فصلنامه مطالعات بین‌المللی
سال ۱۶، شماره ۲ (۶۲)، پاییز ۱۳۹۸
تاریخ دریافت: ۱۳۹۸/٤/۳۱
تاریخ پذیرش: ۱۳۹۸/٦/۳۱
صفحات: ٤۷-۳۱

نوع مقاله: علمی-پژوهشی

سیاست‌های نمادین معاهده جرایم سایبری شورای اروپا

الناز کتانچی*
دکتر بابک پورقهرمانی**

چکیده

توسعه و تکامل فضای سایبری سبب ایجاد اشکال مختلفی از جرایم سایبری شده است. از این رو در دهه‌های اخیر کشورها 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. این معاهده شامل اصول سیاست نمادین از جمله موارد زیر می‌باشد: 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 هر کسی که درصدد انجام فعالیت‌هایی از جرایم سایبری باشد. بررسی این سیاست‌های نمادین سوالاتی را درباره اثر بخشی معاهده جرایم سایبری شورای اروپا و دیگر سیاست‌هایی که از جرایم سایبری بین‌المللی جلوگیری می‌کنند و همچنین قابلیت اجرای قانون برای مبارزه با این مسئله و اینکه با گذشت چندین سال از ایجاد این معاهده، چرا هنوز معاهده از قدرت الزام‌آوری کافی برای اغلب کشورها برخوردار نیست و کشورها در تصویب آن مرددند، ایجاد می‌کند. بدین ترتیب این پژوهش به شیوه توصیفی- تحلیلی درصدد تبیین و شرح سیاست‌های نمادین معاهده و پاسخگویی به سوالات طرح شده است.

کلیدواژگان

سیاست نمادین، معاهده، جرایم سایبری، شورای اروپا.

* دانشجوی دکتری تخصصی حقوق بین الملل عمومی، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران/ ایمیل: e.katanchi20@gmail.com

** نویسنده مسئول، استادیار گروه حقوق جزا و جرم شناسی، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران / ایمیل: b.pourghahramani@yahoo.com

مقدمه

در سال‌های اخیر، اینترنت به یک پدیده وسیع جهانی مبدل گشته است. امروزه، تکنولوژی مردم را از سرتاسر جهان به گونه‌ایی به همدیگر متصل می‌کند که قبلاً امکان‌پذیر نبود (گرکی، ۱۳۸۹: ۱۳). ارتباطات داخلی بیشتر کامپیوترها، با عنوان «فضای سایبری»، به ساکنین کشورهای مختلفی اجازه می‌دهد تا به راحتی با هم ارتباط برقرار کنند. از آنجایی که فضای سایبری توسعه و تکامل پیدا کرده است، اشکال مختلفی از جرایم سایبری نیز ایجاد شده است. تکنولوژی جدید، فرصت‌هایی را برای جرایم تازه به وجود آورده است و تعداد زیاد جرایم سایبری که به مقامات گزارش می‌شدند، افزایش چشم‌گیری داشته‌اند (Nuth, 2008: 439). در واقع شبکه‌های مجازی و رسانه‌های دیجیتال شمشیرهای دو لبه‌ای هستند (MonshiPouri and Prompichai, 2018: 42)، برای رفاه و برای انجام جرائم. تا این لحظه، «اطلاعات دقیق درباره بروز جرایم سایبری علیه افراد وجود ندارد، به این خاطر که بیشتر جرایم ناخواسته گزارش شده‌اند و یا هم ثبت نشده‌اند. با این وجود، اطلاعاتی که گزارش شده‌اند، مربوط به افزایش دراماتیک و قابل توجه تعداد ورودی‌های مزاحمت‌آمیز کامپیوتری در یک و نیم دهه گذشته بوده است»(Schell & Martin, 2004: 50). با وجود افزایش جرایم سایبری، «اجرای قانون نتوانسته است به طور موثر پاسخ‌گوی تهدیدات عدیده‌ایی که از کامپیوتر برای ارتکاب به جرایم استفاده می‌کنند، باشد»(Kellermann, 2010: 7). به این نکته اشاره شده است که فقدان قوانین موثر علیه جرایم سایبری نیز وجود دارد. فراخوان‌های زیادی برای اجرای قوانین جهت جلوگیری بیشتر از خسارت‌های وارده از جرایم سایبری وجود دارد، با این حال ادارات پلیس از اقدامات علیه جرایم صرفاً به دلیل مسائل قضایی یا هویت این مسائل در بررسی جرایم سایبری متوقف شده‌اند. از دیگر مسایل در اجرای قوانین، «وجود استانداردهای فرهنگی مختلف در بین کشورها می‌باشد. گاهی اوقات هم می‌تواند اختلافات اخلاقی، سیاسی و قوانین اساسی در بین کشورها وجود داشته باشد. به طور مثال، عملی که در یک کشوری غیر قانونی است، در کشور دیگری، این عمل مجاز است»(جلالی فراهانی، ۱۳۸۷: ۴۱). بسیاری از تصاویر نوشته جات جنسیتی (شهوت‌انگیز) در ایالات متحده قانونی هستند و تحت اصلاحیه قانون اساسی آمریکا حمایت می‌شوند (Swire, 2005: 1981). در حالی که در کشورهای دیگر، چنین مواردی مجاز و قانونی نیستند. از دیگر تفاوت‌های فرهنگی در این مورد، مربوط به گویش و زبان مردم می‌باشد. گویش و زبانی که در برخی کشورها مجاز می‌باشد و در کشورهای دیگر همان گویش و زبان مجاز نیست. «تفاوت‌های فرهنگی، زمانی که در صدد کنترل محتوای فضای سایبری می‌شود، مشکلاتی را می‌توانند ایجاد کنند. نتیجتاً، محتویاتی که به طور قانونی توسط یک فرد آنلاین از یک مکان پست می‌شود، ممکن است همان محتوا که در مکان دیگری مشاهده می‌شود، نقض قوانین شمرده شود. در چنین شرایطی، قوانین موجود در آن محل با قوانینی که در مکان دیگر حاکم می‌باشد، در تضاد خواهند بود. از این رو، سوالاتی پیش

خواهد آمد که آیا افراد در محل دریافت محتوا، می‌توانند موضوع تنبیه قرار بگیرند یا نه؟ و یا در اصل، اگر فردی که همان محتوا را منتشر می‌کند، بایستی فعالیت‌های خود را اصلاح کند تا آنها با قوانین محدود کننده‌تر آن کشور مطابقت کند؟» (Berman, 2002: 321).

این مورد، اغلب در مسایل قانونی پیچیده مرتبط با جرایم سایبری نتیجه می‌دهد. قوانین سنتی، مبتنی بر ژئوگرافی و مرزبندی فیزیکی می‌باشد، اما جرایم سایبری به راحتی از مرزهای ملی عبور می‌کنند. «قوانین حاکم بر جرایم سایبری اغلب براساس قلمرو کشورها می‌باشند. به طوریکه آنها صرفاً در داخل هر کشوری که قوانین مبارزه با جرایم سایبری در آنجا تصویب شده‌اند، اعمال می‌شوند»(Brenner, S., & Schwerha, 2004: 112).

بیشتر کشورها، قوانین کافی در برخورد با جرایم سایبری ندارند. این مسئله بعد از اینکه یک فرد از فیلیپین ویروس مهلک (من عاشق تو هستم) [1]را منتشر کرد، مشهود است. «در آن برهه زمانی، هیچ قانونی در فیلیپین وجود نداشت که به طور خاص به جرایم کامپیوتری اشاره کند و از این رو متخلفین آزاد بودند. حدود یک ماه بعد از آن اتفاق، قانون تجارت الکترونیکی توسط کنگره فیلیپین تصویب شد. کشورهایی که قانون مقابله با جرایم سایبری را تصویب کرده‌اند، پی به منسوخ بودن، تناقض و تضاد آنها با قوانین دیگر کشورها برده‌اند»(Gercke, 2009: 417). به عنوان مثال، قانون ۱۹۹۰ سوء استفاده از کامپیوتر انگلستان مورد نقد و بررسی قرار گرفتند، به این دلیل که تصورات کلی آن منسوخ شدند و فرم‌های جدید جرایم کامپیوتری را پوشش نمی‌دادند (Coleman, 2003: 134). می‌توان به این نکته هم اشاره کرد که از هر پنج کشور، یک کشور قوانین خود را تغییر داده‌اند که فرم‌های جدید این جرایم را پوشش دهند. با این وجود، اغلب کشورها قوانین مختلفی را تصویب کرده‌اند. بدین معنی که «وقتی جرایم سایبری صورت می‌گیرند، این احتمال وجود دارد که بیشتر قوانین اعمال شوند و یا اینکه هیچ قانونی اعمال نشود و بدتر از این موارد این است که برای قانون گذاردن، مقابله کردن با افرادی که همواره راه‌های جدیدی برای ارتکاب به جرایم سایبری پیدا می‌کنند، سخت است»(Sinrod, & Reilly, 2000: 3).

مشکل دیگر اجرای قانون این است که بررسی، تعقیب و مجازات کردن مرتکبین جرایم سایبری بسیار دشوار است. «اغلب همکاری ضعیفی از میزبان‌های وب در هنگام بررسی جرایم

---

[1]. این ویروس یک اسکریپت نوشته شده در محیط ویژوال بیسیک است که دستمایه خلاقانه آن، وعده دوستی است. و با نام‌های دیگر Love Letter و Bug Love نیز شناخته می‌شود. این ویروس در ابتدا در تاریخ سوم ماه می سال ۲۰۰۰ در کشور هنگ کنگ کشف شد و از طریق ایمیل با موضوع انتشار یافت که ضمیمه آن یک فایل با نام-Love-Letter-For-You-.TXT.vbs بود. به محض این‌که این فایل توسط قربانی باز می‌شد، خود را به تمام آدرس‌های موجود در فهرست تماس برنامه آوت لوک ارسال می‌کرد. همچنین فایل‌های موسیقی، تصویری و ... را با یک نسخه از خود رونویسی می‌کرد. بدتر از آن اینکه، این ویروس اقدام به ربودن شناسه‌ها و کلمات عبور می‌کرد و آن‌ها را برای نویسنده خود ارسال می‌نمود.

وجود دارد و گاهی جمع‌آوری مدرک جرم الکترونیکی دشوار است تا مجرم به پیشگاه عدالت آورده شود. همچنین حفظ چنین شواهدی که هویت جرایم و احتمالات آن را ثابت می‌کند، دشوار است. قابلیت‌های کشورها در بررسی و کیفر خواست جرایم سایبری متفاوت است و در طرز تفکر تکنولوژیکی هم متفاوت هستند»(جلالی فراهانی، ۱۳۹۴: ۱۹-۱۷). در عین حال، تشخیص هدف متخلفین هم یک چالش می‌باشد. هکرها اکثر اوقات از روی سرگرمی و نه با هدف جنایی، به طور غیر قانونی وارد شبکه‌های اینترنتی می‌شوند.[1]

به خاطر وجود چنین مشکلاتی روشن است که قوانین برای جلوگیری از جرایم سایبری کافی نیستند. هر کشوری با توجه به جرایم سایبری قوانین خاص خود را دارد (Ross, 2010: 125) و هیچ هماهنگی بین آن‌ها وجود ندارد. اعمال قانون برای پیشگیری از جرایم سایبری کم بوده و این نهادها به اندازه کافی به آسیب‌های ناشی از جرایم سایبری واکنش نشان نداده‌اند (Katyal, 2001: 1110). بیشتر اجرای قوانین بر روی تمهیدات دراز مدت جرایم اینترنتی برای کسب و کار دولت و افراد متمرکز شده است (Speer, 2000: 268).

در نتیجه خواسته‌های زیادی برای افزایش تنظیم مدیریت فعالیت‌های اینترنتی انجام شده است. به هر حال با اینکه تمام دولت‌ها موافق هستند که جرایم سایبری به عنوان یک مشکل ویژه مطرح می‌شود، اجماع اندکی در مورد اینکه چگونه مشکل را حل کنند وجود دارد. یکی از نهادهایی که به این خواسته‌ها واکنش نشان داد شورای اروپا بود. شورای اروپا، معاهده جرایم سایبری شورای اروپا (۲۰۰۱) را در مورد رسیدگی به جرایم اینترنتی تدوین کرد. این معاهده از کشورهای عضو و کشورهای ناظر خواسته است تا قوانین جدیدی را ایجاد کنند که به جرایم مختلف در اینترنت رسیدگی کنند و همکاری میان ادارات انتظامی کشورهای مختلف به منظور حفظ تحقیقات موثر در مورد مجرمان را افزایش دهند.

در این مقاله، معاهده جرایم سایبری شورای اروپا از نظر مولفه‌های نمادین آن مورد تجزیه و تحلیل قرار گرفته است. این تجزیه و تحلیل پرسش‌هایی در مورد اثر بخشی این معاهده و دیگر سیاست‌های جلوگیری از جرایم سایبری و توانایی اجرای قانون برای مبارزه با این مشکل را مطرح می‌کند که به نظر می‌رسد این معاهده آنگونه که باید اثر بخشی قابل توجهی نداشته است. برخی پیشنهادات برای یک سیاست بهتر برای پرداختن به جرایم سایبری انجام شده است.

۱- معاهده در مورد جرایم سایبری

در سال ۱۹۹۷ «شورای اروپا با همکاری ۴۷ کشور اروپایی، یک کمیته از کارشناسان در

[1] . Wired Society, The Nation. May 4, 2002.

زمینه جرایم سایبری برای تشخیص و تعریف کردن جرایم جدید، حقوق قانونی و مسئولیت کیفری در مورد اینترنت تشکیل دادند»(جلالی فراهانی، ۱۳۹۵: ۲۲). هم چنین کشورهای کانادا، ژاپن، آفریقای جنوبی و ایالات متحده دعوت شدند تا در این کمیته به عنوان کشور ناظر شرکت کنند. هدف ایجاد مجموعه‌ای از قوانین استاندارد در مورد جرایم سایبری برای جامعه جهانی و ایجاد یک سیاست جنایی مشترک برای جلوگیری از جرایم سایبری بود (نمامیان، ۱۳۹۲: ۲۷).

نتیجه نهایی مذاکرات در کمیته کارشناسان منجر به تدوین معاهده جرایم سایبری در ژوئن ۲۰۱۰ شد و در حال حاضر تنها سند جهانی در این زمینه است.[1]«معاهده شامل مقرراتی است در راستای مبارزه با تروریسم، سوء استفاده جنسی کودکان، جرایم سازمان‌دهی شده، نقض حق نسخه برداری، هک کردن و تقلب اینترنتی. این قرارداد هم چنین به عنوان یک چهار چوب برای همکاری‌های بین‌المللی بین کشورها در تحقیق و پیگیری جنایات سایبری عمل می‌کند. اگرچه بخش‌های معاهده شامل شرح و توصیف روشن استرداد می‌باشد»(میریان، ۱۳۸۶: ۱۱).

معاهده به سازمان‌های پلیس قدرت گسترش یافته‌ای برای بررسی و محاکمه جرایم کامپیوتری می‌دهد برای زمانی که این جرایم از مرزهای ملی عبور می‌کند.[2]در هفتم نوامبر سال ۲۰۰۲ شورا یک پروتکل اضافی جدا از جرایم اصلی سایبری تصویب کرد که مواد رایانه نژادپرستانه را از طریق شبکه‌های کامپیوتر سازمان‌دهی می‌کرد.

بعد از اینکه شورای اروپا معاهده پیشنهادی را توسط ۲۶ کشور عضو نهایی کرد، بوداپست امضا شد. کشورهای ناظر (ایالات متحده، آفریقای جنوبی، ژاپن و کانادا) گزینه‌ای برای امضا آن داشتند. سپس آن برای تصویب به کشورهای دیگر فرستاده شد. معاهده زمانی به اجرا در می‌آمد که پنج کشور از جمله حداقل ۳ کشور عضو شورای اروپا آن را تصویب می‌کردند. معاهده در یکم جولای ۲۰۰۴ لازم الاجرا شد. تاکنون کنوانسیون توسط ۳۹ کشور تصویب شده و هم چنین ۲۳ کشور آن را امضا کردند اما تصویب نکردند.[3]اگرچه به نظر می‌رسد که رویکرد معاهده، مبارزه با جرایم سایبری است اما واضح است که در معاهده عناصر نمادین زیادی وجود دارند.

۲- معاهده جرایم سایبری به عنوان سیاست نمادین

معاهده جرایم سایبری به طور عمده به صورت یک سیاست سمبلیک باقی می‌ماند و بنابراین تاثیر محدود و اندکی روی جرایم سایبری در بلند مدت خواهد گذاشت. معاهده آشکارا عناصر ۴

---

[1] . Council of Europe. Convention on Cyber Crime. Retrieved on 12th May 2011 from http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm, 2001

[2] . U.S. Ratifies International Cyber Crime Treaty, Computer Fraud and Security, November 2006, p.p 2-3.

[3] . Council of Europe. Convention on Cyber Crime. Retrieved on 12th May 2011 from http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm, 2001

عملکرد سیاست‌های سمبلیک را دارا است. سیاست‌های نمادین برای اولین بار توسط ادلمن[1] تعریف شدند. کسی که تشخیص داد بعضی سیاست‌ها خلق شده‌اند تا احساس عمومی را طوری بسازند که انگار کاری انجام شده تا مشکل را حل کند در حالی که در واقعیت سیاست‌ها هیچ تغییر واقعی و مهمی را نمی‌سازند و نه اینکه آن‌ها به عمق موضوع خاصی دست می‌برند.

۱-۲- عملکرد اطمینان بخش به عموم

سیاست‌های نمادین عملکردهای بسیاری دارند (Stolz, 1983: 157). اولین عملکرد: دادن اطمینان به عموم است که قانون‌گذاران در مسئله‌ای سخت‌گیری می‌کنند. معاهده جرایم سایبری شورای اروپا به طور واضح شامل عناصر خدمت رسانی است تا به عموم اطمینان بدهد که اقداماتی در مقابل جرایم سایبری انجام می‌شود. این معاهده خودش به عموم ثابت می‌کند که شورای اروپا و دیگر دولت‌ها یک طرحی را برای متوقف کردن آسیب‌های ایجاد شده به وسیله جرایم سایبری آماده می‌کنند و مصوبات انجام شده توسط دولت‌ها مشابه این امر را نشان می‌دهد.

به هر حال سوالاتی از این قبیل مطرح می‌شوند که آیا معاهده در حل مسائل و مشکلات موثر خواهد بود؟ «از طرفی معلوم نیست که متن قرارداد به طور کامل اجرا خواهد شد و بنابراین معاهده مسئله را درست حل نخواهد کرد. تقریباً نوزده سال است معاهده اصلی به تصویب رسیده است. در اصل این معاهده در سال ۲۰۰۱ تصویب شد و تا اوایل ۲۰۱۳، تنها ۳۹ کشور آن را تصویب کردند و ۱۲ کشور نیز آن را امضا نموده‌اند. اگرچه معاهده توسط بسیاری از کشورها به طور رسمی امضا شده، اما به طور مشخص قبول نشده است»(Hilley, 2005: 171). در واقع، تصویب رسمی قوانین هماهنگ مورد توجه قرار نگرفته است (Swire, 2005: 1989). این نشان از یک سیاست نمادین است، اگرچه این معاهده به طور رسمی امضا شده، اما هیچ اقدام دیگری از سوی بسیاری از کشورها برای اجرایی شدن مقررات این معاهده صورت نگرفته است. بنابراین، عموماً به نظر می‌رسد اگرچه اعضای شورای اروپا سیاست‌های جدیدی را برای مقابله با جرایم اینترنتی ایجاد کرده‌اند، اما مقررات آن معاهده در حدود نیمی از کشورهای عضو در حال اجرا نیست.

۱-۱-۲- مشکلات مربوط به کشورها

بسیاری از کشورها به طور رسمی با این معاهده موافق نیستند و بنابراین برای اجرای معاهده الزامی نمی‌بینند. علاوه بر این، «حتی برای کشورهایی که این معاهده را تصویب کرده‌اند، مقررات ممکن است به طور کامل اجرایی نشود. برای جلوگیری از اجرای کامل این معاهده مخالفت‌های زیادی وجود دارد. علاوه بر این، ناسازگاری زیادی از یک کشور با کشور دیگر

[1]. Edelman

وجود دارد، و تلاش برای همکاری بین کشورها مشکل می‌باشد»(سورنسون و جکسون، ۱۳۹۴: ۲۵۸). این احتمال است که بیشتر کشورها قوانین را به صورت متفاوت اجرا کنند، همیشه وجود داشته است.

علاوه بر این، حتی اگر یک کشور معاهده را تصویب کند، به این معنا نیست که آنها قوانین را پیاده سازی خواهند کرد. بنابراین، «این معاهده برای تحقیق و مجازات مجرمان سایبری به همکاری بین‌المللی به ویژه از طریق پلیس بین‌الملل (اینترپل) متکی است. این امر ممکن است منجر به این گردد که برخی از کشورها سخت تر از بقیه بررسی کنند یا به برخی از صدمات بیش از بقیه بپردازند. به علاوه، برخی از کشورها وجود دارند که منابع لازم برای اجرای این قانون را ندارند. از آنجا که معاهده در کشورها تا قبل از امضا و تصویب دارای جنبه قانونی الزام آور و معیارهای هماهنگی نیست، اقدامات تنها اثر محدودی دارند»(Walden, 2004: 329). اگر چه چنین همکاری بین دولت‌ها در روی کاغذ موثر به نظر می‌رسد، اما در عمل بسیار دشوار است. هنگامی که در مورد جرایم اینترنتی موضوعی مطرح می‌شود، تفاوت بین کشورها وجود دارد. برخی منابع کافی ندارند، آموزش لازم با سطح مناسب پیچیدگی یا حتی تمایل به درک ماهیت جرایم اینترنتی. «در بعضی موارد، برخی از کشورها ممکن است احساس کنند که در مورد این جرایم صلاحیت ندارند، بنابراین آن جرایم را به یک کشور دیگر برای بررسی اتهامات ارجاع می‌دهند. اگرچه برخی از کشورها سازمان‌هایی برای هماهنگ کردن تحقیقات جرم و جنایت سایبری تاسیس کرده‌اند، که دیگران انجام نداده‌اند»(Katyal, 2001: 1112). به عنوان مثال شورای اروپا یک سازمان پیشرفته را به نام «انیسا»[1]ایجاد کرد که مسئول هماهنگی تحقیقات جرایم اینترنتی در کشورهای عضو می‌باشد. اما همه کشورها چنین سازمانی ندارند.

تفاوت در جمع آوری حفظ و تحلیل شواهد وجود دارد. کشورها دارای استانداردهای متنوعی برای جستجو و تشنج هستند. در ایالات متحده امریکا الزامات اخذ حکم بازرسی برای ارتباطات مخابراتی کاملاً سختگیرانه است. «گاهی اوقات مقامات مجری قوانین را نادیده می‌گیرند، اما در مواردی که محققین بر این باورند که این قانون را نقض کرده‌اند، اتهامات عنوان شده علیه متهم ممکن است کاهش یابد و او سیستم عدالت کیفری را ترک کند. بعضی از کشورها برای تحقیقات آنلاین در مورد مجرمان اجازه ندارند، زیرا آنها استفاده بیش از حد از قدرت پلیس را تلقی می‌کنند. به دلیل تفاوت در سیاست‌های جستجو و تشنج، مقررات معاهده اروپایی ممکن است به طور یکسان یا پیوسته اجرا نشود»(Grabosky, 2007: 84). برخی از منتقدان معاهده اظهار داشتند که کشورهای امضا کننده این قانون «مشکل» کشورها نیستند (Schell & Martin, 2004: 53). بسیاری از کشورها برای مبارزه با جرایم اینترنتی فوریت را به اشتراک

[1]. ENISA

نمی‌گذارند. «آنها ارزش‌های متفاوتی دارند یا مشکلاتی دارند که بیشتر آنها را مطرح می‌کنند که نیاز به توجه دارد. این کشورها به مجرمان سایبری یک پناهگاه امن برای فعالیت می‌دهند»(Sinrod & Reilly, 2000: 49).

بسیاری از کشورها در مورد جنبه‌های دیگر معاهده نگرانی دارند، همچنین اجرای کامل آن را ممنوع کرده‌اند. نخست این که ماده قانونی دوگانه وجود ندارد. این بدان معنا است که امریکا بایستی در قبال درخواست یک دولت خارجی در زمانی که فعالیت شخص، جرم در کشور خارجی است اما در آمریکا قانونی تلقی می‌شود، اقدام به تحقیق و توقیف نماید. به عبارت دیگر، این فعالیت می‌تواند در امریکا قانونی باشد اما در کشور دیگری غیر قانونی است. شخصی که این فعالیت را انجام می‌دهد می‌تواند توسط مقامات ایالات متحده امریکا براساس درخواست کشور دیگری مورد بازجویی قرار گیرد. به عنوان مثال، فعالیت می‌تواند شامل سخن گفتن از نفرت باشد که در امریکا حمایت می‌شود، اما در آلمان غیر قانونی می‌باشد. احتمال این امر بیشتر است که حقوق کشور امریکا در صورت قانونی بودن رفتاری به بررسی آن در قبال شهروندان بپردازد.

برخی کشورها حتی ممکن است یک پناهگاه امن برای مجرمان سایبری که با استفاده از این تکنولوژی به قربانیان ناآگاه ضرر رسانند، فراهم کنند. «مجرمان سایبری به آن کشورهایی که در اجرای قانون ضعف دارند و دارای قوانین کوچک برای دفاع از خود در مقابل جرایم اینترنتی هستند خواهند رفت. به عنوان مثال، هیچ قانونی در کره شمالی در برابر جرایم اینترنتی وجود ندارد و مجرمان نسبتاً امن از پیگرد قانونی هستند. حتی اگر این قوانین، در کشورهایی که در حال حاضر قوانینی ندارند، تصویب شود یا آنها را اجرا نکند. برای کسانی که سعی در دزدیده شدن یا تحویل دادن اطلاعات دارند، همیشه برای آنها پناهگاه وجود خواهد داشت»(Sharma, 2005: 3042). به طور کلی، حتی اگر مقررات این معاهده اجرایی شود، این شانس وجود دارد که مجرمان اینترنتی راه‌هایی برای فرار از پیگرد قانونی پیدا کنند. همراه با این موارد و به احتمال زیاد پس از اجرای جرایم و آسیب‌ها، جرم‌های فضای مجازی در حال رشد توجه مقامات را به خود جلب می‌کنند. در هر مورد، تعیین این که چه کسی مجرم بوده و یا محل دقیق آنها دشوار است. تحقیق در مورد این جرایم و پیدا کردن و مجازات مجرمان نیاز به منابع متعدد از نظر پول و پرسنل برای تحقیق و پیگرد جنایت دارد. این بدان معنی است که بسیاری از جنایتکاران سایبری به سادگی آزاد خواهند شد.

۱-۲-۲- مشکلات مربوط به ارائه دهندگان خدمات اینترنتی

این معاهده به دولت‌های امضا کننده، که قدرت گسترده نظارت و رهگیری و همچنین قدرت برای کمک به ارائه دهندگان خدمات نیاز دارد (Coleman, 2003: 135)، به نظر می‌رسد که مفاد معاهده برای کاهش جرایم سایبری مفید خواهد بود. بعضی از منتقدان بر این باورند که این واقعاً

راهی برای افزایش قدرت پلیس است. با افزایش نیروهای تحقیقاتی اجرای قانون، دولت‌ها نیز کنترل خود را بر اینترنت و ترویج نظارت به نام جلوگیری از «جرایم اینترنتی»، «جنگ اطلاعاتی» یا حفاظت از «زیرساخت‌های حیاتی» را افزایش داده‌اند. این منجر به خطر بالقوه‌ای می‌شود که معاهده می‌تواند توسط بعضی کشورها برای نظارت بر شهروندان یکدیگر مورد استفاده قرار گیرد، حتی اگر آنها مشکوک به اقداماتی باشند که آن اقدامات در کشور خود جرم محسوب نمی‌شود. بنابراین در صورت اینکه دولت‌ها از دیگر کشور جاسوسی اینترنتی کنند، در صورت اثبات، مسئول هستند. چرا که «مسئولیت دولت از اصول بنیادین حقوق بین‌الملل است که به منظور حمایت از حقوق ملت‌ها در برابر دولت‌ها وضع شده است»(رحیمی، ۱۳۹۷: ۶۷).

نگرانی‌های ناشی از مسئولیت تحقیقات از دیگر نگرانی‌هایی است که ممکن است از اجرای کامل قانون جلوگیری کند. «بر اساس مفاد این معاهده ارائه‌دهندگان خدمات اینترنتی نیازمند این هستند که با توجه به فعالیت‌های کاربران خود اطلاعات آن را حفظ کنند. عده‌ای اعتقاد دارند که این خطر زیادی برای حریم خصوصی و حقوق بشر کاربران دارد. معاهده برای ارائه دهنده‌های خدمات اینترنتی محتوی شخص ثالث که به صورت ناعادلانه برای تولیدکنندگان جدید قرار می‌دهد مسئولیت در نظر می‌گیرد. خدمات شبکه ممکن است نظارت نامناسب بر روی ارتباطات خصوصی را تشویق کند. علاوه بر این ارائه دهنده خدمات اینترنتی ممکن است به دلیل عدم نظارت مناسب بر مشتری‌ها با محتوای کاربر یا برای اعمال جنایی کارکنان خود مجرم شناخته شوند. منتقدان اروپایی این معاهده نگران حق انتقال اطلاعات شهروندان اروپایی به خارج از اروپا و مقامات غیر اروپایی هستند»(Yam, 2001: 9).

نگرانی‌های زیادی در مورد عدم توجه به مراقبت از مسائل مربوط به حفاظت از اطلاعات شخص توسط مقررات این معاهده وجود دارد (Hilley, 2005: 173). بسیاری از سازمان‌های حقوق بشر نگرانی خود را راجع به این معاهده به ویژه از آن جهت که قدرت دولت‌ها را در سراسر جهان گسترش نمی‌دهند ابراز کرده‌اند. «گروه‌های آزادی‌های مدنی تاکید دارند که این کنوانسیون حقوق حریم خصوصی را تحت‌الشعاع قرار می‌دهد و قدرت نظارتی را به مقامات ارائه می‌دهد. سازمان‌های مختلف امریکایی ابراز می‌کند که این معاهده اجازه‌ی انجام نظارت و جست و جوهایی را می‌دهد که توسط قانون امریکا مجاز نمی‌باشد. کمپین بین‌المللی آزادی در نامه‌ای نگرانی‌های خود را ابراز داشت»(Wales, 2000: 7).

۳-۱-۲- ناسازگاری معاهده شورای اروپا

اگرچه این معاهده سعی در تعریف اصطلاحات و ایجاد نوعی انسجام داشت اما به نظر می‌رسد که مقررات آن فاقد شفافیت بوده و معلوم نیست و فقط تعریف بسیار مبهمی از برخی اصطلاحات می‌دهد. مثلاً تعریف «ابزارهای غیرقانونی برای اطمینان از این که کار نمی‌کند» مشخص نیست آیا کافی است یا نه؟ با این وجود به مبنای کلی برای بررسی افراد دیگر در

فعالیت‌های مرتبط با کامپیوتر تبدیل شده است. این کاملاً قانونی است. به عنوان مثال اصطلاح دیگر «ارائه دهنده خدمات» در معاهده با عنوان یک نهاد که داده‌ها را برای چندین سرور ذخیره می‌کند، تعریف شده است. منتقدان می‌گویند براساس این تعریف می‌توان عملیات تحویل یک پیتزا را می‌توان یک سرویس دهنده در نظر گرفت (Yam, 2001: 9). از آنجایی که اصطلاحات بسیار وسیع هستند، اجرای معاهده بسیار سخت خواهد بود و از کشوری به کشور دیگر تعاریف و تفاسیر بسیار متفاوت خواهد بود. دولت‌ها می‌توانند رویکردهای گسترده‌ای را در مورد قوانین خرد داشته باشند و در آن حالت تصویب قوانین بسیار متفاوت خواهد بود. برای مثال «همان طور که تعریف تقلب محتوی پورنوگرافی را نیز در بر می‌گیرد از دولتی به دولت دیگر متفاوت است. تعدادی از کشورها براساس قانونی اساسی از وضع بعضی قوانین منع شده‌اند. علاوه بر این کنگره نمی‌تواند بر روی سخنرانی‌های آزاد روی اینترنت محدودیت‌هایی را اعمال کند»(Simon, 1998: 1035). این امر نیز منجر به ایجاد ناسازگاری‌ها و مشکلات اجرایی می‌شود.

بیشتر ناسازگاری‌ها ناشی از این امر است که معاهده نهایی شامل مقرراتی است که توسط کشورهای عضو مورد توافق قرار نگرفته است. اختلافات واضح و آشکار میان اعضا ناظران شورا در مورد مواردی که عنایت خاصی را مطرح می‌کنند وجود دارد براساس این معاهده ردیابی و محاکمه جرایم سایبری همچنان دشوار خواهد بود (Convention on Cyber crime Computer Fraud and Security, 2002: 4-5). داده‌های رایانه‌ای بسیار فرّار هستند بنابراین می‌توانند با استفاده از چندین کلید میانبر یا با استفاده از برنامه‌های خودکار اطلاعات کلیدی را حذف کنند. در این صورت غیر ممکن است که بتوانیم یک مرتکب جرم را مجرم بنامیم و یا اثر مخرب عمل آن‌ها را از بین ببریم. «مجرمان سایبری کشف کرده‌اند که به آسانی می‌توانند در یک حوزه قضایی در جرمی شرکت داشته و در حوزه قضایی دیگر پنهان شوند خصوصاً در کشورهای توسعه یافته و کشورهای فقیر»(Sinrod & Reilly, 2000: 28).

در واقع جرایم اینترنتی در کشورهای در حال توسعه شایع‌تر است زیرا فقدان قانون کافی و یا اجرای صحیح برای مقابله با این مسئله وجود دارد. مجرمان کامپیوتری در حال حاضر و در آینده به راحتی می‌توانند از مکانی به مکان دیگر حرکت کرده و به دنبال پناهندگی از کشورهایی باشند که به این معاهده نپیوسته‌اند و یا قصد اجرای آن را ندارند. آن‌ها حملات خود را از کشورهایی که قوانین قابل ملاحظه ای ندارند و نسبتاً از پیگرد امن هستند انجام خواهند داد.

٢-٢- عملکرد معاهده در آموزش اخلاقی

سیاست نمادین دیگری که در معاهده جرایم سایبری شورای اروپا مشهود است، آموزش اخلاقی است. این معاهده در جهت کمک به یادگیری مردم است که چه اعمالی در رابطه با اینترنت صحیح و چه رفتارهایی غلط است و این آموزش‌ها ناشی از این است که اینترنت یک

پدیده جدید است برخی از افراد مطمئن نیستند که واقعاً کدام رفتار صحیح و کدام نادرست است و این افراد نیاز دارند تا رفتارهای مورد قبول و رفتارهای غیر قابل قبول در رابطه با اینترنت بیشتر برای آن‌ها توضیح داده شود.

این معاهده همچنین به ایجاد «توافق اخلاقی»، هم در یک کشور و هم در سطح بین‌المللی درباره رفتار مجرمانه در اینترنت و ارائه تعاریف از جرایم کمک می‌کند.

اگرچه هیچ مجازاتی در معاهده جرایم سایبری تعیین نشده است، اما در قواعد اختصاصی کشورهای مختلف تنظیم شده‌اند. این در خدمت کمک به شهروندان است از حیث نشان مراتب جرم با تقویت این ایده که این رفتار بد یا اشتباه است. این قوانین هم چنین به اشخاصی که جرم اینترنتی را مرتکب نمی‌شوند اطمینان خاطر می‌دهد که به طور مناسب عمل می‌کنند و آن‌ها را از کسانی که مرتکب جنایت می‌شوند تمییز می‌دهند. معاهده هم چنین آموزش‌های عمومی راجع به جرایم اینترنتی و راه‌حل‌های ممکن را می‌دهد این موضوع به مردم کمک می‌کند تا مشکلات موجود را بهتر درک کرده و گزینه‌های بالقوه سیاسی را برای حل مشکل در نظر بگیرند.

۳-۲- عملکرد به عنوان نمونه و مدل برای کشورهای دیگر

هدف سوم از سیاست نمادین این است که به عنوان مدلی برای دیگر دولت‌ها عمل کند. معاهده شورای اروپا به وضوح این نقش را برآورده می‌کند. «برای آن دسته از کشورهایی که در مورد جرایم سایبری قوانینی ندارند، این معاهده با عنوان یک الگو عمل می‌کند. مقررات این معاهده به طور خاص مشخص می‌کنند که کدام قوانین بایستی برای هر دولتی به تصویب برسد تا برای مقابله با جرایم سایبری موثر باشند. بنابراین شورای اروپا در پی مدلسازی از قوانین است که چه قوانینی باید تصویب شوند که برای مقابله با جرایم مناسب موثرتر باشند تا به عنوان راهنمایی برای هر کشوری باشد که می‌خواهد برای جلوگیری از جرایم اینترنتی قوانین را توسعه دهند» (Silver, 2001: 5).

قانون مقابله با جرایم اینترنتی در کنگره ایالات متحده آمریکا در سال ۲۰۰۲ به عنوان بخشی از قانون امنیت داخلی تصویب شد. مجازات‌های سخت برای جرایم مربوط به کامپیوتر در نظر گرفته می‌شود. برگه جرایمی که منجر به آسیب به فرد یا مرگ می‌شوند، مانند زندگی در زندان. «در سال ۲۰۰۳ انگلستان یک سری مقررات را تصویب کرد که مردم را مجبور به انتخاب ایمیل‌های ناخواسته می‌کرد. این قانون حریم خصوصی و تنظیمات ارتباطات الکترونیکی نامیده شد. این قانون ایمیل را بدون اخطار قبلی از دریافت کننده ممنوع می‌کرد. در امریکا در سال ۲۰۰۳، کنگره کنترل مبارزه با پورونوگرافی بدون درخواست و بازاریابی، یا عملکرد کن اسپم[1] که در سال ۲۰۰۴ به کار می‌آمدند را تصویب کرد. این فرستنده‌ها را ملزم به ارائه یک گزینه

[1]. Can Spam

اختیاری برای گیرندگان می‌کند»(Kigerl, 2009: 573). همانند قوانین و مقررات انگلستان این قانونگذاری یک سری مجازات‌های کیفری و محدودیت‌ها را برای انتقال ایمیل‌های الکترونیکی ناخواسته تحمیل کرد یا قوانین زیادی در بسیاری از کشورها توزیع سنتی و فیزیکی بچه‌های پورونوگرافی را مجازات می‌کرد.

بنابراین معاهده قوه مقننه کشورها را مجبور کرد تا قوانین جاری خود را دوباره بررسی کرده و آن را به روز رسانی کنند. در طول فرآیند تصویب در ایالات متحده آمریکا، تصمیم گرفته شد که قوانین کافی در مورد درخواست‌هایی که مطابق با معاهده هستند، وجود داشته باشد و سنا را مجبور کرد تا قوانین جاری را بررسی کند و مشخص کند که آیا آن‌ها به روز رسانی شده‌اند یا نه؟

٤-٢- عملکرد به عنوان رفتار بازدارنده جنایی آینده

عنصر نهایی یک سیاست نمادین این است که به عنوان یک بازدارنده برای رفتارهای جنایی آینده خدمت می‌کند. نقش معاهده به عنوان یک بازدارنده جای سوال دارد. معاهده مجازاتی برای جرایمی که آنها مشخص کرده بودند معین نکرده بود. به جای آن هر کشوری اجازه داشت طبق ساختار و عملکرد جرایم‌شان تعیین کند. این چیزی است که به عنوان یک ضعف در معاهده درک می‌شود (Coleman, 2003: 136). بازدارنده‌ها سپس براساس تنبیه ها و مجازات‌هایی پایه گذاری می‌شوند که توسط دولت فردی تعیین شده‌اند تا اینکه توسط یک سازمان بین‌المللی. با وجود این ممکن است مردمی که در این کشورها به خاطر جرایم سایبری مجازات شده بودند از ارتکاب جرایم سایبری به خاطر احتمال مجازات خودداری کنند.

علاوه بر این از آنجایی که معاهده توسط تمامی کشورها امضا نشده بود. واضح است که تعداد قابل توجهی از کشورها قوانین را برای جرایم سایبری اعمال نکرده‌اند. برای اینکه آن بازدارنده باشد کشورهای بیشتری مجبورند که معاهده را امضا کنند و بر اساس دستوراتش عمل کند.

پیشنهادها

متاسفانه تنظیم اینترنت دشوار است چرا که جهان پهناور است و مرزها را نمی شناسد. چرا که هیچ یک از مقررات قانون بر کل اینترنت اولویت ندارد، جرایم سایبری جرایمی نیستند که توسط عملکردهای دولت حل شوند. معاهدات جدید کافی نیستند. بایستی سیاست‌های جامع در بسیاری از جهان به منظور داشتن یک مبارزه کامل و موثر در مقابل جرایم سایبری اعمال شوند.

بایستی مبارزه جدی در مقابل جرایم سایبری در سطوح مختلف مورد توجه قرار گیرد. در یک مقیاس بزرگ، قوانین مرتبط بایستی ایجاد شود و در یک سطح محلی بایستی شیوه‌های

مدیریتی بهتری اتخاذ شوند تا جرایم جدید را کنترل نماید. موارد زیر پیشنهاداتی برای سیاست‌های بهتر در زمینه جرایم سایبری هستند.

۱- در ابتدا محل‌های کسب و کار و سازمان‌ها بایستی نقش فعالی در مبارزه با جرایم سایبری داشته باشند. «در بسیاری از موارد نقض امنیتی نتیجه عملکرد ضعیف فرآیندهای داخلی است مانند کمبود آگاهی کارکنان یا کنترل ضعیف. بنابراین سازمان‌های کسب و کار بایستی مجازات‌های خودشان را در زمینه جرایم سایبری پیاده کنند»(Lawrie, 2002: 5). محل‌های کسب و کار و سازمان‌ها بایستی مسئولیت تشخیص بافت‌های امنیتی بالقوه را در سیستم‌های کامپیوتر خود بر عهده بگیرند و همچنین بایستی مسئولیت درست کردن و پیاده سازی طرح‌هایی برای برخورد با این گونه خطرات را بر عهده بگیرند. «توصیه می‌شود که شرکت‌ها یک مسابقه هک را اجرا کنند که مردم بتوانند هک کردن در سایت‌ها را به عنوان یک بازی یا تمرین امنیتی امتحان کنند و یاد بگیرند. تا حفره‌های بالقوه را یک چشم‌انداز تشخیص دهند و یک شبکه یا امنیت بالا را بوجود آورند»(Wible, 2003: 1579).

۲- بهتر است تمامی صنایع مرتبط با تکنولوژی یا کامپیوتر برای تولید تکنولوژی‌هایی با امنیت بالا و جدید تشویق شوند تا در مقابل جرایم سایبری در آینده محافظت شوند. اینها باید دائماً به عنوان مجرمان سایبری توسعه پیدا کنند. و شیوه‌های جدیدی برای ارتکاب جنایات در اینترنت ایجاد کنند.

۳- کاربرها و صاحبان سیستم‌ها بایستی در مورد تهدید آن و آسیب پذیری‌های اینترنتی اگاهی پیدا کنند. لازم است که آنها در مورد جرایم بالقوه هوشیار باشند. و هر موقع لازم است احتیاط کنند و همچنین بهتر است زمانی که آسیبی یا تهدیدی اتفاق می‌افتد آن را گزارش دهند.

۴- لازم است قوانین موجود به طور منظم به روز شوند. زمانی که تکنولوژی‌های جدید توسعه و گسترش پیدا می‌کنند و جرایم جدید پیشرفت می‌کنند یا زمانی که جرایم سایبری شیوه‌های جدید برای فرار کردن از پلیس پیدا می‌کنند.

۵- محققان واجد شرایط و شناخته شده خصوصی یا دولتی باید آموزش ببینند که بتوانند از پیشرفت‌های خود در تکنولوژی حمایت کنند و دانش تخصصی در راستای بررسی جرایم رایانه‌ای ایجاد کنند (Chung & Chou, 2006: 672). آنها می‌توانند آسیب‌پذیرهای الکترونیکی را بیابند و نواحی بالقوه نگران کننده را قبل از اینکه آسیب برسانند شناسایی کنند.

۶- تحقیقات لازم است که براساس همکاری میان پلیس از تمامی کشورها پایه‌گذاری شوند. «اینترپل آژانسی است که می‌تواند تبادل اطلاعات و همکاری در سطح بین‌الملل را فراهم آورد. اما همکاری در قانون از اجرای تمام قانون در پیاده سازی قوانین جرایم سایبری در آینده ضروری تر است»(Brenner & Schwerha, 2004: 114). همزمان آمریکا نیاز دارد تا اصول دیپلماتیک

اقتصادی، نظامی، اطلاعاتی خود را برای پیگیری مشارکت جهانی که می‌توانند در فراهم آوردن یک فضای سایبری امن کمک کنند، تعامل کند.

۷- همچنین ممکن است به خوبی از وقوع جرم و جنایت جلوگیری کند. اینترنت به آسانی و به ارزانی به یک مجرم توانایی ارتکاب جرم را می‌دهد و به میلیون‌ها قربانی بالقوه دسترسی دارد و قادر است فعالیت‌هایش را بلافاصله به پایان برساند. آنها می‌توانند عملکردههایشان را با استفاده از سیستم‌ها در چندین کشور پنهان کنند. آی اس پی‌ها می‌تواند به طور تصادفی ترافیک شبکه را برای فعالیت‌های مشکوک نظارت کند. به خصوص با در نظر گرفتن سایت‌های مهم انتقادی مانند رایانه‌های نظامی یا شبکه‌های برق آن‌ها می‌توانند وب سایت‌های میزبانی شده در شبکه‌های خودشان را از برنامه‌های غیر قانونی اسکن کنند.

اسکن ایمیل برای ویروس حتی ساختن محدودیت‌های نرم‌افزار و سخت افزار برای سیستم‌هایشان آی اس پی‌ها می‌توانند در توسعه پروفایل‌های هکرها کمک کنند و اگر لازم باشد می‌توانند بعضی مشترکان را از شبکه خارج کنند. آی اس پی‌ها می‌تواند نمونه‌هایی از جرایم رایانه‌ای بالقوه را گزارش کند و آن را برای اجرای قوانین آسان کند تا جرایم سایبری را بررسی کند.

۸- در پایان نیاز به مقررات بین‌المللی جهانی اینترنت واضح است. مشارکت گروه‌هایی مانند ایالات متحده یا دیگر جوامع جغرافیایی مانند شورای اروپا به دلیل جنبه‌های جهانی در تاثیر موثر قوانین مربوط به جرایم سایبری و اجرای آن کلیدی هستند. با توجه به جنبه‌های جهانی اینترنت، هیچ قانون واحد در یک کشور به طور موثر آسیب ناشی از آن را توسط جنایتکاران اینترنت کاهش نخواهد داد.

نتیجه‌گیری

شکی نیست که جرایم سایبری بالقوه مضر و منشعب هستند. از این رو، جرایم سایبری عملاً بر روی همه دولت‌ها اثر گذار است. هیچ سوالی درباره نیاز به مضر بودن و هماهنگ بودن با قوانینی که همکاری بین‌المللی را برای مبارزه با جرم در فضای سایبری درگیر می‌کند وجود ندارد. روابط بین‌الملل نمی‌توانند نسبت به جرایم فضای مجازی بی‌تفاوت باشند که این بی‌تفاوتی تشویقی برای طمع ورزی مهاجمان فضای مجازی و نتیجه‌ای برای رفتارهای مجرمانه جدی خواهد بود. معاهده شورای اروپا مهم‌ترین معاهده برای نظارت بر جرایم رایانه‌ای می‌باشد. با وجودی که چشم انداز بین‌الملل در جنگ با جرایم مجازی مهم است همزمان مشکل می‌نماید.

در ایجاد معاهده شورای اروپا نمایندگانی از بسیاری کشورها گرد آمدند؛ هم از اعضا و هم از کشورهای خارجی، برای بحث و مناظره درباره تعریف فعالیت‌های مشخصی که در اینترنت رخ

می‌دهد و سپس با ارائه تعریفی که چه فعالیت‌هایی بیشتر مناسب و منصفانه و همچنان تاثرگذار برای مبارزه با جرایم فضای مجازی خواهند بود. آن‌ها متوجه نیاز به رویکرد بین‌المللی سازگار برای مبارزه با جرایم فضای مجازی که شامل همکاری بین نمایندگان اجرای قانون جهت رسیدگی به جرایم می‌باشند، شدند.

به هر حال، به جهت اینکه این قرارداد تا حد زیادی نمادین است؛ باید تاثیرات بلند مدتش زیر سوال برده شود. برخی مشکلات در رابطه با تعریف شرایط ذکر شده در معاهده وجود دارد. مسئله حفظ حریم خصوصی توانایی رسیدگی و ایجاد اسناد به علاوه قانون بین‌المللی خواستار همکاری بین کشورها است که از پیش بردن این کار دشوار می‌نماید. به طور کلی شکاف‌های زیادی برای اجازه به ادامه حیات جرایم وجود دارد. راه‌های زیادی برای مجرمان وجود دارد که حتی با وجود معاهده به اجرای اعمال خود ادامه می‌دهند.

برای اینکه معاهده اثرگذار باشد نیاز خواهد بود که کشورهای زیادی معاهده را امضا و تصویب کنند و آن را به یک قانون بین‌المللی تبدیل سازند. تا آن زمان جرایم فضای مجازی با هیچ کدام از راه‌های قابل توجهی تاثیر گذار نخواهد شد.

منابع

- جلالی فراهانی، ا. (۱۳۹۵)، ***کنوانسیون جرایم سایبر و پروتکل الحاقی آن***، تهران، انتشارات خرسندی، چاپ دوم.
- جلالی فراهانی، ا. (۱۳۸۷)، جنبه‌های حقوقی اقدامات کیفری بین‌المللی مجریان قانون در قبال جرایم سایبری، ***فصلنامه مطالعات پیشگیری از جرم***، سال ۳، شماره ۸، صص ۸۱-۳۵.
- جلالی فراهانی، ا. (۱۳۹۴)، ***درآمدی بر آئین دادرسی کیفری جرایم سایبری***، تهران: انتشارات خرسندی، چاپ دوم.
- سورنسون، گئورک و رابرت جکسون (۱۳۹۴)، ***درآمدی بر روابط بین‌الملل***، مترجمین: احمد تقی زاده، مهدی ذاکریان و حسن سعید کلاهی، تهران: انتشارات میزان.
- رحیمی، رئوف (۱۳۹۷)، «مسئولیت دولت و بخش خصوصی در قبال حقوق بشر»، ***فصلنامه مطالعات بین‌المللی***، سال ۱۵، شماره ۵۹، صص ۶۵-۸۸.
- گرکی، م. (۱۳۸۹)، ***جرایم سایبری: راهنمایی برای کشورهای در حال توسعه***، ترجمه مرتضی اکبری، تهران: نیروی انتظامی جمهوری اسلامی ایران، پلیس امنیت فضای تولید و تبادل اطلاعات.
- میریام، اف. میکولون (۱۳۸۶)، «کنوانسیون جرم‌های سایبری: اجرای هماهنگ حقوق کیفری بین‌المللی؛ چشم انداز فرآیند دادرسی عادلانه چیست؟»، ترجمه ا. جوانبخت، ***مجله حقوقی دادگستری***، شماره ۵۹، صص ۲۱۶- ۱۸۱.

- نمامیان، پ. (۱۳۹۲)، «مواجهه با تروریسم سایبری در حقوق بین‌الملل کیفری»، ***فصلنامه پژوهش‌های ارتباطی***، سال ۲۰، شماره ۱، صص ۴۲ -۹.

English Reference

- Berman, P. S. (2002), "The Globalization of Jurisdiction", ***University of Pennsylvania Law Review***, 151(2), pp. 317-329.

- Boni, B. (2001), ***Creating a Global Consensus Against Cyber Crime***, New York: Network Security.

- Brenner, S. and J. J. Schwerh (2004), "Introduction—Cyber Crime: A Note on International Issues", ***Information Systems Frontiers***, 6(2), pp. 105-114.

- Chung, W., H. Chen & S. Chou (2006), "Fighting Cyber Crime: A Review and The Taiwan Experience", ***Decision Support Systems***, 1(4), pp. 667-679.

- Coleman, C. (2003), "Security Cyberspace—New Laws and Developing Strategies", ***Computer Law and Security Report***, 19(2), pp. 129-141.

- Convention on Cyber Crime Update (2002), ***Computer Fraud and Security***, pp. 4-5.

- Council of Europe. (2011), "Convention on Cyber Crime", Retrieved on 12th May 2011 from ***http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm***

- Gercke, M. (2009), "Europe's Legal Approaches to Cyber Crime", ***ERA Forum 10***, pp. 145-153.

- Grabosky, P. (2007), ***Electronic CrimeUpper Saddle River***, New Jersey: Pearson/Prentice Hall.

- Hilley, S. (2005), "Pressure Mounts on US Senate to Pass Cyber Crime Treaty", ***Digital Investigation***, 1(2), pp.167-178.

- Katyal, N. K. (2001), "Criminal Law in Cyberspace", ***University of Pennsylvania Law Review***, 149(4), pp. 106-119.

- Kellermann, T. (2010), "Building a Foundation for Global Cybercrime Law Enforcement", ***Computer Fraud and Security***, 4(10), pp. 5-12.

- Kigerl, A.C. (2009), "CAN SPAM Act: An Empirical Analysis", ***International Journal of Cyber Criminology***, 3(2), pp. 571-579.

- Lawrie, L. (2002), "A Twin-Pronged Approach in the Fight Against Cyber Crime", ***The Scotsman***, May 8, pp. 5-18.

- Monshipouri, M., Prompichai, T. (2018), "Digital Activism in Perspective: Palestinian Resistance via Social Media", ***International Studies Journal (ISJ)***, 14(4), pp. 42-63.

- Nuth, M. S. (2008), "Taking Advantage of New Technologies", For and ***Against Crime Computer Law and Security Report***, 24, pp. 431-442.
- Ross, J. I. (2010), ***Criminal Investigations: Cyber Crime***, New York: Chelsea House.
- Schell, B. H., & C. Martin (2004), ***Cyber crime: A Reference Handbook***, Santa Barbara, California: ABC-CLIO.
- Sharma, A. (2005), "World Seeks a Wider Web Role", ***Congressional Quarterly Weekly***, Report Nov 14, pp. 3039-3047.
- Simon, G. E. (1998), "Cyberporn and Censorship: Constitutional Barriers to Preventing Access to Internet Pornography by Minors", ***The Journal of Criminal Law and Criminology***, 88(3), pp. 1033-1043.
- Silver, O. (2001), "European Cyber Crime Proposal Released", ***Computer Fraud and Security***, (5), pp. 3-17.
- Sinrod, E. J. & W.P. Reilly (2000), "Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws", ***Santa Clara Computer and High Technology Law Journal***, 16(2), pp. 3-51.
- Speer, D. L. (2000), "Redefining Borders: The Challenges of Cyber Crime", ***Law and Social Change***, 34, pp. 261-273.
- Stolz, B. A. (1983), "Congress and Capital Punishment: An Exercise in Symbolic Politics", Law and Policy Quarterly, 5(2), pp. 153-165.
- Swire, P. P. (2005), "Elephants and Mice Revisited: Law and Choice of Law on the Internet", ***University of Pennsylvania Law Review***, 153(6), pp. 1979-1992.
- U.S. Ratifies International Cyber Crime Treaty (2006), ***Computer Fraud and Security***, November 5, pp. 1-27.
- Walden, I. (2004), "Harmonising Computer Crime Laws in Europe", ***European Journal of Crime; Criminal Law and Criminal Justice***, 12(4), pp. 325-335.
- Wales, E. (2000), "Draft Council of Europe Cyber Crime Convention Upsets Civil Rights Bodies", ***Computer Fraud and Security Issue***, 12, pp. 5-17.
- Wible, B. (2003), "A Site Where Hackers Are Welcome: Using Hack-In Contests to Shape Preferences and Deter Computer Crime" ***The Yale Law Journal***, 112(6), pp. 1573-1581.
- ***Wired Society*** (2002), The Nation, May 4.
- Yam, J. T. (2001), "Cyber crime Treaty Under Way", ***Business Word***, May 3, pp. 5-13.