Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

فصلنامه علمی فقه و حقوق نوین

Print ISSN: 2717- 1469
Online ISSN: 2717 – 1477

ISC.SID.NOORMAGZ.MAGIRAN
GOOGLESCHOLAR.ENSANI
www.jaml .ir

سال پنجم، شماره هفدهم،
صفحات ۱۱-۱

پیشگیری و مبارزه با جرایم سایبری در پرتو اجماع بین المللی با تاکید بر کنوانسیون بوداپست

دکتر میثم موسی پور استادیار گروه حقوق خصوصی، دانشگاه پیام نور، تهران، ایران .

سجاد شاهکرمی دانشجوی حقوق رشته حقوق جزا و جرم شناسی، دانشگاه علوم و تحقیقات تهران، واحد بروجرد

چکیده

یکی از پدیده‌های مهم قرن بیست یکم ظهور فضای سایبری است که سوء استفاده‌های فراوان از آن موجب پیشبینی تدابیر کیفری در این زمینه شده است. اما با توجه به مشکلات بسیاری که فراروی تدابیر کیفری وجود دارد، سیاست پیشگیری از وقوع این جرائم مناسب‌ترین تدبیر سیاست جنایی است. . دولت‌ها برای مبارزه با جرایم سایبری در جهت تدوین معاهدات بین‌المللی گام برداشته‌اند. یکی از این معاهدات بین‌المللی معاهده جرایم سایبری شورای اروپا (کنوانسیون بوداپست) در سال ۲۰۰۱ می‌باشد که به عنوان نخستین معاهده در زمینه جرایم سایبری نگاشته شده است. ماهیت فضای سایبر به گونه‌ای است که تجلی هرچه بیشتر آزادی بیان و جریان آزاد اطلاعات را موجب شده و همچنین با امکاناتی که جهت برقراری انواع ارتباطات ایمن فراهم آورده، به نوعی در جهت حفظ حریم خصوصی افراد گام برداشته است. در تحقیق پیش رو به بررسی پیشگیری و مبارزه با جرایم سایبری در پرتو اجماع بین المللی با تاکید بر کنوانسیون بوداپست می‌پردازیم.

واژگان کلیدی: فضای سایبر، جرایم سایبری، مبارزه، کنوانسیون بوداپست.

طبقه‌بندی JEL: فقه – حقوق – جزا و جرم شناسی – حقوق بین الملل – حقوق خصوصی

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

Scientific Journal of Modern Jurisprudence and Law

Print ISSN: 2717- 1469
Online ISSN: 2717 - 1477

Profile in ISC,SID, Noormags, Magiran, Ensani, GoogleScholar
www.jaml .ir

fifth year, Issue 17

Pages 1-11

Preventing and combating cybercrime in light of international consensus, with emphasis on the Budapest Convention

Dr. Meysam Mousapour Assistant Professor, Department of Private Law, Payam Noor University, Tehran, Iran.

Sajjad Shahkarami Law Student, Criminal Law and Criminology, Tehran University of Science and Research, Boroujerd Branch

Abstract

Intoxicants are those materials that using them makes one to lose his/her will power and reason. Therefore there are juridical impacts in using them that need to be studied. Moreover intoxicants and narcotics due to their common harmful effects and causing trouble for reason and will power, might juridicaly be compared and one can claim that the term "intoxicant" includes narcotics as well. Since using intoxicants can be a start for committing other crimes, one can also study its role on punitive responsibility.

Even though there were some gaps in the previous Islamic penalty regulation which was passed in 1370 in this regard that caused some complexities for the courts, however regulation passed in 1392 solved those shortcomings through a proper comparison between intoxicants and narcotics, along with issuing regulations and mentioning specific common cases in the punitive responsibility. At the end; sometimes being drunk -due to using intoxicants- while committing a crime can intensify punitive responsibility and sometimes if the criminal is to be regarded without will power- due to using intoxicants- while committing a crime, then this can be regarded as a relative causes for removing punitive responsibility.

Keywords: Intoxicants , narcotics, Alqiyas-o-lolaviyyah, punitive responsibility, will power .

JEL Classification: Jurisprudence - Law - Criminal and Criminology - International Law - Private Law

مقدمه

فضای سایبر همانند دیگر عناصر زندگی اجتماعی، از گزند یک پدیدهٔ بسیار انعطاف‌پذیر و لاینفک از اجتماع به نام جرم در امان نمانده است. به طور کلی، آنچه امروز تحت عنوان جرم سایبر قرار می‌گیرد، دو طیف از جرائم است: گروه اول جرائمی هستند که نظایر آنها در دنیای فیزیکی نیز وجود دارد و فضای سایبر بدون تغییر ارکان مجرمانه‌شان، با امکاناتی که در اختیار مجرمان قرار می‌دهد، ارتکابشان را تسهیل می‌کند. جرائم تحت شمول این حوزه بسیار گسترده‌اند و از جرائم علیه امنیت ملی و حتی بین‌المللی نظیر اقدامات تروریستی گرفته تا جرائم علیه اموال و اشخاص را در برمی‌گیرند. نمونه‌ای از این طیف، تشویش اذهان عمومی از طریق سایبر است. اما طیف دیگر جرائم سایبر، به سوء استفاده‌های منحصر از این فضا مربوط می‌شود که امکان ارتکاب آنها در فضای فیزیکی میسر نیست. جرائمی نظیر دسترس غیرمجاز به داده‌ها یا سیستم‌ها یا پخش برنامه‌های مخرب نظیر ویروس‌ها، جز در فضای سایبر قابلیت ارتکاب ندارند و به همین دلیل به آنها جرائم سایبری محض نیز گفته می‌شود.جرایم سایبری عملاً بر روی همه دولت‌ها اثرگذار است روابط بین‌المللی نمی‌تواند نسبت به جرایم فضای سایبری بی‌تفاوت باشد. توسعه و تکامل فضای سایبری سبب ایجاد اشکال مختلف از جرایم سایبری شده است. در دهه‌های اخیر کشورها برای مبارزه با جرایم سایبری در جهت تدوین معاهدات بین المللی گام برداشته‌اند. یکی از این معاهدات بین المللی، معاهده جرایم سایبری شورای اروپا کنوانسیون بوداپست در سال ۲۰۰۱ می‌باشد که به عنوان نخستین معاهده در زمینه جرایم سایبری نگاشته شده است. این معاهده شامل اصول سیاست نمادین از قبیل اطمینان بخشیدن به مردم در جهت خنثی کردن سلاح‌های جاسوسی سایبری، آموزش عمومی درباره جرایم سایبری تلاشی به عنوان یک طرح برای دولت و به عنوان یک بازدارنده برای هرکسی که در صدد انجام فعالیت‌هایی از جرایم سایبری باشد، است.

۱-۱- تعریف و ویژگی‌های فضای سایبر

کلمه سایبر از لحاظ ریشه‌ای به معنی سکاندار است و از نظر مفهومی دلالت بر خودکار شدن کنترل مصنوعی و رایانه‌ای شدن دارد. برخی فضای سایبر را فضای خیالی و برخی دیگر فضای سایبر دور از واقعیت را می پندارند اما بعضی دیگر بر این باور هستند که فضای سایبر واقعی و حاضر است و آن را با ذخیره و انتقال الکترونیکی اطلاعات برابر گرفته‌اند نقطه بعضی نیز آن را با ارتباطات در شبکه‌های رایانه‌ای یکسان پنداشته‌اند.[۱]

همچنین ، مهمترین عنصر در نگرشی که محیط مجازی را یک جهان به موازات جهان واقعی می‌داند گستره بی‌منتهای فضای مجازی باشد ، گستره‌ای که دائماً در حال قبض و بسط است و شاید کم از گستره جهان واقعی نداشته باشد. در کنار

[۱] –عاملی، سعیدرضا(۱۳۹۶)، فلسفه فضای مجازی، تهران: انتشارات امیرکبیر،ص۹۲

این موضوع برخی ویژگی‌های فضای مجازی که از آن به عنوان فرا متغیر[۲] یاد می‌شود شامل سرعت بالا ، فرامکانی بودن ، انتشار یافتگی و تکثر پذیری ، تعاملی بودن و تشدید واقعیت مویدی بر جهان دگر بودن فضای مجازی است.[۳]

۲-۱-تعریف جرایم سایبری

جرایم سایبری شامل جرایمی است که توسط اشخاص در محیط سایبر ارتکاب می‌یابند. جرایمی همچون کلاهبرداری رایانه‌ای ، جعل رایانه‌ای ، جاسوسی رایانه‌ای ، تخریب و اخلالگری(سابوتاژ) رایانه‌ای ، دستتیابی و شنود غیر مجاز رایانه‌ای از جمله جرایم سایبری هستند. چنین به نظر می‌رسد ویژگی خاص فضای سایبر سبب شده تا همان گونه که افراد مرتکب جرایم سایبری می‌شوند دولت‌ها نیز بتوانند مرتکب جرایم سایبری شوند. در حقیقت در این فضا بعضی دولت‌ها علاوه بر جنگ ، به جرم و تروریسم دست می‌زنند در صورتی که افراد علاوه بر جرم و تروریسم به جنگ نیز دست می‌زنند. سازمان همکاری و توسعه اقتصادی ، جرایم سایبری را سوء استفاده از رایانه شامل هر نوع رفتار غیرقانونی ، غیر اخلاقی یا غیر مجاز که مربوط به پردازش اتوماتیک و انتقال داده‌ها می‌باشد تعریف می‌نماید.[۴]

۳-۱-تاریخچه جرایم سایبری

جرایم سایبری از زمان پیدایش تاکنون با سه نسل یا تیپ روبرو گشته است. دهه‌های ۶۰ و ۷۰ و اوایل ۸۰ زمان حاکمیت نسل اول تحت عنوان جرایم رایانه‌ای است. در این زمان در مورد جرایم ، محوریت بحث با رایانه بود به همین جهت تعداد توصیف‌های مجرمانه بسیار کم بود. به تدریج در دهه ۸۰ تا اوایل دهه ۹۰ نسل دوم ایجاد گردید که بحث محتوا مورد استفاده قرار گرفت یعنی به موضوع جرایم داده و اطلاعات توجه شد. به همین جهت نسل دوم تحت عنوان جرایم علیه داده‌ها مطرح گردید. پس از ۴ یا ۵ سال ، حاکمیت نسل سوم که از آن به جرایم سایبری یاد می‌شود به وجود آمد که ویژگی این نسل تجمیع رایانه با مودم و مخابرات با حالات شبیه‌سازی و مجازی‌سازی است. در این نسل تاکید بر رایانه نیست بلکه رایانه خود وسیله ارتکاب جرم است.جرایم نسل سوم در بستر شاهراه‌های الکترونیکی ارتباطی و اطلاعاتی به وقوع می‌پیوندند. اگر در ۴ دهه حاکمیت جرایم رایانه ، شاهد جرایم انگشت شمار بودیم اما در فضای سایبر ۵ دسته اصلی جرم وجود دارد که هر کدام بالغ بر چندین عنوان مطرح هستند و شاید تعداد مصادیق عمد و غیر عمد آن بالغ بر ۲۰۰

---

[۲] – فرا متغیرها ، عواملی هستند که همه چیز را تحت تاثیر قرار می‌دهند و در یک رابطه متقابل ، تاثیر و تاثر پذیری پیچیده‌ای بر یکدیگر نیز دارند.

[۳] – انصاری ، باقر؛ انصاری ، اسماعیل(۱۳۹۱) ، حقوق اطلاعات از منظر تحلیل اقتصادی ، مجله مطالعات حقوق تطبیقی ، دوره ۳ ، شماره ۲ ،ص ۸

۴ –خداقلی ، زهرا(۱۳۸۴) ، جرایم کامپیوتری ، چاپ اول ، انتشارات آریان ،ص ۲۹

عنوان مجرمانه شود. نخستین جرم سایبری در ایران به سال ۱۳۸۱ و ناظر به عمل دانشجویان برای اسکن اسکناس و پرینت رنگی از آن عطف شده اما گزارش‌های غیر رسمی حاکی از این است که در دهه ۶۰ تغییر نمرات درسی و تغییر بعضی از اسامی پذیرفته شده در کنکور ۶۴ اتفاق افتاد.[۵]

۴-۱-تعریف پیشگیری

طبق بند ۵ اصل ۱۵۶ قانون اساسی یکی از وظایف قوه قضائیه «اقدام مناسب برای پیشگیری از وقوع جرم» است. با توجه به تاریخ و شیوه‌های مبارزه بشر با پدیده جرم، جرم‌شناسان پیشگیری از جرم را به دو گونه پیشگیری کیفری و پیشگیری غیرکیفری تقسیم کرده‌اند، اصطلاح پیشگیری از جرم در معنای وسیع خود شامل اقدامات کیفری و غیرکیفری برای خنثی کردن عوامل ارتکاب جرم و کاهش بزهکاری می‌شود ولی در مفهوم مضیق پیشگیری فقط تدابیر غیرکیفری را شامل می‌شود.[۶]

۲- کنوانسیون بین المللی جرایم سایبری بوداپست

معاهده بوداپست در شناسائی بین‌المللی تسلیم میکروارگانیسم‌ها برای استفاده در تشریفات ثبت اختراع که به معاهده بوداپست مشهور است یک معاهده بین‌المللی است که در بوداپست، مجارستان، در تاریخ ۲۸ آوریل ۲۸ ژانویه ۲۰۲۴ میلادی امضا شد. این قانون در تاریخ ۹ اوت ۱۹۸۰ اجرایی شد و سپس در ۲۶ سپتامبر ۱۹۸۰ اصلاح شد. این پیمان توسط سازمان جهانی مالکیت فکری اداره می‌شود. از ژوئیه سال ۲۰۱۹، ۸۲ کشور عضو معاهده بوداپست هستند. الحاق این پیمان برای دولت‌های عضو کنوانسیون پاریس برای حمایت از مالکیت صنعتی سازمان مالکیت صنعتی منطقه‌ای آفریقا (ARIPO)، سازمان ثبت اختراعات اوراسیا (EAPO) و سازمان ثبت اختراعات اروپا (EPO) طبق ماده ۹ پیمان‌نامه مجاز می‌باشد. بر اساس مفاد این معاهده، یک کشور متعاهد که تسلیم میکروارگانیسم‌ها را برای استفاده از تشریفات ثبت اختراعات اجازه داده یا آن را اجباری می‌کند، موظف است که یک میکروارگانیسم را نزد مقام یا مرکز سپرده‌گذاری بین‌المللی بسپارد و بدون در نظر گرفتن این که چه مقام یا مرکزی در داخل یا خارج از آن قلمرو است، نسبت به شناسایی و رسمیت بخشیدن به آن اقدام کند.[۷]

۱-۲- اعمال صلاحیت کیفری تعارض قوانین در مورد جرایم ارتکابی در فضای سایبر

یکی از مسائل جدیدی که به موازات تحول و پیشرفت تکنولوژی در زمینه فناوری اطلاعات و ارتباطاتبه وجود آمده

---

۵ – شیرزاد ، کامران(۱۳۸۸) ، جرایم رایانه‌ای ، چاپ اول ، تهران: نشر بهینه فراگیر ،ص ۲۳

۶ – معظمی، شهلا (۱۳۸۶)، پیشگیری جرم‌شناختی، فصلنامه پژوهشی تحلیلی و آموزشی مجد (حقوقی)، سال اول، شماره اول، ص۹۳.

۷ – پورجاهد، محمد (۱۳۹۵)، بررسی حقوقی جرایم سایبری ایران در پرتو کنوانسیون جرایم سایبری، پایان نامه برای دریافت درجه کارشناسی ارشد، رشته حقوق جزا و جرم شناسی، دانشگاه آزاد اسلامی واحد تفت، ص ۵۶

است مسأله چگونگی تعیین مرجع قضایی صالح جهت فضای سایبر، ایجاد دنیای مجازی جدید به نام رسیدگی به جرائم ارتکابی در فضای مذکور است. براساس قواعد سنتی مهمترین ضابطه تعیین صلاحیت مراجع قضایی کیفری، مکان وقوع جرم می‌باشد و در فضای جدید سایبر که یک فضای مجازی و فارغ از مکان می‌باشد، چنین ضابطه‌ای قابل اجرا نبوده و یا مستلزم تعدیل ویژه می‌باشد.در همین جهت، برخی سعی کرده‌اند همان قواعد سنتی ناظر بر صلاحیت کیفری مراجع قضایی را با نگرشی جدید در این فضا اجرا کنند و برخی دیگر با طرح تدوری‌های نو در خصوص صلاحیت، از قبیل فضای سایبر بعنوان یک فضای آزاد بین المللی و یا پیش بینی دادگاهی ویژه به نام دادگاه دیجیتالی یا سایبری و یا صلاحیت دادگاه ذی ارتباط منطقی با جرم را مطرح کرده‌اند.[۸]

۲-۲- پیشگیری از جرایم سایبری با محوریت جرم‌یابی

توسعه انواع بزهکاری در اشکال مختلف، پیچیدگی‌های مسیر کشف جرم ، لزوم تسریع در دستگیری مجرمین و تحقق فرایند دادرسی کیفری و تاثیر آن در کاهش میزان وقوع جرم در حیطه جرم‌یابی سبب طرح راهکارهای علمی گوناگونی جهت کشف جرم شده است.با عنایت بـه این که به تناسب پیشرفت زمان، جرائم موضوعه شکل تازه‌ای به خود گرفته‌اند؛ به همین جهت، جایگاه پلیس علمی در قوانین امروزه ، به ویژه قانون آیین دادرسی کیفری اهمیت بسیار زیادی دارد. از مهمترین وظایف نیروی انتظامی کشف جرم و جمع آوری دلایل و ارائه آن به مقامات قضایی می‌باشد در این میان پلیس علمی که نتایج بررسی‌های خود را در زمینه نحوه وقوع عمل مجرمانه و دیگر مسائل مرتبط در اختیار دستگاه قضایی قرار می‌دهد نقش مهمی در روند دادرسی و در نهایت صدور حکم ایفا خواهد کرد ، با این همه باید دقت نمود ابزارها و فناوری‌های نوین با کارکرد دو سویه ، از جهتی به دلیل کارآمد و مفید بودن آنها در کشف و پیشگیری از جرایم اهمیت زائد وسیع در ایجاد نظم و امنیت عمومی ، می‌کنند ، اما از سوی دیگر قابلیت بالایی در نقض حریم خصوصی افراد دارند. به دیگر سخن ، فناوری‌های اخیر علاوه بر اینکه قلمروهای نوین از حریم خصوصی را ایجاد کرده‌اند ، ابزارهایی را نیز در اختیار اشخاص اعم از حقیقی و حقوقی قرار داده‌اند که به واسطه آنها نقض حریم خصوصی افراد به سهولت امکان‌پذیر است. با این توصیف بهترین راهبرد در این مورد ایجاد تعادل میان دو مقوله صیانت از حریم خصوصی و دفاع از نظم و امنیت عمومی است.[۹]

۲-۳- سیاست جنایی ایران در قبال جرم تولید و توزیع و انتشار بدافزارها در فضای سایبر در پرتو کنوانسیون بوداپست

سیاست جنایی تقنینی مطلوب در قبال جرم انگاری تولید، توزیع و انتشار بدافزارهای رایانه‌ای، باید تدابیر کیفری و غیرکیفری را توأمان مورد نظر قرار دهد و در عین حال، بزه-

[۸] –امینی نیا، عاطفه؛ علیزاده، حمیدرضا(۱۳۹۷)، اعمال صلاحیت کیفری(تعارض قوانین) در مورد جرائم ارتکابی در فضای سایبر، نشریه پژوهش ملل، دوره سوم، شماره۳۰،ص ۲۱

[۹] – مجتهدی ، هاشم(۱۴۰۰) ، پیشگیری از وقوع جرم با محوریت جرم‌یابی نوین ، نشریه دانش انتظامی و چهارمحال و بختیاری ، شماره ۳۵ ،ص ۱۳۲

دیدگان این جرائم نیز تحت شمول سیاست‌ها و راهبردهای حمایتی افتراقی قرار گیرند. به این ترتیب، در تحلیل سیاست جنایی جمهوری اسلامی ایران در زمینه جرم‌انگاری تولید، توزیع و انتشار بدافزارها می‌توان گفت نظام حقوقی ایران، به منظور پیشگیری و مقابله با مرتکبان این جرایم در بُعد تقنینی، عمدتاً به کیفر متوسل شده و مقررات خاصی در زمینه پیشگیری غیرکیفری پیشبینی نکرده است؛ لیکن در مقررات فراتقنینی و فروتقنینی میتوان نشانه‌هایی از هر دو نوع پیشگیری کیفری و غیرکیفری یافت. لذا از این جهت سیاست جنایی کلان ایران نسبت به کنوانسیون بوداپست مترقی‌تر است؛ در عین حال اما، سیاست جنایی ایران در قبال بزه-دیدگان جرایم رایانه‌ای با توجه به خاص بودن این جرایم و گستره دامنه بزه‌دیدگی آنها، افتراقی نبوده و به نظر در مقایسه با کنوانسیون مذکور، ناکارآمد و ناقص می‌باشد.[۱۰]

۴-۲- مقایسه و تحلیل تولید و توزیع و انتشار، استفاده و مورد معامله قرار دادن برنامه‌های مخرب رایانه‌ای در قانون ایران با کنوانسیون بوداپست

ایران تا قبل از تصویب قانون جرائم رایانه‌ای کار تولید یا انتشار یا توزیع و استفاده و مورد معامله قراردادن برنامه‌های مخرب رایانه‌ای را جرم نمی‌دانست فقط قانونگذار تعداد کمی از جرائم رایانه‌ای که با جرائم سنتی مشابهت داشت مثل کلاهبرداری یا جاسوسی رایانه‌ای و ... را در بعضی قوانین مثل قانون تجارت الکترونیک، قانون مطبوعات و قانون مجازات جرائم نیروهای مسلح جرم‌انگاری کرده بود با تصویب قانون جرائم رایانه‌ای قانونگذار ایران به تأسی از کنوانسیون بوداپست جرم مذکور را درماده ۲۵ جرم‌انگاری کرده است. تدوین کنندگان ماده ۲۵ قانون جرایم رایانه‌ای ماده ۶ کنوانسیون بوداپست را الگوی خود قرار داده‌اند. ماده ۶ کنوانسیون بوداپست چنین اشعار داشته: «هر یک از اعضاء باید به گونه‌ای اقدام به وضع قوانین و مقررات کند که در صورت لزوم بر اساس حقوق داخلی خود هرگونه اقدام‌های عمدی و بدون مجوز زیر را جرم‌انگاری کند». هرچند ایران عضو کنوانسیون نبوده لیکن به توصیه‌های کنوانسیون به خوبی عمل نموده و تقریباً تمامی مواردی که کنوانسیون پیشنهاد جرم‌انگاری در مورد آن نموده را در قانون جرایم رایانه‌ای جرم‌انگاری کرده است. با این تفاوت که کنوانسیون عبارت «تامین و تهیه برای استفاده» و «فروش» را به کار برده در حالی که قانونگذار ایران ظاهراً به جای آن، اصطلاح «معامله» را به کار برده است پس «معامله» به معنی خرید و فروش است که ایران با این واژه، خرید وسایل الکترونیکی که به منظور ارتکاب جرایم رایانه‌ای به کار می‌روند را جرم‌انگاری کرده که شاید بتوان گفت تأمین و تهیه برای استفاده هم در آن مستتر باشد چون کسی که وسیله‌ای را می‌خرد در واقع آن را تأمین یا تهیه کرده برای استفاده. بنابراین از این جهت نمی‌توان به قانونگذار ایران خرده گرفت. کنوانسیون، پیشنهاد جرم‌انگاری تولید، توزیع، فروش و تأمین و به نحو دیگری در دسترس قرار دادن «عمدی و بدون مجوز» وسایلی که اساساً به منظور ارتکاب هر یک از

---

[۱۰] – نجفی، حسین (۱۳۹۸)، سیاست جنایی تقنینی ایران در قبال جرم تولید، توزیع و انتشار بدافزارها در فضای سایبر (در پرتو کنوانسیون بوداپست)، پایان نامه جهت دریافت درجه کارشناسی ارشد، رشته حقوق جزا و جرم شناسی، دانشگاه کاشان، ص ۱

جرایم مندرج در ماده ۲ تا ۵ طراحی یا سازگار شده است را داده لیکن قانونگذار ایران قیدی از «عمدی و بدون مجوز» به میان نیاورده است. پس با این نحوه قانونگذاری، اگر وسیله‌ای تولید، یا از روی اشتباه یا سهو یا ناآگاهی توزیع، یا معامله ... یا منتشر شود که به قصد ارتکاب جرم نباشد مثلًا؛ برای آزمایش، ساخته شده باشد و دارای مجوز نیست و یا اصلا بامجوز باشد؛ مانند وسایلی که برای آموزش یا جهت مقابله با جرم، تولید یا توزیع یا معامله یا منتشر می‌شوند؛ جرم تلقی کردن عمل، چگونه توجیه می‌شود؟ این در حالی است که کنوانسیون بوداپست به کشورهای عضو توصیه کرده که از جرم‌انگاری چنین موقعیت‌هایی خودداری کنند. ممکن است گفته شود عبارت «صرفاً به منظور ارتکاب جرایم رایانه‌ای به کار رود» دلالت بر عمد و بدون مجوز دارد در حالیکه این عبارت، ربطی به قصد مرتکب ندارد بلکه اختصاص به داده‌ها یا نرم‌افزارها یا ابزارها و وسایل الکترونیکی دارد. در واقع می‌خواهد بین ابزارهایی که صرفاً به منظور ارتکاب جرایم رایانه‌ای به کار می‌روند با ابزارهایی که کاربرد دوگانه دارند، تفاوت قائل شود؛ یعنی آنهایی که کاربرد دوگانه دارند را از شمول جرم، خارج نماید نه آنهایی که قصد ارتکاب جرم ندارند[۱۱].

۵-۲- خلأهای قانونی و اجرایی پیشگیری از ارتکاب جرایم سایبری

قوانین و مقررات حاکم بر بستر عبور و مرور در فضای مبادلات اینترنتی از مقررات موجود برای مبادلات تجاری در دنیای واقعی بسیار متفاوت‌تر است. نامعین بودن حیطه‌های جغرافیایی یکی از خلاهای موجود در مقابله با جرایم سایبری است. موقعیت شبکه آنچنان به موقعیت جغرافیایی بی‌ربط است که اغلب تعیین مکان فیزیکی یک منبع یا کاربر اینترنتی ناممکن است. اطلاع از این موقعیت مکانی برای عملکرد شبکه و ایجاد کنندگان آن اهمیتی ندارد لذا در طراحی یک شبکه امکان تشخیص مکان جغرافیایی در نظر گرفته نشده است. در فضا و مکان واقعی، یک شرکت یا طرف تجاری معمولاً می‌تواند مکان واحد یا شخصی را که با او در تبادل است شناسایی کند چرا که این کار به شناسایی طرفین و اعتبار و مشروعیت مبادلات کمک می‌کند ولی انجام این کار در محیط مجازی بسیار دشوار است. از سوی دیگر مسائل مربوط به صلاحیت قضایی در قبال جرایم تقریباً همیشه با در نظر گرفتن محل ارتکاب آنها بیان می‌شود. این به آن دلیل است که صلاحیت قضایی جنایی همواره بر مبنای حضور واقعی و فیزیکی مجرم در درون حوزه استحفاظی و در مقابل میز محاکمه تعیین می‌شود. با توجه به ماهیت جرایم اینترنتی تعیین محل وقوع جرم و یا محل حصول نتیجه همیشه و به آسانی مقدور نیست

---

[۱۱] – نجفی، حسین (۱۳۹۸)، سیاست جنایی تقنینی ایران در قبال جرم تولید، توزیع و انتشار بدافزارها در فضای سایبر (در پرتو کنوانسیون بوداپست)، پایان نامه جهت دریافت درجه کارشناسی ارشد، رشته حقوق جزا و جرم شناسی، دانشگاه کاشان، ص ۱۲۷

و به فرض شناسایی محل ارتکاب جرم و یا محل حصول نتیجه جرم اینکه کدام دادگاه صالح خواهد بود دشوار است[۱۲].

۶-۲- اقدام سازمان ملل متحد در مبارزه با جرایم سایبری

جدا از فعالیت‌های پراکنده این سازمان برای نخستین بار پیشنهاد کنگره هشتم پیشگیری از جرایم و رفتار با مجرمان در ۱۹۹۰ از جرایم کامپیوتری سخن می‌گوید. در دوازدهمین نشست عمومی کنگره هشتم نماینده کانادا پیش نویس قطعنامه‌ای را از جانب ۲۱ کشور برپا کننده در مورد جرایم مرتبط با کامپیوتر ارائه داد که از جمله به مدرنیزه کردن قوانین کیفری برای جبران خسارتی که از طریق جرایم مرتبط با کامپیوتر به وجود می‌آید. تاکید داشت در این قطعنامه از جمله مشکلات تعقیب، تحقیق، کشف جرایم، آموزش قضات و نهادهای مسئول برای امر تعقیب و تحقیق آشنایی این نهادها با عصر انفورماتیک و سیاست حمایت از بزهدیدگان کامپیوتری مورد توجه قرار گرفته است. این سازمان در ۱۹۹۴ کتابچه پیشگیری و کنترل جرایم مرتبط با کامپیوتر را منتشر کرد. تعدادی از بخش‌های سازمان ملل موضوعات مربوط به جرایم سایبری را مورد بررسی قرار دادند. اداره مبارزه با مواد مخدر و جرایم سازمان ملل کمیسیون پیشگیری از جرایم و قضاوت جنایی بیانیه را پذیرفتند. در مورد پیشگیری موثر از جرم عدالت کیفری برای مبارزه با سوء استفاده جنسی از کودکان. شورای اقتصادی و اجتماعی سازمان ملل با بیانیه‌ای در مورد همکاری بین‌المللی در پیشگیری موافقت کرد و با مجازات کلاهبرداری سوءاستفاده و جعل هویت و جرایم مربوطه موافقت کرد. مجمع عمومی سازمان ملل مجموعه‌ای از قطعنامه‌ها را در خصوص پیشرفت‌های حاصل شده در خصوص اطلاعات و ارتباطات از راه دور و تاثیر آن بر امنیت ملی تصویب نموده و تاکید کرده است سوء استفاده‌های جنایتکارانه از فناوری‌های اطلاعاتی می‌تواند تاثیر شدیدی بر تمامی کشورها داشته باشد[۱۳].

نتیجه گیری

جرایم سایبری جرایمی هستند که عموماً علیه سیستم‌های رایانه‌ای و از طریق همین سیستم‌ها به وقوع می‌پیوندند. این قبیل فعالیت‌ها به تهدیدی برجسته برای زیرساخت‌های حیاتی کشورها، حقوق اساسی افراد و صلح و ثبات جهانی بدل شده است. بنابراین، رویکرد کلان شورای اروپا برای مبارزه با این عنصر مخرب نوظهور، بهره گیری از ۳ اصل اساسی را در بر می‌گیرد. استانداردهای مشترک کنوانسیون جرایم سایبری که (به خاطر امضا شدن در بوداپست، مجارستان، در نوامبر ۲۰۰۱ به کنوانسیون بوداپست معروف است) به عنوان مرتبط‌ترین معاهده حقوقی- کیفری بین المللی در مورد جرایم سایبری و شواهد الکترونیکی اساسی‌ترین ابزار در

[۱۲] – زلفی، علی؛ مالمیر، محمود (۱۳۹۹)، خلاءهای قانونی و اجرایی و راهکارهای پیشگیری از ارتکاب جرایم سایبری، نشریه کارآگاه، شماره ۵۲، ص ۹۲

[۱۳] – فتحی، صابر (۱۳۹۶)، نقش و عملکرد سازمان‌های بین المللی دولتی و غیردولتی در حوزه جرایم سایبری، پایان نامه برای دریافت درجه کارشناسی ارشد، رشته حقوق بین الملل، دانشگاه پیام نور مرکز تهران، ص ۷۲

اختیار شورای اروپا است. از اعضای این کنوانسیون می‌توان به ۶۵ کشور از سراسر جهان اشاره کرد.. کمیته کنوانسیون جرایم رایانه‌ای(TCY) ، متشکل از نمایندگان طرف‌های کنوانسیون بوداپست ابزار دیگری در اختیار سیاستمداران اروپایی جهت مبارزه با جرایم سایبری است. این نهاد مسئولیت ارزیابی اجرای صحیح کنوانسیون، تهیه دستورالعمل‌های اجرایی، اسناد قانونی اضافی و تسهیل همکاری بین طرف‌ها را بر عهده دارد. این روزها، با توجه به گسترش روزافزون جرایم سایبری و پیچیدگی فزاینده فرایند به دست آوردن شواهد الکترونیکی، تنها بخش بسیار کوچکی از جرایم سایبری گزارش شده به مراجع قضائی، به بررسی در دادگاه و صدور حکم ختم می‌شود. علاوه بر این، بسیاری از شواهد و دیگر اطلاعات، ممکن است در حوزه‌های قضائی خارجی، در حال تغییر یا ناشناخته ذخیره و موجود باشند. به روز رسانی اخیر در دستورالعمل‌های موجود، واکنشی آشکار به گسترش جرایم سایبری محسوب می‌شود و مبنایی برای چارچوب‌مند سازی نحوه افشای اطلاعات حساس و همکاری مستقیم با ارائه دهندگان خدمات آنلاین، به شمار می‌رود.

سپاسگزاری

از معاونت محترم پژوهشی به خاطر حمایت حمایت معنوی در اجرای پژوهش حاضر سپاسگزاری می‌شود.

از آقای دکتر عبدالله علیزاده به خاطر بازبینی متن مقاله و ارائه نظرهای ساختاری تشکر و قدردانی می‌شود.

از داوران محترم به خاطر ارائه نظرهای ساختاری و علمی سپاسگزاری می‌شود.

نگارندگان بر خود لازم می‌دانند از آقای دکتر محمد رسول آهنگران به خاطر مطالعه متن مقاله حاضر و ارائه نظرهای ارزشمند سپاسگزاری نمایند.

منابع

- -خداقلی ، زهرا(۱۳۸۴) ، جرایم کامپیوتری ، چاپ اول ، انتشارات آریان
- ۲-شیرزاد ، کامران(۱۳۸۸) ، جرایم رایانه‌ای ، چاپ اول ، تهران: نشر بهینه فراگیر
- ۳-عاملی، سعیدرضا(۱۳۹۶)، فلسفه فضای مجازی، تهران: انتشارات امیرکبیر
-
- **مقالات**
- ۱-افتخارجهرمی، گودرز؛ اسلامی، ابراهیم (۱۳۹۳)، **نحوه اعمال صلاحیت دادگاه‌ها در رسیدگی به جرایم فضای مجازی**، *نشریه حقوقی دادگستری*، شماره ۸۸، صص ۶۲-۳۷
- ۲-امینی نیا، عاطفه؛ علیزاده، حمیدرضا(۱۳۹۷)، **اعمال صلاحیت کیفری(تعارض قوانین) در مورد جرائم ارتکابی در فضای سایبر**، *نشریه پژوهش ملل*، دوره سوم، شماره۳۰،صص ۴۱-۲۱
- ۳-انصاری، باقر؛ انصاری، اسماعیل(۱۳۹۱) ، **حقوق اطلاعات از منظر تحلیل اقتصادی** ، *مجله مطالعات حقوق تطبیقی* ، دوره ۳ ، شماره ۲ ،صص۲۰-۷
- ۴-رضوی، محمد(۱۳۸۶) ، **جرایم سایبری و نقش پلیس در پیشگیری از این جرایم و کشف آنها**، *نشریه دانش انتظامی*، دوره ۹، شماره۱، صص۱۴۰-۱۲۰
- ۵-زلفی، علی؛ مالمیر، محمود (۱۳۹۹)، **خلاءهای قانونی و اجرایی و راهکارهای پیشگیری از ارتکاب جرایم سایبری**، *نشریه کارآگاه*، شماره ۵۲، صص ۹۸-۸۳
- ۶-مجتهدی، هاشم(۱۴۰۰)، **پیشگیری از وقوع جرم با محوریت جرم‌یابی نوین** ، *نشریه دانش انتظامی و چهارمحال و بختیاری* ، شماره ۳۵،صص ۱۳۴-۱۱۳
- ۷-معظمی، شهلا (۱۳۸۶)، **پیشگیری جرم‌شناختی**، *فصلنامه پژوهشی تحلیلی و آموزشی مجد (حقوقی)*، سال اول، شماره اول، صص ۶۵-۷۸
-
- **پایان نامه‌ها**
- ۱-پورجاهد، محمد (۱۳۹۵)، **بررسی حقوقی جرایم سایبری ایران در پرتو کنوانسیون جرایم سایبری**، پایان نامه برای

دریافت درجه کارشناسی ارشد، رشته حقوق جزا و جرم شناسی، دانشگاه آزاد اسلامی واحد تفت

- ۲-فتحی، صابر (۱۳۹۶)، **نقش و عملکرد سازمان‌های بین المللی دولتی و غیردولتی در حوزه جرایم سایبری**، پایان نامه برای دریافت درجه کارشناسی ارشد، رشته حقوق بین الملل، دانشگاه پیام نور مرکز تهران
- ۳-نجفی، حسین (۱۳۹۸)، **سیاست جنایی تقنینی ایران در قبال جرم تولید، توزیع و انتشار بدافزارها در فضای سایبر (در پرتو کنوانسیون بوداپست)**، پایان نامه جهت دریافت درجه کارشناسی ارشد، رشته حقوق جزا و جرم شناسی، دانشگاه کاشان.