امضاء نمود. این تفاهم‌نامه راجع به همکاری (به ویژه در حوزه‌ی ظرفیت‌سازی و ارائه‌ی مساعدت-های فنی به کشورهای در حال توسعه) و برگزاری کارگاه‌های آموزشی مشترک می‌باشد. همچنین این دو سازمان بر تبادل متقابل و مشترک تحلیل اطلاعات، علوم و داده‌ها توافق نمودند (Ibid, p: 121).

## شورای اروپا

شورای اروپا<sup>۵</sup> که در سال ۱۹۴۹ تأسیس شد و مقر آن در استراسبورگ می‌باشد، نقش بسیار فعالی را در زمینه پرداختن به مسائل و چالش‌های جرایم سایبری ایفا می‌نماید. این شورا سازمانی بین‌المللی با ۴۷ کشور عضو در ناحیه اروپا است. شورای اروپا سازمانی معجزا است. در سال ۱۹۷۹

<sup>1</sup> ITU- WTS Resolution 52- Countering and combating spam

<sup>2</sup> ITU Resolution 58 (Johannesburg, 2008)

<sup>3</sup> World Telecommunication Development Conference

<sup>4</sup> ITU Resolution 45 (Doha, 2006)

<sup>5</sup> Council of Europe

شورای اروپا در کنفرانسی که راجع به «جنبه‌های جرایم اقتصادی» برگزار شده بود، ماهیت بین-المللی جرایم رایانه‌ای را مورد توجه قرار داد.<sup>۱</sup> در سال ۱۹۸۵، شورای اروپا کمیته‌ای تخصصی را<sup>۲</sup> برای بحث در مورد جنبه‌های قانونی و حقوقی جرایم رایانه‌ای تعیین نمود (کنفرانس سازمان ملل در تجارت و توسعه، ۲۰۰۵: ۲۳۳). در سال ۱۹۸۹، «کمیته ی اروپایی بررسی مشکلات جرایم»<sup>۳</sup>، گزارشی در مورد جرایم رایانه‌ای که مقررات حقوقی کیفری ماهوی ضروری در راستای مبارزه با اشکال جدید جرایم الکترونیکی - شامل کلاهبرداری و جعل رایانه‌ای - تجزیه و تحلیل نموده بود را منتشر کرد. همچنین «کمیته وزیران شورا»<sup>۴</sup>، در سال ۱۹۸۹ توصیه نامه ی شماره ۹(۸۹) را که مشخصاً به ماهیت بین‌المللی جرایم رایانه‌ای می‌پرداخت را صادر نمود.<sup>۵</sup> به موجب این توصیه‌نامه: «کمیته ی وزیران وفق مفاد بند ب از ماده ی ۱۵ اساسنامه ی شورای اروپا، با در نظر گرفتن این که هدف شورا دستیابی به یکپارچگی بیشتر بین اعضایش می‌باشد اهمیت نشان‌دادن عکس‌العمل مناسب و سریع به چالش‌های نوین جرایم مرتبط با رایانه (توجه به این که جرایم رایانه‌ای اغلب خصوصیتی فرامرزی دارند)، آگاه بودن از نیاز برای یکسان‌سازی و هماهنگی بیشتر قوانین و رویه‌ها و همچنین بهبود همکاری‌های حقوقی بین‌المللی را مورد شناسایی قرار می‌دهد و به دول عضو توصیه می‌نماید:

---

<sup>۱</sup> دوازدهمین کنفرانس مدیران موسسات تحقیقاتی جرم‌شناسی: جنبه‌های جرم شناختی جرایم اقتصادی در استراسبورگ، ۱۹۷۶.

<sup>۲</sup> کمیته متخصصان شامل ۱۵ عضو به علاوه ناظرانی از ژاپن، کانادا، ایالات متحده، سازمان ملل متحد، سازمان توسعه و همکاری‌های اقتصادی و جامعه اقتصادی اروپا می‌باشد.

<sup>۳</sup> European Committee on Crime Problems

<sup>۴</sup> Committee of Ministers

<sup>۵</sup> Council of Europe, Committee of Ministers, Recommendation No. R (89) 9 (1989)

توصیه‌نامه ی شماره ۹(۸۹)، صادر شده توسط کمیته وزرا در ۱۳ سپتامبر ۱۹۸۹ در چهارصد و بیست و هشتمین نشست وزرا؛ با موضوع جرایم مرتبط با رایانه.

۱- به هنگام بازبینی قوانین و مقررات با وضع قوانین جدید خود، گزارش «کمیته‌ی اروپایی بررسی مشکلات جرایم» در مورد جرایم مرتبط با رایانه، و به ویژه خطوط راهنمای قانونگذاری‌های ملی را مد نظر قرار دهند؛ و

۲- از هرگونه پیشرفت در قانونگذاری‌ها، رویه‌های قضایی و تجربه‌های همکاری حقوقی بین-المللی خود در ارتباط با جرایم رایانه‌ای گزارش جامعی تهیه و به دبیرکل شورای اروپا ارائه نمایند (Gercke, 2014: 134).

علاوه بر توصیه‌نامه‌ی مذکور «کمیته‌ی وزیران شورای اروپا» توصیه‌نامه‌های مرتبط دیگری را نیز صادر نموده است. از جمله: توصیه‌نامه‌های شماره (۸۵) ۱۰ راجع به قطع ارتباطات<sup>۱</sup>، توصیه‌نامه شماره (۸۷) ۱۵ راجع به تنظیم و قاعده‌مند نمودن استفاده از داده‌های شخصی در بخش‌های انتظامی<sup>۲</sup> و توصیه‌نامه‌ی شماره (۹۵) ۴ راجع به حمایت از داده‌های شخصی در حوزه‌ی خدمات ارتباطی<sup>۳</sup>. در سال ۱۹۹۵ نیز این کمیته توصیه‌نامه‌ی دیگری را در مورد مشکلات ناشی از جرایم رایانه‌ای

---

<sup>1</sup> Council of Europe, Ccommittee of Ministers, Recommendation No. R (85) 10 (1985).  
توصیه‌نامه‌ی شماره (۸۵) ۱۰ صادر شده توسط کمیته‌ی وزیران در ۲۸ ژوئن ۱۹۸۵ در سیصد و هشتاد و هفتمین نشست وزرا؛ با موضوع اجرای عملی کنوانسیون اروپا راجع به همکاری‌های متقابل در موضوعات کیفری راجع به قطع ارتباطات.

توصیه‌نامه‌ی شماره (۸۷) ۱۵ صادره در ۱۷ سپتامبر ۱۹۸۷ در چهارصد و دهمین نشست وزیران؛ با موضوع قاعده‌مند-سازی استفاده از داده‌های شخصی در بخش‌های انتظامی.

<sup>2</sup> Council of Europe, Ccommittee of Ministers, Recommendation No. R (87) 15 (1987).

<sup>3</sup> Council of Europe, Ccommittee of Ministers, Recommendation No. R (95) 4 (1995).

توصیه‌نامه‌ی شماره (۹۵) ۴ صادره در ۷ فوریه ۱۹۹۵ در پانصد و بیست و هشتمین نشست وزیران؛ با موضوع حمایت از داده‌های شخصی در زمینه‌ی خدمات ارتباطی به ویژه خدمات تلفنی.

فراملی صادر نمود<sup>۱</sup> که خطوط راهنما برای نگارش قوانین مورد نیاز در ضمیمه این توصیه نامه به طور خلاصه آورده شده است.<sup>۲</sup>

### کنوانسیون جرایم سایبری شورای اروپا و پروتکل الحاقی آن

« کمیته ی اروپایی بررسی مشکلات جرایم»<sup>۳</sup>، در سال ۱۹۹۶ تصمیم به ایجاد کمیته ای متشکل از متخصصین امر برای مقابله با جرایم سایبری گرفت<sup>۴</sup>. در واقع ایده ی اولیه حرکت ورای اصول موجود برای صدور توصیه نامه های دیگر و البته مهم تر از آن پیش نویس نمودن یک کنوانسیون، در زمان تشکیل کمیته ی تخصصی بین سال های ۱۹۹۷ و ۲۰۰۰ شکل گرفت (گزارش تفصیلی از کنوانسیون جرایم سایبری (۱۸۵)، شماره ۱۰). طی این سال ها کمیته مذکور ۱۰ نشست عمومی و ۱۵ نشست با حضور گروه تدوین کننده کنوانسیون برگزار نمود. مجمع شورای اروپا در دومین بخش از نشست های عمومی خود در آپریل سال ۲۰۰۱ پیش نویس کنوانسیون را پذیرفت و متن نهایی کنوانسیون برای تأیید به « کمیته اروپایی بررسی مشکلات جرایم» ارسال گردید و پس از آن متن نهایی کنوانسیون برای تصویب و امضا به کمیته وزیران شورا تسلیم شد. این کنوانسیون برای امضای کشورها در مراسمی با عنوان «مراسم امضاء» در بوداپست مجارستان در ۲۳ نوامبر سال ۲۰۰۱ باز اعلام گردید، که در طول مراسم ۳۰ کشور (از جمله ۴ کشور غیر عضو شورای اروپا یعنی کانادا، ایالات متحده، ژاپن و آفریقای جنوبی که در مذاکرات شرکت کرده بودند) کنوانسیون را امضا نمودند. کنوانسیون جرایم رایانه ای بوداپست در سال ۲۰۰۴ لازم الاجرا گردید و امروزه به عنوان یک سند بین المللی بسیار مهم و تنها سند بین المللی الزام آور برای دول عضو در مبارزه با جرایم سایبری، شناسایی و توسط سازمان های بین المللی متفاوتی حمایت می شود. بدین صورت که اینترنت

<sup>1</sup> Council of Europe, Ccommittee of Ministers, Recommendation No. R (95) 13 (1989)

توصیه نامه ی شماره ۱۳(۹۵) صادر شده توسط کمیته ی وزیران در ۱۳ سپتامبر ۱۹۸۹ در پانصد و چهل و سومین نشست وزیران؛ با موضوع مشکلات آیین دادرسی کیفری مرتبط با فناوری اطلاعات.

<sup>۲</sup> «خطوط راهنما» مذکور با ابزارهای پیگیری (برای مثال جستجو و توقیف) و ادله الکترونیک و همکاری های بین المللی سر و کار دارد.

<sup>3</sup> The European Committee on Crime Problems

<sup>۴</sup> رأی شماره ۱۰۳ / ۲۱۱۱۹۶ کمیته ی مشکلات جرایم اروپا.

بر اهمیت کنوانسیون جرایم سایبری در بیانیه‌ی ششمین کنفرانس بین‌المللی در مورد جرایم سایبری که در قاهره مصر برگزار گردید، بدین شرح تاکید کرده است: «کنوانسیون جرایم سایبری شورای اروپا باید به کمیته‌ی تدوین قوانین بین‌المللی پیشنهاد گردد و به عنوان استاندارد و معیار در جهت مبارزه با جرایم سایبری در نظر گرفته شود و کشورها باید برای پیوستن به آن تشویق شوند. و این که این کنوانسیون باید بین تمامی کشورهای عضو اینترپل در چهار زبان رسمی توزیع گردد»<sup>۱</sup>؛ یا «اجلاس جهانی جامعه‌اطلاعاتی» در دستور جلسه خود در اجلاس سال ۲۰۰۵ که در تونس برگزار شد بیان داشت: «ما از کشورها در همکاری با یکدیگر برای توسعه‌ی قانونگذاری‌های مورد نیاز با هدف پیگیری و تعقیب جرایم سایبری دعوت می‌کنیم، تا با ملاحظه به چهارچوب‌های موجود، برای مثال، قطعنامه‌های شماره ۵۵/۶۳ و ۵۶/۱۲۱ مجمع عمومی سازمان ملل متحد راجع به مبارزه با جرایم سوء استفاده از فناوری‌های اطلاعات و ارتباطات، و ابتکارات منطقه‌ای شامل (نه محدود به) کنوانسیون جرایم سایبری شورای اروپا اقدام نمایند<sup>۲</sup>؛ یا این که سازمان همکاری اقتصادی آسیا - اقیانوسیه برای مطالعه‌ی جرایم سایبری از اقتصاددانان دعوت به عمل آورده است» (دستورات مورد بحث امنیت سایبری جهانی، ۲۰۰۸: ۱۸). سازمان همکاری کشورهای آمریکایی نیز از کشورهای عضو برای ارزیابی کنوانسیون به هنگام وضع قوانین مربوط، دعوت به عمل آورده است (همان، ص ۱۹).

همچنین در نوامبر سال ۲۰۰۲، پروتکل الحاقی به کنوانسیون جرایم سایبری تدوین و آماده امضا گردید<sup>۳</sup>. در طول مذاکرات در خصوص متن کنوانسیون مشخص شد که جرم‌انگاری جرایمی مانند نژادپرستی و انتشار محصولات بیگانه‌ستیزی مسئله‌ی بحث برانگیزی بوده است<sup>۴</sup>، چرا که برخی

<sup>۱</sup> [http://www.interpol.com/Public/TechnologyCrime/Conferences/6thIntConf/Resolution\\_Asp](http://www.interpol.com/Public/TechnologyCrime/Conferences/6thIntConf/Resolution_Asp) (visited on 11.5.1394).

<sup>۲</sup> [http://ec.europa.eu/information\\_society/activities/internationalrel/docs/wsis/tunis\\_agenda.pdf](http://ec.europa.eu/information_society/activities/internationalrel/docs/wsis/tunis_agenda.pdf) (visited on 11.5.1394).

<sup>۳</sup> پروتکل الحاقی به کنوانسیون جرایم سایبری در خصوص جرم‌انگاری اعمال نژادپرستی و موضوعات بیگانه‌ستیزی ارتکاب یافته از طریق رایانه. ETS شماره ۱۸۹.

<sup>۴</sup> گزارش تبیینی پروتکل الحاقی به کنوانسیون جرایم سایبری اروپا، شماره ۴ کمیته‌ی نگارنده کنوانسیون احتمال.

کشورها که حمایت شدیدی از اصل آزادی بیان داشتند نگرانی خود را در خصوص این که اگر مقررات ناقص این اصل در کنوانسیون باشد آن را امضا نخواهند کرد، بیان نمودند (کنفرانس تجارت و توسعه ی سازمان ملل، ۲۰۰۵: ۲۳۴). در چهارمین نسخه پیش نویس، از سال ۱۹۹۸ کنوانسیون همچنان شامل مقرره‌ای بود که طرفین را ملزم می ساخت موضوع محتوای مجرمانه به ویژه در خصوص هزینه نگاری کودکان و دشمنی های نژادپرستانه<sup>۱</sup> را جرم انگاری نماید و به جهت اجتناب از وقوع شرایطی که مانع از امضای سایر کشورها به دلائل مرتبط با آزادی بیان گردد، موضوعات این چنینی در طول روند نگارش از کنوانسیون حذف و در پروتکل دیگری گنجانده شدند. به هر حال پروتکل مذکور در ژانویه سال ۲۰۰۳ برای امضا گشوده شد و در مارچ ۲۰۰۶ لازم الاجرا گردید. همچنین تا آغاز سال ۲۰۱۵، ۲۲ کشور آن را تصویب و ۱۳ کشور آن را بدون تصویب امضاء نمودند (Gercke, 2012: 26).

کنوانسیون جرایم سایبری شورای اروپا دارای ۴ فصل است که فصل اول آن راجع به تعریف واژه های تخصصی، فصل دوم آن در مورد حقوق کیفری ماهوی (انواع جرایم رایانه ای) و حقوق کیفری شکلی (آئین دادرسی کیفری) می باشد. در فصل سوم به همکاری های بین المللی اشاره شده و فصل چهارم کنوانسیون راجع به مقررات مربوط به امضا، لازم الاجرا شدن و الحاق به کنوانسیون می باشد. در مقدمه کنوانسیون آمده است:

«دولت های امضاکننده این کنوانسیون با هدف دستیابی به اتحاد فراگیر میان اعضا و یا اعتقاد به ضرورت اتخاذ سیاست های جنایی عمومی در حمایت از جامعه در برابر جرایم سایبری، به تصویب قوانین مناسب و گسترش همکاری های بین المللی اقدام کرده و با آگاهی از تحولات شگرفی که در اثر همگرایی و تداوم روند جهانی شدن شبکه های رایانه ای و داده های الکترونیکی به منظور ارتکاب جرایم و با احساس نیاز به همکاری بین دولت ها و بخش های خصوصی در زمینه مبارزه با جرایم سایبری و حمایت از منافع مشروع در توسعه ی فناوری اطلاعات در راستای تصویب قوانین

<sup>۱</sup> ماده ۳ چهارمین پیش نویس کنوانسیون

یکپارچه و یکسان در این زمینه گام بر می‌دارند». این کنوانسیون توصیه می‌نماید دولت‌های امضا-کننده از طرق مختلف و ممکن در موارد لزوم بخصوص در مسایل مربوط به ارائه ادله جرم و اعلام دقیق محل وقوع آن با یکدیگر مساعدت نمایند. همچنین در این سند هماهنگ‌سازی بین حقوق کیفری داخلی و مقررات یکپارچه بین‌المللی در خصوص عناصر تشکیل‌دهنده جرایم سایبری به چشم می‌خورد.

محتوای کنوانسیون در ۴ بخش و ۴۸ ماده دسته‌بندی شده‌اند که عبارتند از:

۱. استفاده از اصطلاحات؛

۲. اقدامات داخلی کشورها (که در ۳ بخش قوانین ماهوی، قانون آئین دادرسی کیفری و

صلاحیت آمده است)؛

۳. همکاری بین‌المللی؛

۴. مقررات نهایی<sup>۱</sup>

اهداف کنوانسیون بوداپست نیز شامل موارد ذیل ذکر شده‌اند:

الف - هماهنگی ارکان تشکیل‌دهنده جرم در حقوق جزای ماهوی داخلی کشورها و مسایل

مربوط به بخش جرایم فضای سایبری؛

ب- فراهم آوردن اختیارات لازم آئین دادرسی کیفری داخلی برای پیگیری و تعقیب جرایمی

که با استفاده از سیستم‌های رایانه‌ای انجام می‌شود با مدارک مرتبط با جرم به شکل الکترونیکی

است؛

ج- تدوین سیستم سریع و موثر برای همکاری‌های بین‌المللی (باقری اصل، ۱۳۸۴: ۷)

کنوانسیون بوداپست

کنوانسیون بوداپست به نام «پیمان جرایم اینترنتی بین‌المللی» نیز معروف است و اولین پیمان

بین‌المللی ایجاد شده برای مقابله با جرایم اینترنتی است که حدود ۴۰ کشور مختلف در کنفرانس

بین‌المللی بوداپست با موضوعیت جرائم اینترنتی در ۲۳ نوامبر ۲۰۰۱ در مجارستان آن را امضاء

<sup>1</sup> Council of Europe, Convention on Cybercrime, Budapest 23.11.2001



کردند که از آن پس این پیمان به نام پیمان بوداپست معروف شد. این پیمان شامل تعاریف دقیق برای همه نوع از جرایم اینترنتی است و کیفر مربوط به هر کدام نیز مشخص شده است. در این پیمان سیستم کامپیوتری دسترسی غیرقانونی به اطلاعات، نقض قانون مالکیت معنوی تولید و پخش ویروس کامپیوتری و ترویج پورنوگرافی کودکان به عنوان یک عمل مجرمانه تعریف شده است و کشورها را موظف به الحاق به این قانون و ممنوعیت این گونه جرم‌ها در قوانین داخلی خود می‌سازد. همه کشورهایی که این پیمان را امضاء کرده‌اند قانون و مقررات یکسانی برای کنترل جرایم اینترنتی داشته و جهت همکاری بین المللی یک خط تلفن استاندارد برای این بخش فراهم کرده‌اند. دستاورد این پیمان این است که تغییراتی عملی یا بهتر بگوییم انقلابی در قانونگذاری جرایم اینترنتی ایجاد کرده است. شورای اروپا در حدود ۲۰۰۶ پروژه‌ای جهانی در مورد جرایم اینترنتی راه‌اندازی کرد که به منظور تقویت ثبات داخلی بر اساس پیمان بوداپست طراحی شده بود. انقلاب قانونی و نهادی در مورد جرائم اینترنتی به حدود ۱۲۰ کشور مختلف توصیه شد؛ تحت تأثیر این فرایند مجمع عمومی سازمان ملل متحد، پیمان بوداپست را به عنوان پایه‌ای برای توسعه قانون و نهادی برای تحقیق و تعقیب جرایم اینترنتی ذکر کرده است و الحاق به آن را به تمام کشورهای جهان پیشنهاد کرد. سازمان ملل متحد نقش پیشگام در استانداردسازی پیمان بوداپست و مدیریت بهبود آن را بر عهده داشته است.

### **کنوانسیون حمایت از کودکان در برابر سواستفاده و بهره‌کشی جنسی**

شورای اروپا در راستای رویکرد خود با هدف بهبود حمایت از اطفال در برابر سواستفاده جنسی، کنوانسیون جدیدی را در سال ۲۰۰۷ تدوین نمود<sup>۱</sup>. یکی از اهداف کلیدی کنوانسیون، یکسان‌سازی آن دسته از مقررات قوانین کیفری است که در مورد حمایت از کودکان در برابر سواستفاده‌های جنسی می‌باشند و برای رسیدن به این هدف، کنوانسیون مجموعه‌ای از قوانین کیفری را پیش‌بینی نموده است. جدا از جرم‌انگاری سواستفاده جنسی از کودکان (ماده ۱۸)، کنوانسیون در بردارنده ی

---

<sup>1</sup> Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (2007)

ماده‌ای در خصوص جرم دانستن تبادل هرزه‌نگاری کودکان (ماده ۲۰) و همچنین درخواست از کودکان برای مقاصد جنسی (ماده ۲۳) می‌باشد (Gercke, 2009: 95).

- در بند یک از ماده ۲۰ کنوانسیون آمده است: هر کشور عضو می‌بایست هرگونه اقدام لازمی (از جمله قانونگذاری یا سایر اقدامات) را به منظور تضمین این که اقدامات عمدی زیر در صورت ارتکاب، جرم شناخته خواهند شد را اتخاذ نماید:

الف - تولید محصولات هرزه‌نگاری کودکان؛

ب- سفارش یا قابل دسترسی نمودن محصولات هرزه‌نگاری کودکان؛

ج- انتشار یا تجارت محصولات هرزه‌نگاری کودکان؛

د- تأمین محصولات هرزه‌نگاری کودکان؛

ه - در اختیار داشتن محصولات هرزه‌نگاری کودکان؛ و

ی - دستیابی آگاهانه به محصولات هرزه‌نگاری کودکان از طریق فناوری‌های ارتباطاتی و

اطلاعاتی<sup>۱</sup>

- ماده ی ۲۳: هر کشور عضو باید هرگونه اقدام لازمی (از جمله قانونگذاری یا سایر اقدامات) را به منظور جرم‌انگاری درخواست عمدی - از طریق فناوری‌های اطلاعاتی و ارتباطاتی - از یک فرد بالغ برای ملاقات با کودکی که به سن مندرج در بند ۲ ماده ۱۸ این کنوانسیون نرسیده است و به منظور ارتکاب هریک از جرایم مذکور در قسمت الف بند یک ماده ۱۸ یا بند یک ماده ۲۰ علیه وی انجام می‌گیرد را صورت دهد.

روند تدوین قانون جرایم رایانه‌ای در ایران

با توجه به پیشرفت سریع رایانه و کاربردهای متعدد و متنوع در بخش‌های مختلف امکان سواستفاده از این صنعت و عدم پاسخگویی قوانین مرسوم کیفری به مسائل جرم رایانه‌ای، در جریان بازنگری بخشی از قانون مجازات اسلامی، (تعزیرات) هیات محترم وزیران مقرر ساخت تا در

<sup>1</sup> Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (2007), Art 20 and 23.

خصوص جرایم رایانه‌ای نیز بررسی‌های لازم صورت گرفته و چنانچه پیشنهادهای مشخصی وجود دارد به متن لایحه ی جدید تعزیرات افزوده شود. دو متن پیشنهاد گردید، یکی توسط دبیرخانه شورای عالی انفورماتیک و دیگری به وسیله ی بانک مرکزی که متون پیشنهادی در کمیسیون لوایح دولت بررسی گردید و در نهایت یک لایحه با عنوان «چگونگی برخورد با جرایم رایانه‌ای» در جلسه هیات وزیران مورخ ۱۳۷۳/۶/۶ به تصویب رسید که طبق آن فصلی با ۲ ماده به قانون مجازات اسلامی افزوده می‌شود. متأسفانه این لایحه در مجلس شورای اسلامی به تصویب نرسید. با وجود تلاش متخصصان و حقوقدانان کشور، فصل یا قانونی با این عنوان به قانون مجازات اسلامی افزوده نشد.

تقریباً از اواخر دهه ۷۰ و ابتدای ۱۳۸۰ تدابیر گوناگونی در رده‌های حاکمیتی کشور در خصوص ضرورت مقابله با سواستفاده‌های مجرمانه سایبری اتخاذ شده که مهم‌ترین آن ابلاغیه ۷ ماده‌ای مقام معظم رهبری درباره ی شبکه‌های اطلاع‌رسانی رایانه‌ای در سال ۱۳۸۰ است که می‌توان از آن به عنوان منشور سیاست جنایی ملی جرایم رایانه‌ای یاد کرد. این سیاست‌نامه، علاوه بر جنبه‌های کیفری موضوع، حاوی تدابیر پیشگیرانه و ارزشمندی است که توجه و پایبندی به آن می‌تواند مشکلات این حوزه را تا حد زیادی برطرف کند. در سخنرانی مورخ ۱۳۹۰/۱۲/۱۷ نیز رهبر معظم انقلاب در خصوص فضای مجازی چنین ایراد فرمودند: «گسترش فزاینده فناوری‌های اطلاعاتی و ارتباطاتی به ویژه شبکه ی جهانی اینترنت و آثار چشمگیر آن در ابعاد زندگی فردی و اجتماعی، و لزوم سرمایه‌گذاری وسیع و هدفمند در جهت بهره‌گیری حداکثری از فرصت‌های ناشی از آن در جهت پیشرفت همه‌جانبه کشور و ارائه خدمات گسترده و مفید به اقشار گوناگون مردم و همچنین ضرورت برنامه‌ریزی و هماهنگی مستمر به منظور صیانت از آسیب‌های ناشی از آن اقتضا می‌کند که نقطه‌ی کانونی متمرکزی برای سیاست‌گذاری، تصمیم‌گیری و هماهنگی در فضای مجازی کشور به وجود آید».

از سال ۱۳۸۱ فعالیت مجدد حوزه ی جرایم رایانه‌ای آغاز گردید که به تنظیم پیش‌نویس جرایم رایانه‌ای در شورای عالی توسعه ی قضایی قوه ی قضاییه منجر شد و نهایت لایحه ی جرایم رایانه‌ای

بعد از گذشت ۱۵ سال (از زمان تصویب آن در هیات وزیران آن زمان) توسط شورای عالی توسعه‌ی قضایی تهیه و پیشنهاد گردید که در خردادماه ۱۳۸۸ به تصویب مجلس شورای اسلامی و مورد تایید شورای نگهبان قرار گرفت.

این قانون (قانون جرایم رایانه‌ای) مشتمل بر سه بخش و پنجاه و چهار ماده است و در بخش یکم این قانون به جرایم و مجازات مقرر در قانون می‌پردازد و در هفت فصل جرایم، به تقسیم‌بندی و در فصل هشتم موارد تشدید مجازات را مطرح می‌کند. فصل یکم با عنوان جرایم، علیه محرمانگی داده‌ها و سامانه‌های رایانه‌ای و مخابراتی دسترسی غیر مجاز، شنود غیر مجاز و جاسوسی رایانه‌ای را از مصادیق این نوع جرم شناخته و حداکثر مجازات این گونه جرایم توسط افراد عادی را بیست میلیون ریال تا شصت میلیون ریال جزای نقدی و از یک تا سه سال حبس در نظر گرفته است. عنصر مادی این گونه جرایم، شبیه جرایم علیه امنیت در فضای واقعی است و فقط ابزار جرم تغییر یافته است.

قانونگذار در فصل دوم و سوم جرایم، علیه صحت و تمامیت داده‌ها و سامانه‌های مخابراتی را عنوان نموده که عنصر مادی این نوع جرایم را می‌توان مانند جرایم علیه اموال و مالکیت دانست. قانونگذار در این فصول، جرایم همچون جعل رایانه‌ای، تخریب و اختلال در سامانه‌های رایانه‌ای و سرقت و کلاهبرداری مرتبط با رایانه را مطرح نموده و حداکثر مجازات را برای جعل رایانه‌ای، حبس از یک تا پنج سال و جزای نقدی از بیست میلیون ریال تا یکصد میلیون ریال در نظر گرفته است. به نظر می‌رسد با توجه به این که جرایم رایانه‌ای مانند سرقت و کلاهبرداری رایانه‌ای ابتدا با جعل یک سایت مشهور شروع می‌شود قانونگذار چنین مجازات سنگینی را نسبت به دیگر جرایم در این بخش در نظر گرفته است.

فصل چهارم قانون، به جرایم علیه عفت و اخلاق عمومی پرداخته و مصادیق محتویات مستهجن را بیان نموده است. عنصر مادی این جرایم مانند جرایم علیه عفت عمومی و ماده ۶۴۰ قانون مجازات اسلامی می‌باشد. حداکثر مجازات در نظر گرفته شده برای این گونه جرایم، حبس از نود و یک روز تا یکسال و جزای نقدی از پنج میلیون تا بیست میلیون ریال است.

فصل پنجم به مصادیق جرم هتک حیثیت و نشر اکاذیب به وسیله‌ی سامانه‌های رایانه‌ای پرداخته که عنصر مادی این گونه جرایم مانند مواد ۶۹۷ تا ۷۰۰ قانون مجازات اسلامی می‌باشد.

در فصل ششم مواد ۷۶۷ تا ۷۵۲ قانون مجازات اسلامی، قانونگذار مسئولیت کیفری اشخاص حقیقی و حقوقی مانند شرکت‌های ارائه‌دهنده‌ی خدمات دسترسی را مشخص نموده و عدم تأمین نظر قانونگذار را جرم تلقی و حتی مجازات جزای نقدی تا یک میلیارد ریال و تعطیلی موقت در نظر گرفته است. از آنجایی که نوع خدمات این گونه شرکت‌ها نقش به‌سزایی در کنترل جرایم سایبری دارند و در صورتی که موازین قانونی و اخلاقی را مانند پالایش سایت‌های غیراخلاقی، رعایت نمایند خسارات مادی و معنوی زیادی به جامعه وارد خواهد شد؛ قانونگذار چنین ضمانت اجرایی سنگینی را به نسبت سایر جرایم تعیین نموده است. ضمناً در این فصل، قانون کارگروهی را برای بررسی محتوای مجرمانه فضای سایبری تعیین نموده که این کارگروه به ریاست دادستان کل کشور دوبار در ماه تشکیل جلسه می‌دهد و مصادیق پالایش را رسیدگی می‌نماید. این کمیته وظیفه دارد هر شش ماه در خصوص پرونده‌ی پالایش محتوای مجرمانه گزارشی را به روسای قوای سه‌گانه و شورای عالی امنیت ملی تقدیم کند.

در فصل هفتم مواردی مانند توزیع و انتشار ویروس، معامله نرم‌افزار، آموزش تخریب در سامانه‌های رایانه‌ای و مجازات حبس از نود و یک روز تا یکسال و جزای نقدی پنج میلیون ریال تا بیست میلیون ریال پیش‌بینی شده است.

در فصل هشتم و قسمت آخر بخش یکم، مواردی همچون کارمند دولت یا عضویت نیروهای مسلح یا مقامات قضایی و به طور کلی عضویت رسمی و غیررسمی قوای سه‌گانه را که به مناسبت انجام وظیفه مرتکب جرم رایانه‌ای شده‌اند و نیز تکرار جرم برای بیش از دو بار را جزء تشدید مجازات قلمداد نموده که مرتکب را به بیش از دو سوم حداکثر یک یا دو مجازات مقرر در قانون محکوم می‌نماید. در بخش دوم، قانونگذار، آیین دادرسی برخورد با جرایم رایانه‌ای را مشخص کرده و در ابتدا، اصل سرزمینی بودن و جرایم علیه حاکمیت جمهوری اسلامی را مطرح می‌کند و در ادامه نحوه‌ی حفظ ادله‌ی جرم، تفتیش و توقیف سامانه‌های رایانه‌ای را توسط ضابطان و نیز

وظایف شرکت‌های ارائه‌دهنده‌ی خدمات اینترنتی را در حفظ داده‌ها و اطلاعات رایانه‌ای مشخص می‌نماید. ضمناً اینکه ضابطین موظف به رعایت حریم خصوصی افراد بوده و در صورتی که ضابط برابر دستور مقام قضایی عمل نکرده باشد، مجازات‌های لازم پیش‌بینی شده است.

می‌توان گفت در حوزه‌ی برخورد با جرایم سایبری از نظر قانون مشکل خاصی وجود ندارد تنها در خصوص برخی از جرایم مانند جرایم علیه عفت و اخلاق عمومی و یا انتشار ویروس رایانه‌ای، مجازات‌های خفیفی در نظر گرفته شده که بایستی با توجه به گستردگی این فضا و حجم خسارت‌هایی که وارد می‌آید تناسب جرم و مجازات رعایت و در مجازات‌ها تجدید نظر شود. در آخر می‌توان به این نکته اشاره کرد که رسیدگی به پرونده‌های جرایم رایانه‌ای در تهران و در دادسرای ویژه مبارزه با جرایم رایانه‌ای صورت می‌گیرد و امید است با تلاش مسئولان در سایر نقاط کشور نیز راه‌اندازی دادسراهای مشابه تسری یابد.

مفهوم سیاست جنایی تقنینی در پیشگیری از جرایم سایبری:

پیدایش اصطلاح «سیاست جنایی» توسط فون‌رباخ<sup>۱</sup>، حقوقدان آلمانی در پایان قرن هجدهم میلادی به همین «حکمت‌گرایی» در برخورد با جرم مربوط بوده و زاینده آن است. واژه «سیاست» که متضمن مفهوم اندیشیدگی، هدایت‌شدگی و غایت‌دار بودن است با معنای ویژه‌ای که به اصطلاح «سیاست جنایی» داده موجب پذیرش و رواج این اصطلاح در زبان حقوقی و جامعه‌شناسی امروز شده است. همانند رواج اصطلاحاتی از قبیل «سیاست اقتصادی» و «سیاست فرهنگی».

یکی از مهمترین سیاست‌های جنایی ایران در پیشگیری از جرایم رایانه‌ای بحث قانونگذاری آن در همین حوزه می‌باشد. قانونگذاری در فضای سایبری را با رویکردی در سه مرحله می‌توان تبیین کرد. قانونگذاری در روش‌های حقوق کیفری باید با شناخت به کارگیری فناوری جدید شروع شود و بخش‌های ویژه به همراه ساختارهای امنیتی انتظامی یا در مفهوم کلی پلیس مورد نیاز می‌باشند که برای بررسی جرایم سایبری دارای شرایط لازم باشند.

<sup>۱</sup> اصطلاح سیاست جنایی برای اولین بار توسط آنسلیم فون فون‌رباخ (Anselm von Feuerbach) در کتاب حقوق کیفری او که در سال ۱۸۰۳ میلادی منتشر گردید به کار برده شد.

پی ریزی قانون موثر، مقایسه قانون کیفری در قوانین موضوعه با نیازهای برخاسته از انواع جدید تخلفات جنایی ضروری است. در موارد زیادی، قانون های موجود ممکن است نتوانند تغییرات جدید جرایم موجود را پوشانند.

مرحله ی سوم نگارش قوانین جدید است. براساس تجربه ممکن است برای مراجع قانونی اجراکردن فرآیند نگارش قانون برای جرایم سایبری بدون همکاری بین المللی به دلیل رشد سریع فناوری شبکه و ساختارهای پیچیده آنها سخت و مشکل است. نگارش قوانین جرایم سایبری به طور جداگانه ممکن است به تعارض قوانین و هدر رفتن منابع منجر گردد و همچنین دنبال کردن توسعه ی استراتژی ها و استانداردهای بین المللی ضروری است.

بر همین مبنا می توان گفت تقسیم بندی جرایم رایانه ای از یک سو شامل جرایم علیه اشخاص، علیه اموال و جرایم علیه امنیت و آسایش عمومی و از طرف دیگر جرایم نرم افزار، جرایم داده ها و جرایم علیه حقوق خصوصی فردی می باشند. از این رو، به منظور پیشگیری از جرایم رایانه ای سیاست جنایی ایران در بحث قانونگذاری بر این است که با تقنین و وضع قوانین در همین حوزه از ارتکاب جرم توسط مجرمان بالقوه و بالفعل پیشگیری نماید.

با رشد جرایم رایانه ای و نوظهور در عصر کنونی پلیس به عنوان یکی از ارکان موثر در سیاست قضایی کشور نسبت به اصلاح و تحول در ساختار سازمانی خود اقدام نموده است و با توجه به این بحث، به منظور ایجاد امنیت در فضای تولید و تبادل اطلاعات ضمن تحول در ساختار امنیتی و انتظامی یعنی تشکیل پلیس فضای تولید و تبادل اطلاعات، براساس دومین راهبرد از سند راهبردی امنیت فضای تولید و تبادل اطلاعات کشور که در تاریخ ۱۳۸۷/۱۲/۷ به تصویب هیات وزیران رسید برای نیروی انتظامی جمهوری اسلامی ایران وظیفه ای در نظر گرفته شد.

## نتیجه

از این مقاله نتیجه می‌گیریم که جرایم رایانه‌ای نیز مانند سایر جرایم دارای ارکان سه‌گانه‌ی قانونی معنوی و مادی هستند؛ یعنی برای تحقق این جرایم نیز این سه عنصر باید وجود داشته باشد. البته در بین عناصر مذکور عنصر قانونی بحث برانگیزتر است. دیدیم که اغلب کشورها ناچار شدند در زمینه‌ی جرایم مذکور قانون وضع کنند و حتی برخی از آن‌ها به اصلاح همان قوانین جدید مبادرت ورزیده‌اند. با توجه به استدلالات مذکور در متن نوشتار به این نتیجه رسیدیم که در حقوق نیز باید قوانین لازم در مورد جرایم رایانه‌ای توصیف شوند شاید در مرحله‌ی نخست چنین به نظر می‌رسد که تجاوزات به سخت‌افزار از حیثه‌ی رایانه‌ای بیرون است؛ ولی باید گفت سخت‌افزار بدون داده و نرم‌افزار کمترین اهمیتی ندارد دیگر این که سخت‌افزار اجرا کننده‌ی برنامه و پردازش-کننده‌ی داده‌ها و محلی برای نگه‌داری آن‌ها است. از این نظر لازم است تا در بحث جرایم رایانه‌ای مطرح شود اما آن‌چه که بیشتر مدنظر مجرمان است داده‌ها و برنامه‌ها است. بنابراین در مورد برنامه‌ها به‌عنوان اصلی‌ترین موضوع مورد نظر متجاوزان باید دقت و توجه خاصی از طرف قانونگذار صورت پذیرد. بخشی از مرتکبین جرایم رایانه‌ای متخصصان و اهل فن هستند هدفی که این دسته دنبال می‌کنند واقعاً مجرمانه نیست؛ بلکه نتیجه‌ی کار آن‌ها اغلب منتهی به یک اکتشاف و نوآوری می‌گردد. این نکته مسلم است که قابلیت‌های تکنولوژی به کشورها این امکان را داده تا به داده‌های موجود در کشورهای دیگر دست یابند به عبارتی مسئله دستیابی به این داده‌ها از لحاظ فنی امری گریزناپذیر است؛ بنابراین به‌جای ممنوع ساختن دستیابی داده‌ها آن را تحت نظم و قاعده درآورد نظم و قاعده به این موضوع در حقیقت همان جمع کردن بین دو مسئله ضرورت تحقیق و حاکمیت دولت دارنده داده است. به این ترتیب کشورها و به خصوص کشورهایی که میزان وابستگی اجتماعی و اقتصادی آن‌ها به محیط سایبر بیشتر است به اصلاح یا وضع قوانین کیفری در این زمینه اقدام کرده‌اند. احساس این وابستگی به محیط سایبر در کشور ما نیز هر روز افزون‌تر می‌گردد و به این ترتیب باید بر آن بود که حقوق ایران نیز باید در راستای حمایت از امنیت داده‌ها و سیستم‌های رایانه‌ای کاربران، دستگاه‌های دولتی، نهادهای عمومی و موسسات خصوصی به وضع قوانین کیفری



یا اصلاح قوانین موجود اقدام نماید تا به این ترتیب موجبات امنیت داده‌ها و شبکه‌های رایانه‌ای و در نتیجه رشد و توسعه ی اجتماعی و اقتصادی کشور را در محیط سایبر فراهم آورد.

## پیشنهاد و راهکارها

جرایم سایبری مستلزم مبارزه فراملی و فرامرزی از سوی پلیس و قضات است. برای جرایم سایبری باید قوانین منسجم جداگانه، تدوین و تضمین شود این قوانین شامل ابعاد ماهوی و شکلی بین‌المللی به علاوه ضمانت اجراهای جزایی برای کپی‌رایت حمایت از داده‌ها و... می‌شود.

باید پلیس و قضات به صورت تخصصی آموزش ببینند؛ آموزش تخصصی پلیس از بدو تحصیلات نظامی باید شروع شود و به صورت تخصصی تر پلیس جرایم سایبری برای هر جرم سایبری به طور جداگانه وجود داشته باشد. مثلاً پلیس متخصص کلاهبرداری سایبری، پلیس متخصص جعل سایبری و به تبع قضات متخصص هم باید وجود داشته باشند.

باید در واحدهای تخصصی مبارزه با جرایم رایانه‌ای و سایبری در نیروی انتظامی، وزارت اطلاعات، وزارت دفاع و فرماندهی نیروهای مصلح تجهیزات روزآمد و لازم به کار گرفته شود و اگر چنین واحدهایی تأسیس نشده است بدو این واحدها تأسیس و تجهیز شوند.

باتوجه به این که فناوری اطلاعات و ارتباطات فضای جدیدی را برای متخلفان جامعه فراهم کرده‌اند. ازاین رو، بر سیاست‌گذاران و مدیران جوامع است که برای این مشکل راهکارهای قانونی و اجرایی تدارک ببینند.

به منظور مهار کردن جرایم رایانه‌ای در سطح جهانی لازم است تاکید کشورها دارای قوانین مصوب بوده و سعی شود قوانین تاحد توان همگرایی داشته باشند در این رابطه اقدام به ایجاد یک الگوی جهانی ضروری به نظر می‌رسد.

دستورات مورد بحث امنیت سایبری جهانی / گروه متخصصان حرفه ای، گزارش استراتژیک

مشارکت عمومی جامعه به‌ویژه بخش خصوصی ضمانت اجرایی قوانین و طرح آموزش‌ها را قویاً تقویت می‌نمایند.

قوانین جرایم رایانه‌ای و نیز طرح ملی آموزش‌های عمومی در کشورها توسط شورای متشکل از سازمان‌های علمی و صنعتی، تجاری، امنیتی و خدماتی تدوین می‌گردد.

در بسیاری از کشورها مراکز با عنوان مراکز مراقبت از سامانه‌های حساس اطلاعاتی و مراکز و واکنش سریع رایانه‌ای فعالیت می‌کنند؛ این مراکز از جانب دانشکده‌های برق، رایانه و حقوق، حمایت علمی و از جانب سازمان‌های دفاعی و امنیتی، حمایت‌های مالی و سیاسی دریافت می‌کنند. دولت‌ها ضمن ایجاد بستر قانونی، اجرایی و قضایی برای رسیدگی امر جرایم رایانه‌ای موظف به ایجاد اطمینان از گردش اطلاعات مناسب بین سازمان‌های دولتی، سیاست‌گذاری مجرمان قانون و بخش خصوصی از جمله وظایف خطیر دولت‌ها ترویج فرهنگ رعایت اخلاق در محیط زندگی و کار در فضای اطلاعاتی جدید است.

## منابع

فارسی:

- باقری اصل، رضا، «کنوانسیون جرایم سایبر و گزارش توجیهی آن»، گروه ارتباطات و فناوری های نوین، گروه کارشناسان، کمیسیون حقوقی و قضایی مجلس، شماره ۷۶۴۶، ۱۳۸۴، ص ۷.
- پروتکل الحاقی به کنوانسیون جرایم سایبری در خصوص جرم‌انگاری اعمال نژادپرستی و موضوعات بیگانه‌ستیزی ارتکاب یافته از طریق رایانه. ETS شماره ۱۸۹.
- توصیه‌نامه ی شماره (۸۹) ۹، صادر شده توسط کمیته ی وزیران در ۱۳ سپتامبر ۱۹۸۹ در چهارصد و بیست و هشتمین نشست وزرا؛ با موضوع جرایم مرتبط با رایانه.
- توصیه‌نامه ی شماره (۸۵) ۱۰ صادر شده توسط کمیته ی وزیران در ۲۸ ژوئن ۱۹۸۵ در سیصد و هشتاد و هفتمین نشست وزرا؛ با موضوع اجرای عملی کنوانسیون اروپا راجع به همکاری‌های متقابل در موضوعات کیفری راجع به قطع ارتباطات.
- توصیه‌نامه ی شماره (۸۷) ۱۵ صادره در ۱۷ سپتامبر ۱۹۸۷ در چهارصد و دهمین نشست وزیران؛ با موضوع قاعده‌مندسازی استفاده از داده‌های شخصی در بخش‌های انتظامی.
- توصیه‌نامه ی شماره (۹۵) ۴ صادره در ۷ فوریه ۱۹۹۵ در پانصد و بیست و هشتمین نشست وزیران؛ با موضوع حمایت از داده‌های شخصی در زمینه ی خدمات ارتباطی به ویژه خدمات تلفنی.
- توصیه‌نامه شماره (۹۵) ۱۳ صادر شده توسط کمیته ی وزیران در ۱۳ سپتامبر ۱۹۸۹ در پانصد و چهل و سومین نشست وزیران؛ با موضوع مشکلات آیین دادرسی کیفری مرتبط با فناوری اطلاعات.
- حسینی خواه، نورالله، ۱۳۹۰، پلیس و جرایم رایانه ای، تهران: انتشارات معاونت تربیت و آموزش ناجا.
- خداقلی، زهرا، جرایم کامپیوتری، ۱۳۸۳، چاپ اول، انتشارات آریان، ص ۳۸.
- دوازدهمین کنفرانس مدیران موسسات تحقیقاتی جرم‌شناسی: جنبه‌های جرم شناختی جرایم اقتصادی در استراسبورگ، ۱۹۷۶.
- زندى، محمدرضا، تحقیقات مقدماتی در جرایم سایبری، انتشارات جنگل، ۱۳۸۹.

فهیمی، مهدی، جرایم رایانه‌ای و روش‌های مقابله و پیشگیری از آن، ۱۳۸۰، فصلنامه دیدگاه‌های حقوقی، دانشکده علوم قضایی و خدمات اداری، ش ۲۳ و ۲۴، ص ۱۳۶.

کنفرانس سازمان ملل در تجارت و توسعه، گزارش اقتصاد اطلاعاتی، ۲۰۰۵، فصل ۶، ص ۲۳۳.

انگلیسی:

Council of Europe, Ccommittee of Ministers, Recommendation No. R (89) 9 (1989)

Council of Europe, Ccommittee of Ministers, Recommendation No. R (85) 10 (1985).

Council of Europe, Ccommittee of Ministers, Recommendation No. R (87) 15 (1987).

Council of Europe, Ccommittee of Ministers, Recommendation No. R (95) 4 (1995).

Council of Europe, Convention on Cybercrime, Budapest 23.11.2001

Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (2007)

Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (2007), Art 20 and 23.

<http://www.interpol.com/Public/TechnologyCrime/Conferences/6thIntConf/Resolution.Asp> (visited on 11.5.1394).

[http://ec.europa.eu/information\\_society/activities/internationalrel/docs/wsis/tunis\\_agenda.pdf](http://ec.europa.eu/information_society/activities/internationalrel/docs/wsis/tunis_agenda.pdf) (visited on 11.5.1394).

Marco, Gercke (2009) Understanding Cybercrime: A Guide For Developing Countries, ITU, p: 95.

Marco Gercke (2012), Understanding Cybercrime: Phenomena, Challenges and Legal Responses, ITU.

Marco Gercke (2014), Understanding Cybercrime: Phenomena, Challenges and Legal Responses, ITU, p.133.

Resolution 149 (Antalya, 2006) – Study of definitions and terminology relating to building confidence and security in the use of information and communication technologies.