



اصول حاکم سیاست جنایی تقنینی جرایم سایبری

احسان پهلوانی فردایوبمحمد عسگرخانی***مریم مرادی***ایرج گلدوزیان

تاریخ دریافت: ۱۳۹۷/۰۹/۱۲ تاریخ پذیرش: ۱۳۹۷/۱۱/۱۹

چکیده

سیاست کیفری جرایم در تمام جهان با توجه به ارزش ها، اعتقادات و آرمان های ملی و مذهبی با هم فرق دارد. جرایم سایبری با استفاده از تکنولوژی اینترنت و فضای مجازی روز به روز در حال دگرگونی مرزها و ارزش های ملی سرزمینی می باشد. جرم سایبری مرزهای سرزمینی را کنار گذاشته است با مرزهای بین المللی در ارتباط است لکن دولت های بین الملل برای جلوگیری از این جرم میبایستی یکسری اصول و قواعد بین المللی را اجرا نمایند در قانون جرایم رایانه ای ایران هم در ماده ۵۲ به ضرورت همکاری بین المللی توجه شده است. این ماده مقرر می دارد که به منظور ارتقای همکاری های بین المللی در زمینه جرائم رایانه ای، وزارت دادگستری موظف است با همکاری وزارت ارتباطات و فناوری اطلاعات اقدامات لازم را در زمینه تدوین لوایح و پیگیری امور مربوط جهت پیوستن ایران به اسناد بین المللی و منطقه ای و معاهدات راجع به همکاری و معاضدت دوجانبه یا چندجانبه قضایی انجام دهد. مع الوصف در این مقاله درصدد تبیین جایگاه دول بین الملل جهت جلوگیری و مجازات خاطین در فضای مجازی بر مبنای اصول و قواعد بین المللی میباشیم.

واژگان کلیدی: سیاست جنایی، جرایم سایبری، فراسرزمینی، فضای مجازی.

***گروه حقوق، دانشکده بین الملل، واحد قشم، دانشگاه آزاد اسلامی، قشم، ایران.

***استاد روابط بین الملل دانشگاه تهران نویسنده مسئول: abuata@semnan.ac.ir

***استادیار گروه حقوق، دانشکده بین الملل، واحد قشم، دانشگاه آزاد اسلامی، قشم، ایران.

***استاد حقوق کیفری و جرم شناسی دانشگاه تهران

مقدمه

بحث جرائم رایانه ای در ایران به اوایل دهه ۱۳۸۰ باز می‌گردد. جرم رایانه ای در آن زمان بیشتر به جعل اسناد دولتی و شخصی مربوط می‌شد. اولین جرم رایانه ای در ایران در خرداد ماه ۱۳۸۷ به ثبت رسیده است که در آن یک دانشجوی کامپیوتر و یک کارگر چاپخانه در کرمان چک های تضمینی را جعل کردند. جرائمی نظیر جعل بلیط های اتوبوس رانی، اوراق خرید و فروش خودرو و ... در این دوره به وفور ارتکاب یافت. پس از آن برخی وبلاگ نویسان به اتهامات مختلف نظیر نوشتن مطالب توهین به مقدسات، افشای اسناد دولتی و ... محاکمه شدند. دولت نیز با ایجاد فیلترینگ شدید در صدد مقابله با چنین جرائمی برآمد. گذشته از اینها برخی افراد بر سر مسائلی مانند برندهای شرکت ها، نام ها و ... با هم دچار اختلاف شدند. بنابراین با شروع دهه هشتاد و فراگیر شدن استفاده از کامپیوتر و رایانه میزان چنین جرائمی نیز به شدت افزایش یافت. (ایوانز و دیگران، ۱۳۰:۱۳۸۱) تصویب قوانین و مقررات کیفی لازم‌الاجراء امنیت و نهادن پایه های توسعه در هر جامعه ای است. یکی از ابعاد مهم توسعه نیز افزایش توان در زمینه فناوری اطلاعات است که رایانه رکن جدایی ناپذیر این موضوع شناخته می‌شود. بنابراین چنانکه گفته شد با افزایش جرائم رایانه ای قانونگذار به مانند فضای واقعی اجتماعی می‌بایست امنیت فضای مجازی و سایبری را نیز ایمن سازد. در این زمینه در سال های اخیر مجلس شورای اسلامی قانون حمایت از پدیدآورندگان نرم افزارهای رایانه ای را در سال ۱۳۷۹ به تصویب رسانید و آیین نامه اجرایی آن نیز در هفتاد ماده به تصویب هیات وزیران رسید. بعد از آن پیش نویس قانون جرایم رایانه ای ایران توسط کمیته مبارزه با جرایم رایانه ای قوه قضائیه تهیه شد و لایحه آن نیز توسط مجلس شورای اسلامی به تصویب رسید. پس از تصویب این قانون در سال ۱۳۸۲ مجلس شورای اسلامی قانون تجارت الکترونیک را به تصویب رسانید تا خلاهای موجود در تجارت الکترونیک را از بین ببرد. قانون بسیار مهم و مرتبط با پژوهش

حاضر به در سال ۱۳۸۸ تحت عنوان قانون جرائم رایانه ای به تصویب مجلس شورای اسلامی رسید. با توجه به قوانین به تصویب رسیده در دو دهه اخیر در کشورمان کاملاً مشخص است که این موضوع اهمیت خود را پیدا کرده است و قانونگذار به ضرورت وجود قوانین کافی در این زمینه پی برده است.

در متون و نوشته های مربوط به حقوق بین الملل و نیز در احکام صادره از مراجع بین المللی، پیوسته از اصول حقوق بین الملل یا قاعده حقوق بین المللی یاد میشود. این که کجا و چگونه میتوان تعریف و مفهوم این اصول یا قواعد و نیز به مبانی و منبع آنها به طور دسته بندی شده و جامع دست یافت، کارآسانی نیست بلکه محتاج استقصاء در متون و آراء مراجع بین المللی است. دشواری کار از آنجا است که حقوق بین الملل فاقد مرجع قانونگذاری است. اصولاً نیروهای سازنده حقوق بین الملل طیف وسیعی را تشکیل میدهد که از معاهدات و عرف شروع و به تصمیمات مراجع بین المللی ختم میگردد، از این رو بر خلاف آنکه در نظام های حقوق داخلی به سهولت میتوان به اصول و قواعد ثابت و از قبل تعریف شده هر نظام حقوقی، به عنوان یک سیستم یا دستگاه حقوقی، مشخص پی برد. در حقوق بین المللی به ویژه در حقوق بین المللی عرفی دستیابی و تدوین مجموعه اصول و قواعد آن به نحوی که یک دستگاه حقوق را تشکیل دهد، به آسانی ممکن نیست، خصوصاً که در معرفی و تعیین اصول و قواعد حقوق بین المللی، هنوز بین حقوقدانان بحث و گفتگو پایان نیافته و حتی ضابطه روشن و قطعی بدست نیامده یا لااقل مورد توافق قرار نگرفته تا به کمک آن بتوان گفت کدام مطلب جزو قواعد و اصول حقوق بین الملل است و کدام نیست. به عبارت دیگر هنوز در حقوق بین المللی جدال و بحث در تعیین و تدوین قواعد و احکام پایان نیافته است چه رسد به تشخیص و تعیین موضوعی قضایا. (باستانی، ۱۳۸۳: ۴۵)

در چنین شرایطی نمیتوان فهرست قابل اعتماد و مشخصی از مجموعه آنچه اصول حقوق بین المللی یا قواعد حقوق بین الملل نامیده شده است بدست داد، مگر این که به قدر متقنی موجود یا احیاناً اجماع علما و صاحب نظران حقوق بین الملل کفایت شود.

۲۳۴.....تحقیقات حقوقی تطبیقی ایران و بین‌الملل، سال یازدهم، شماره چهل و دوم، زمستان ۱۳۹۷

در این مجموعه اصول، دو اصل وجود دارد که در آن‌ها اختلافی نیست. این اصول عبارتند از اصل عدم مداخله و اصل منع توسل به زور. این اصول در حقوق بین‌الملل نقش بسیار مهمی دارند. این اصول در حوزه جرایم رایانه‌ای هم اعمال می‌گردند.

۱- اصل عدم مداخله در امور داخلی کشورها

اصل تساوی حاکمیت دولتها یکی از اصول پنجگانه همزیستی مسالمت آمیز است که با همت کشورهای جهان سوم در کنفرانس آسیای آفریقائی سال ۱۹۵۵ اندونزی مطرح شد و مورد تصویب کلیه اعضا قرار گرفت. متعاقباً کشورهای عضو جنبش عدم تعهد نیز در کنفرانس بندوک این اصل را به عنوان یکی از اصول مسلم حقوق بین‌الملل در اساسنامه سازمان و به عنوان پایه و اساس روابط دولتها با یکدیگر مورد تصویب قرار دادند.

بند اول از ماده ۲ منشور سازمان ملل متحد اصل تساوی حاکمیت دولت‌های عضو را تاکید نموده و وضع حقوقی تمامی دول عضو را به طور کلی در سازمان ملل متحد و ارکان‌های وابسته به این سازمان متساوی و متشابه با یکدیگر تعریف کرده است. قطعنامه‌های سازمان ملل نیز همواره از این اصل به عنوان یکی از اصول اساسی حقوق بین‌الملل یاد کرده و دولتها را موظف نموده است تا ضمن رعایت این اصل از دخالت در امور داخلی و یا اعمال زور بر علیه دیگر اعضا خودداری نمایند. در این خصوص منشور حقوق و وظایف دولتها در بخش اول خود بر اصل تساوی حاکمیت دولتها به عنوان اساسی‌ترین اصل در روابط دولتها تاکید کرده است. (پور قهرمان و همکاران، ۱۳۸۸: ۵۵)

یکی از پراوندهای اصل تساوی حاکمیت‌ها این است که هیچ دولتی نمی‌تواند در اموری که تحت صلاحیت داخلی دولت دیگر است دخالت کند. اصل عدم مداخله در امور داخلی کشورها محدود به سایر کشورها نیست بلکه سازمان‌های بین‌المللی هم تحت شمول این اصل قرار دارند.

مبنای حقوقی اصل عدم مداخله را میتوان در سند‌های بین‌المللی زیر یافت: منشور سازمان ملل متحد ۱۹۴۵، اعلامیه مجمع عمومی ملل متحد سال ۱۹۷۰ درباره اصول حقوق بین‌الملل در زمینه روابط دوستانه و همکاری میان دولتها مطابق منشور ملل متحد، اعلامیه اصول سند نهایی هلسنکی ۱۹۷۵، اعلامیه مجمع عمومی ملل متحد سال ۱۹۸۲ ترسایی درباره ناروایی مداخله در امور داخلی دولتها و حمایت از استقلال و حاکمیت آنها.

اصل عدم مداخله دولتها را مکلف میسازد که به امور هیچ دولت دیگری مداخله نکنند. یعنی، هیچ دولت و یا گروه از دولتها حق ندارند، به هر علتی که باشد، بطور مستقیم و یا غیر مستقیم، به امور داخلی و یا خارجی یک کشور دیگر مداخله کند. در نتیجه، مداخله نظامی و هرگونه مداخله دیگر، یا تهدید برضد شخصیت حقوقی یک دولت یا بر ضد بنیادهای سیاسی، اقتصادی و فرهنگی یک دولت، نقض حقوق بین‌الملل محسوب میشوند.

هیچ دولتی نمیتواند با به کارگیری تدبیرهای اقتصادی، سیاسی و غیره، یک دولت دیگر را ناگزیر بسازد تا اجرای حقوق حاکمیت آن را تابع خویش سازد و یا امتیازهای را از آن برای خویش محفوظ بدارد. همچنان، هیچ کشوری نباید، فعالیت‌های خرابکارانه، دهشت افگانه یا نظامی را که مقصد اش سرنگونی خشونت بار حکومت در کشور دیگر است، سازماندهی کند، یاری رساند، برانگیزاند، تمویل کند، تحریک نماید و یا آنرا تحمل کند؛ هیچ دولتی نباید به کشمکشهای داخلی کشور دیگر مداخله کند. توسل به زور برای سلب مردمان از هویت ملی ایشان، نقض حقوق جداناپذیر ایشان شمرده میشود و تخلف از اصل عدم مداخله است. هر کشور، بدون هرگونه مداخله از سوی کشور دیگری، حق جداناپذیر دارد تا نظام سیاسی، اقتصادی، اجتماعی و فرهنگی خویش را برگزیند. (جاویدنیا، ۱۳۸۸: ۱۴۰)

باید گفت که مداخله در امر داخلی یک کشور ارتباط راسته و مستقیم به مسأله صلح و امنیت بین‌المللی دارد. مداخله یک کشور در امور داخلی کشور همواره به زیان

۲۳۶.....تحقیقات حقوقی تطبیقی ایران و بین‌الملل، سال یازدهم، شماره چهل و دوم، زمستان ۱۳۹۷

صلح و امنیت بین‌المللی است. بنابراین «امور داخلی» را تنها با توجه به موازین بین‌المللی می‌توان سنجید. هر چه بر پیکره نظام حقوقی بین‌المللی افزوده شود، به همان نسبت نیز از اموری که اساساً ملی هستند کاسته خواهد شد. در حقیقت، اسنادی که در بالا به آنها اشاره شد، همگی قواعد دیگری دارند که مویذ این نگرش است. از جمله در اعلامیه ۲۱۳۱، ضمن آنکه به اهمیت حفظ صلح و نفی مداخله تأکید شده، با اعلام مقدماتی اینکه «در اعلامیه جهانی حقوق بشر، مجمع عمومی اعلام داشته که شناسایی شان ذاتی و حقوق برابر و تفویض ناپذیر همه اعضای خانواده بشری، بدون هر گونه تمایزی، مبنای آزادی، عدالت و صلح در جهان است»، در بند ششم اجرایی به «احترام مطلق برای حقوق بشر و آزادی‌های اساسی» تأکید کرده و دولت‌ها را مکلف دانسته در رفع انواع تبعیض نژادی و استعمار سهیم باشند.

در اعلامیه ۲۶۲۵ نیز، ضمن تأکید بر موازین حقوق بشر، تأکید شده که دولت‌ها باید تعهداتی را که مطابق منشور بر عهده گرفته‌اند، با حسن نیت ایفا کنند. این مساله که یکی دیگر از اصول حقوق بین‌الملل است، در منشور ملل متحد نیز به عنوان یکی از اصول مصرح در ماده دو ملاحظه می‌شود. این امر برای تشخیص حدود اموری که در صلاحیت داخلی دولت‌ها قرار دارند، با توجه به مقررات مسوولیت بین‌المللی دولت‌ها اهمیت زیادی دارد.

بر اساس نظام بین‌المللی مسوولیت دولت‌ها، هر عمل متخلفانه بین‌المللی موجب مسوولیت بین‌المللی دولت خواهد بود. عمل متخلفانه، فعل یا ترک فعلی است که از نظر حقوق بین‌الملل قابل انتساب به دولت بوده و متضمن نقض تعهدی بین‌المللی باشد. واضح است که تعهد بین‌المللی دولت را از منابع مختلفی می‌توان دریافت، از جمله اصول کلی حقوقی، عرف و معاهدات. به تعبیر دیگر، اگر دولتی به موجب هر یک از این منابع تعهدی حقوقی داشته باشد و آن را نقض کند، عمل متخلفانه‌ای مرتکب شده که می‌تواند مسوولیت بین‌المللی آن را مطرح کند. ولی نکته‌ای که باید به آن توجه داشت این است که برخی از قواعد حقوق بین‌الملل، ماهیتی آمره دارند و نه

تنها هیچ گونه تخلفی از آنها جایز نیست، بلکه هر دولتی می‌تواند اقداماتی به عمل آورد تا از استمرار نقض جلوگیری کند و جبرانی موثر برای قربانیان آن فراهم گردد. در حقیقت، بر اساس طرح کمیسیون حقوق بین‌الملل درباره مسوولیت بین‌المللی دولتها، نقض قواعد آمره دولتها را مکلف می‌کند برای خاتمه دادن به آن نقض با یکدیگر همکاری کنند و وضعیت حاصل از آن را نباید شناسایی کنند.

اگر به قواعد مندرج در اسناد بین‌المللی حقوق بشر توجه شود، ملاحظه می‌گردد که برخی از آنها در نظام حقوقی کیفری بین‌المللی نیز انعکاس یافته‌اند. برای مثال، با مراجعه به ماده هفت اساسنامه دیوان کیفری بین‌المللی ملاحظه می‌شود که قتل، شکنجه، ناپدید شدن اجباری، زنای به عنف، حبس بر خلاف قواعد بنیادین حقوق بین‌الملل، آپارتاید، آزار و اذیت گروهها که به دلایل قومی، سیاسی، مذهبی، ملی، فرهنگی یا جنسی صورت گیرد و سایر اعمال غیرانسانی که عمداً به منظور ایجاد درد و رنج شدید یا صدمه جدی به سلامت روحی یا جسمی انجام شوند، همگی از مصادیق جرایم علیه بشریت بوده و قواعدی آمره به حساب می‌آیند.

بنابراین، هیچ دولتی نمی‌تواند به ارتکاب چنین اعمالی مبادرت کرده و در مقابل اعتراض دولتهای دیگر مدعی دخالت در امور داخلی خود شود. همانگونه که هیچ کس در هیچ کشوری نمی‌تواند در منزل خود مرتکب قتل شود و به استناد اینکه در منزل خود چنین عملی مرتکب شده، آن را در زمره مسایل مربوط به حریم خصوصی خود بداند و از مراجع رسمی بخواهد واکنشی نشان ندهند. جامعه بین‌المللی نیز نسبت به نقض قواعد آمره طبیعتاً واکنش نشان داده و خواهان توقف آن خواهد شد. چنین واکنشی نه تنها مصداق مداخله در امور داخلی دولت خاطی نیست، بلکه نظام حقوقی بین‌المللی دولتها را مکلف می‌داند برای توقف چنین مواردی اقدام کرده و با سایر دولتها همکاری لازم را به عمل آورند.

مداخله عبارت از اجرای تدبیرهای نظامی، سیاسی، اقتصادی و غیره است که هدفش وادار کردن دولت دیگر برای حصول امتیازها از آن برای خویش باشد. مداخله میتواند

۲۳۸.....تحقیقات حقوقی تطبیقی ایران و بین‌الملل، سال یازدهم، شماره چهل و دوم، زمستان ۱۳۹۷

مستقیم یا غیر مستقیم باشد. مداخله مستقیم آن است که بصورت مستقیم از طرف یک دولت و یا ارگانهای آن اجرا می شود. مداخله نظامی و یا تهدید با زور از نوع مداخله مستقیم اند. همچنان اتخاذ تدابیر اقتصادی مانند محاصره اقتصادی، قطع روابط بازرگانی بمقیاس وسیع، انصراف از اجرای برنامه های بزرگ اقتصادی و فنی که هدف آن گرفتن امتیاز به نفع خویش است، مداخله مستقیم شمرده میشوند. مداخله غیر مستقیم آن اقدامها نظامی، سیاسی، اقتصادی و غیره اند که بوسیله خود دولت نه، بلکه بوسیله افراد و سازمانهای زیر نظارت آن انجام میگردد. سازماندهی، کمک و تشویق، تمویل و اجازه دهی فعالیتهای نظامی و جنگ روانی که به قصد تغییر نظام سیاسی دولت دیگر براه انداخته میشود، و یا برای واداشتن دولت دیگر برای کسب منافع صورت میگیرد، مداخله غیر مستقیم شمرده میشود. (جلالی فراهانی، ۱۳۸۹: ۵۹)

مداخله غیر مستقیم نیز با اصل عدم مداخله ناسازگار است. دادگاه بین‌المللی دادگستری در رای خویش در پرونده نیکارگوا علیه ایالات امریکا، کاملن روشن ساخت که حمایت ایالات متحده امریکا از فعالیتهای نظامی و شبه نظامی «کنتراس» در نیکارگوا، در آن وقت، که با تمویل، تمرین، آموزش و تامین اسلحه و تهیه اسرار و اطلاعات صورت میگرفت، تخطی آشکار از اصل عدم مداخله است.

بر اصل عدم مداخله در امور داخلی کشورها استثنائاتی چند وارد شده است که مهمترین آن ها این است که مسائل حقوق بشر است. بر طبق تئوری و عمل حقوق بشر بین‌المللی، مسائل حقوق بشر جزء مسائل تحت صلاحیت داخلی کشورها نیست.

دفاع از انسان و انسانیت، هدف اصلی و نهایی حقوق بشر دوستانه است؛ اصلی که کلی است و مورد قبول همه نظامهای حقوقی دنیاست. مداخله انسان دوستانه یا به صورت دقیق تر مداخله بشر دوستانه نیز در این راستا انجام می‌گیرد. به دنبال تصویب منشور ملل متحد و ظهور اصولی مانند اصل منع توسل به زور و اصل عدم مداخله در امور داخلی دیگر دول، مفهوم مداخله بشر دوستانه نیز متحول گردید. علاوه بر دولت‌ها، سازمان‌های بین‌المللی من جمله شورای امنیت سازمان ملل متحد نیز به

مداخله بشر دوستانه استناد نمودند. در دوره معاصر، علاوه بر حمایت از اتباع خودی، دولت‌ها توانستند با مبنا قرار دادن نقض گسترده حقوق بینادین و اساسی اتباع دولت دیگر، از اتباع غیر خودی نیز حمایت نمایند. در اینجا مسئله اصلی حمایت از افراد بشر به صورت کلی مطرح است، در واقع دولت‌ها، نمی‌توانند بصورت دلخواهی با شهروندان خود رفتار نمایند. به عبارت دیگر در چنین وضعیتی وجدان عمومی جامعه بشری خدشه‌دار می‌گردد و دخالت بشر دوستانه را موجب می‌شود. (حسن بیگی، ۲۳۲:۱۳۸۳)

در بررسی وضعیت و جایگاه مداخله بشر دوستانه در نظام حقوق بین‌الملل بایستی گفت در حال حاضر اجماع جهانی در مورد مشروعیت و یا عدم مشروعیت آن وجود ندارد. عده‌ای با استناد به حقوق توسل به زور آن را مشروع و قانونی می‌دانند اما در مقابل عده‌ای دیگر آن را با مبنا قرار دادن اصل منع توسل به زور و اصل عدم مداخله موجه نمی‌دانند. و تنها استثناء وارد بر دو اصل مذکور را دفاع مشروع (فردی و جمعی) و سیستم امنیت دسته جمعی می‌دانند.

در حال حاضر مداخله بشر دوستانه بیشتر توسط شورای امنیت انجام می‌شود تا توسط دولت‌ها؛ زیرا که شورای امنیت مسئولیت اولیه و اصلی حفظ صلح را بر عهده دارد. برخلاف مداخله بشر دوستانه‌ای که توسط دولت‌ها صورت می‌گیرد، اعمال این نوع مداخله توسط شورای امنیت با استقبال و پذیرش جامعه بین‌المللی روبرو شده است. لازم به ذکر است که شورای امنیت در توسل به مداخله بشر دوستانه از صلاحیت نامحدودی برخوردار نیست بلکه بایستی شرایطی مانند نقض وسیع و گسترده حقوق بشر (مانند نسل‌کشی و تبعیض نژادی)، انسان دوستانه بودن مداخله، رعایت اصل تناسب بین حملات نظامی و نقض گسترده حقوق بشر و احترام به استقلال و تمامیت عرضی دولت مداخله شونده محقق گردد.

در بحث از جایگاه اصل عدم مداخله در بحث از جرایم اینترنتی، تنها بحث از دخالت افراد خصوصی در اطلاعات دولتی یا خصوصی افراد نیست بلکه گاه دولت‌ها

۲۴۰.....تحقیقات حقوقی تطبیقی ایران و بین‌الملل، سال یازدهم، شماره چهل و دوم، زمستان ۱۳۹۷

هم به دخالت در این امور می‌پردازند. در این حال، اصل عدم مداخله مانع اعمال نفوذ دولت‌ها در امور سایبری سایر دول است بدان معنا که با استفاده از تکنولوژی‌های جدید هم دولت‌ها نباید در امور داخلی یکدیگر مداخله نمایند. (خداقلی، ۱۳۸۳: ۱۵۳)

در باب جرایم رایانه‌ای ارتكابی از سوی افراد هم دولت‌ها هستند که وظیفه پیگیری این جرایم را دارند. هنگامی که دولت‌ها از وجود یک گروه خرابکاری رایانه‌ای در سرزمینش مطلع باشد که علیه منافع دولت دیگر فعالیت می‌کنند، دولت اول موظف است که مانع اقدامات آن‌ها شود و آن‌ها را مجازات و یا در صورت وجود شرایط، مسترد نماید.

در باب شمول اصل عدم مداخله بر فضای مجازی، بحث دیگر بحث آزادی اطلاعات است. دولت‌ها نمی‌توانند مانع آزادی اطلاعات شده و به دلایل واهی از گردش آزادانه اطلاعات جلوگیری نمایند. به عبارت دیگر، هم مداخله مستقیم دولت و هم مداخله غیر مستقیم دولت در امور داخلی کشورهای دیگر با استفاده از یا مرتبط با ابزارهای تکنولوژیک ممنوع است.

اصل آزادی اطلاعات، شامل آزادی اطلاعات در فضای سایبر هم می‌گردد و از حقوق بشر تلقی می‌گردد. حال در صورتی که دولتی این حق را به رسمیت نشناسد و مانع آزادی اطلاعات در فضای مجازی گردد، سایر دولت‌ها می‌توانند با توسل به مداخله برای اعمال حقوق بشر یعنی مداخله بشر دوستانه علیه آن دولت وارد عمل گردند. البته ایراد این استدلال در آن جاست که کلیت اصل مداخله بشر دوستانه مشکلی ندارد اما حوزه اعمال آن محدود به خطرات جانی است و دشوار می‌توان آزادی اطلاعات را هم مشمول حقوقی قرار داد که مداخله سایر دولت‌ها را توجیه نماید. (خرم‌آبادی، ۱۳۸۴: ۷۳)

۲- اصل منع توسل به زور

این اصل از اصول هفت‌گانه ماده ۲ و یکی از اصول مندرج در منشور ملل متحد می‌باشد. اصل عدم توسل به زور به عنوان یک اصل قابل بررسی جداگانه است که ارزش و اعتبار خود را از یک ارزش متعالی یعنی بشریت می‌گیرد. منطق‌های سه‌گانه حاکم بر حقوق بین‌الملل یعنی منطق رابطه قدرت، همکاری و برابری، حقوق بین‌الملل را تحت تاثیر خود قرار می‌دهد و این اصل نیز تحت تاثیر منطق رابطه قدرت و نفوذ و تاثیر گسترده آن بر حقوق بین‌الملل مورد توجه واضعین منشور ملل متحد قرار گرفته است.

در صحنه بین‌المللی چون مطابق منشور ملل متحد و حقوق بین‌الملل تمام دولت‌ها چه بزرگ و چه کوچک باهم برابرند و حق حاکمیت برابر دارند و هیچ قدرتی مافوق حاکمیت دولتی وجود ندارد. عملاً یگانه قدرتی که می‌تواند از زور استفاده کند بازهم دولت است. اما دولت‌ها آزادی‌ای را که برای اجرای قانون در داخل مملکت دارند، در صحنه بین‌المللی نمیتوانند داشته باشند. یعنی اینکه هیچ دولتی هرچند نیرومند و توانا باشد قانوناً نمی‌تواند در روابط بین‌المللی به اعمال زور توسل جوید. حدود و ثغور استفاده از زور در حقوق بین‌الملل کاملاً مشخص است. (ذاکریان، ۱۳۸۳: ۶۳)

بسیاری از حقوق دانان بین‌المللی حتا در سده‌های ۱۶ و ۱۷ به فکر محدود کردن جنگ بودند. آنان برآن بودند که جنگ فقط در صورت دفاع از خود و یا در صورت آخرین وسیله برای احقاق حق می‌تواند مورد استفاده قرار گیرد. ولی دولت‌ها که در آن وقت در پی استعمار و تسخیر منابع سرزمین‌های بیگانه و انباشتن درآمد‌های هنگفت بودند این عقیده را هرگز قبول نکردند: آنان جنگ کردن را حق طبیعی خود می‌دانستند. البته این روش به وضوح با حقوق بین‌الملل ناسازگار است. باید گفت که اندیشمندان و مشاهیر ما نیز در سده‌های گذشته جنگ را عمل شنیع، بد توصیف و آن را با خصایل انسانی و نیک‌خواهی بشر ناسازگار دانسته‌اند.

۲۴۲.....تحقیقات حقوقی تطبیقی ایران و بین‌الملل، سال یازدهم، شماره چهل و دوم، زمستان ۱۳۹۷

پیمان پاریس سال ۱۹۲۸ م اولین سند رسمی است که در آن جنگ همچون ابزار اجرای سیاست ملی مردود شمرده شده است. در ماده دوم این پیمان تاکید شده است که طرفها رسماً می‌پذیرند که اختلافهای خویش را فقط از طرق و وسیله‌های مسالمت آمیز حل و فصل کنند. (Electronic, ۲۰۰۶: ۱۰۷) اصل عدم توسل به زور امروزه و رای ارزشی که در منشور ملل متحد دارد، اصلی اساسی در حقوق بین‌الملل عرفی است و بدین لحاظ برای همه دولتهای عضو جامعه بین‌المللی لازم الاجرا است. بند ۴ ماده ۲ به جای اشاره به «عدم توسل به جنگ» از اصطلاح «عدم توسل به زور» استفاده نموده است که به دنبال گسترش این ممنوعیت به سایر وضعیتهایی که از لحاظ شرایط فنی، حالت جنگ را ندارد بوده است.

اصل عدم توسل به زور دارای ابهاماتی است؛ یک نکته این که این اصل فقط به ممنوعیت اعمال زور در روابط بین‌المللی پرداخته است و توسل به زور در صحنه داخلی مثل استفاده از زور از سوی یک دولت علیه نیروهای شورشی در جنگهای داخلی را مد نظر قرار نداده است و دست دولتها را در این رابطه باز گذاشته است. شاید، پاسخ این باشد که منشور ملل متحد در سال ۱۹۴۵ به دنبال رهایی بشریت از آتش دو جنگ خانمان سوز بوده است، در حالی که بشریت در صحنه داخلی نیز نمود پیدا می‌کند و نکته دیگر راجع به این اصل این است که آیا عدم توسل به زور و یا کلمه «زور» به کار رفته در بند ۴ ماده ۲ منشور ملل متحد صرفاً شامل اعمال مسلحانه زور می‌باشد یا اشکال دیگر استفاده از زور مثل اعمال زور اقتصادی، سیاسی را نیز در بر می‌گیرد، با توجه به ظاهر کلام منشور ملل متحد از آنجا که منشور به «ضرورت» تضمین آن که «زور مسلح» باید در جهت نفع مشترک به کار رود اشاره می‌کند. این امر موجب شده است که کلمه زور در بند ۴ ماده ۲ را به معنای «زور مسلحانه» تلقی نمایند، همچنین ماده ۵۱ که به دفاع مشروع می‌پردازد این حالت را در برابر استفاده از زور مسلحانه بکار برده است. (راسخی، ۱۳۹۰: ۲۸)

دولت های عضو ملل متحد نباید در روابط خویش با همدیگر از زور یا تهدید به زور کار بگیرند. کاربرد زور یا تهدید به آن، قبل از همه بمعنای استفاده از زور نظامی و براه انداختن جنگ تجاوزکارانه است. تجاوز علیه دولت دیگر به ذات خود عمل غیر قانونی بوده و مطابق حقوق بین الملل جنایت علیه صلح به حساب می آید.

تجاوز طوریکه در اسناد بین المللی تعریف شده است، عبارت است از توسل به زور یا استفاده از نیروهای مسلح از طرف یک دولت برضد حاکمیت ملی، تمامیت ارضی و استقلال سیاسی دولت دیگر. البته منظور از کلمه زور در اصل فوق نیروهای مسلح و استفاده از قوت های نظامی و اجرای عملیات جنگی به مقیاس وسیع است که حاکمیت ملی و تمامیت ارضی کشور دیگر را به مخاطره می اندازد. بناء برخورد های کوچک مرزی را نمی توان حمله مسلحانه نام گذاشت. اشغال کشور دیگر به هر نام و عنوان که باشد ناجایز است و یکی از خشن ترین اشکال تجاوز به حساب می آید. زیرا در این صورت کشور دیگر نه تنها از حاکمیت ملی و استقلال سیاسی اش محروم می شود بلکه تمامیت ارضی آن نیز به زیر سوال قرار میگیرد. (زیبر، ۱۳۹۰: ۹۷)

۳- قواعد حاکم در بعد بین المللی

حقوق داخلی مبتنی بر ضرورت های جامعه شناختی داخلی کشورها است. حقوق بین الملل هم مبتنی بر ضرورت های زیست بین المللی کشورها است به عبارت دیگر، مبنای حقوق داخلی جامعه شناسی داخلی است و مبنای حقوق بین الملل هم جامعه شناسی بین المللی. تصویب قانون در هر یک از این نظام های حقوقی هنگامی ضرورت پیدا می کند که نشانه های جامعه شناختی و فرهنگی برای تصویب آن قانون وجود داشته باشد. (Electronic, ۲۰۱۱: ۷۶)

از این منظر، جرم انگاری جرایم سایبری در نظام حقوقی داخلی و مبتنی بر ضرورت های زیست جمعی بشر احساس شده فلذا کشورها در حوزه صلاحیت خود اقدام به تصویب قوانینی در این زمینه کردند. همین ضرورت در عرصه زیست بین

۲۴۴.....تحقیقات حقوقی تطبیقی ایران و بین‌الملل، سال یازدهم، شماره چهل و دوم، زمستان ۱۳۹۷

المللی هم تشخیص داده شد فلذا در حوزه حقوق بین‌الملل هم قوانینی در این باره روی کار آمدند که این ضرورت را پاسخگو باشند.

آن چه که خاصه در این حوزه برای جرایم بین‌المللی حائز اهمیت است، نحوه تعیین دولت صالح برای رسیدگی به این جرایم است. از سوی دیگر، بحث همکاری دولت‌ها برای مقابله با این دسته جرایم هم شایان توجه است که ذیل عنوان معاضدت قضایی بحث می‌گردد. (زینالی، ۱۳۸۸: ۸۹)

۴- صلاحیت کیفری در حقوق بین‌الملل

صلاحیت به قدرت دولت بر اشخاص، اموال و امور اشاره دارد این قدرت ممکن است جنبه قانون‌گذاری بر افراد اموال و امور داشته باشد و یا جنبه اجرایی، مانند توقیف اشخاص و اموال یا رسیدگی به دعاوی توسط محاکم باید بین اعمال قدرت اجرایی و اعمال قدرت قضایی (صلاحیت محاکم) تفکیک قایل شد زیرا اگر در کشوری جرمی اتفاق بیفتد، بنابر اصل سرزمینی بودن جرم، دادگاه کشور مربوط صالح برای رسیدگی به آن جرم است ولی پلیس آن کشور نمی‌تواند مثلاً وارد خاک کشور همسایه شده مجرم را دستگیر و برای محاکمه به کشور خود بیاورد، بلکه در این مورد باید از مقامات کشور همسایه تقاضای استرداد متهم را بنماید. (سالاری، ۱۳۸۹: ۹۱)

از منظر معیارهای صلاحیت قانونی دولت لازم به ذکر است که در حال حاضر معیارهای صلاحیت سرزمینی، صلاحیت شخصی، صلاحیت واقعی و صلاحیت جهانی به طور سنتی مورد پذیرش جامعه بین‌المللی قرار گرفته است. سایر دکترین‌های نوین مانند صلاحیت مبتنی بر دکترین اثرگذاری (Effect doctrine) و دکترین اجرا نیز با موافقین و مخالفینی مواجه است.

۵-۱ صلاحیت سرزمینی یا درون مرزی

این اصل مهمترین و قدیمی ترین اصل در تعیین صلاحیت کیفری است و با اصل حاکمیت دولتها هم همخوانی دارد. به موجب این اصل صلاحیت دولت برای رسیدگی به جرم با توجه به محل ارتکاب تمام یا بخشی از آن جرم تعیین می گردد. این اصل مورد تاکید دیوان دائمی دادگستری بین المللی در دعوی لوترس قرار گرفته، که آن را در همه نظامهای حقوقی از اهمیت اساسی برخوردار دانسته است.

از جمله فوایدی که برای پذیرش این اصل، که با ظهور دول بزرگ تحول یافته است، ارائه می شود آن است که با پذیرش این اصل بررسی دلایل، امارات و قرائن موود در مورد هر جرم با سهولت بیشتری انجام می گیرد.

بسیاری کشورها از جمله ایران نظریه سرزمینی صلاحیت کیفری را پذیرفته اند. کشور محل وقوع جرم بیش از هر کشور دیگری برای رسیدگی به جرم صلاحیت دارد، نه تنها از حیث اینکه نظم اجتماعی او مختل شده بلکه از حیث جمع آوری ادله و مبارزه با جرم، اعم از اینکه جرم به وسیله اتباع داخلی یا بیگانگان ساکن یا مقیم در کشور ارتکاب شده باشد. به علاوه ماده مزبور طبق اصل گسترش صلاحیت سرزمینی یا صلاحیت برون مرزی برخی جرایم مانند اقدام علیه امنیت و تمامیت ارضی کشور، جعل اسکناس و اوراق بهادار، جعل فرامین و دستخط مقامات رسمی را که در خارج از قلمرو حاکمیت ایران توسط اتباع ایران یا اتباع بیگانه ارتکاب شده باشد، جرم واقع شده در ایران» محسوب دانسته است.

همچنین ماموران دولت در خارج، که دارای مصونیت سیاسی هستند، چنانچه مرتکب جرم شوند مشمول صلاحیت دولت ایران خواهند بود. و نیز طبق بنده ماده ۳ قانون راجع به مجازات اسلامی کسانی که به موجب قوانین خاص یا عهود بین المللی هر کجا یافت شوند قابل محاکمه می باشند، اگر در ایران دستگیر شوند طبق قوانین جمهوری اسلامی ایران، محاکمه و مجازات می شوند. (شاهبندرزاده و دیگران، ۱۳۹۱

۲۴۶.....تحقیقات حقوقی تطبیقی ایران و بین‌الملل، سال یازدهم، شماره چهل و دوم، زمستان ۱۳۹۷

نکته ای که در این باب مطرح است این است که مفهوم فضای سایبر سرزمین ندارد که بتوان با استفاده از این اصل به تنهایی تمام جرایم این حوزه را پوشش داد. در بحث از مرزهای سایبری دیدیم که این فضا نه مکان دارد و نه زمان یعنی مفاهیم مانی و زمانی شناخته شده، در فضای سایبر مفهوم خود را تا حد زیادی از دست داده اند. با توجه به این مسائل اعمال اصل صلاحیت سرزمینی به تنهایی قادر به حل مشکلات موجود در این زمینه نیست و باید به سایر مبانی صلاحیت هم هم‌زمان توجه نمود.

برای اعمال اصل صلاحیت سرزمینی بر جرایم سایبری و رایانه ای هم می‌توان مبانی خاصی پیدا کرد. در هر حال، برای ارتکاب یک جرم رایانه ای، مرتکب باید در یک کشور مستقر باشد. اگر در اعمال صلاحیت سرزمینی بر این جرایم باید به وجود چنین مشکلی هم توجه کرد چه همانگونه که گفته شد، به علت مدرن بودن این جرم، پیدا کردن مرتکب کار بسیار دشواری است ولی به هر حال این شخص تحت قلمرو حاکمیتی یک کشور قرار دارد لذا کشور مذکور برای رسیدگی به این جرم صلاحیت خواهد داشت. (شریفی، ۱۳۷۹:۴۳)

نکته ای که در این باب قابل توجه است این است که تمام ارتباطات سایبری از طریق یک واسط انجام می‌گیرد. به عنوان مثال ارسال یک نامه الکترونیکی، احتیاج به استفاده از سرور دارد که این سرور ممکن است در هر کجای این کره خاکی مستقر باشد. حال در چنین حالتی باید کدام کشور را صالح به رسیدگی دانست؟ استفاده مجرمانه از واسط‌هایی که ماهیت مجرمانه ندارند، علی‌الاصول نباید باعث مجرم دانستن واسط گردد اما در حالتی که هدف از واسط قرار گرفتن در این ارتباطات صرفاً ارتکاب جرم باشد می‌توان با استفاده از صلاحیت سرزمینی، کشور محل استقرار سرور را برای رسیدگی به جرایم واسط، و کشور محل استقرار مباشر را صالح به رسیدگی به جرایم مباشر دانست. (Convention, ۲۰۱۱:۶۹)

۵-۱۲ اصل صلاحیت شخصی

صلاحیت شخصی مربوط به وجود خصوصیت و کیفیتی است در شخصی که موضوع صلاحیت قرار می گیرد، مانند رابطه تابعیت. بنابراین دولتی که تبعه خود را تحت تعقیب قرار می دهد صلاحیت شخصی خود را بکار برده است. اصل صلاحیت شخصی بر دو نوع است؛ اصل صلاحیت شخصی فعال و اصل صلاحیت شخصی منفعل. اصل نوع اول با اصلی که در حقوق استرداد وجود دارد، ارتباط دارد که به موجب آن هیچ دولتی ملزم نیست تبعه خود را برای جرمی که در خارج مرتکب شده است به دولت دیگر تسلیم کند.

صلاحیت شخصی جنبه دیگری نیز دارد و آن موردی است که تبعه دولت در خارج مورد صدمه و زیان قرار گرفته باشد و دولت سرزمینی از تعقیب و مجازات متخلف خودداری نماید. در این صورت هنگامی که متخلف در اختیار دولت متبوع فرد متضرر قرار گرفت، قابل تعقیب و مجازات می باشد. مبنای این اصل عبارت از حق هر دولت است که از اتباع خود حمایت کند و چنانچه متخلف در اختیار او قرار گرفت نسبت به محاکمه و مجازات او اقدام کند.

به نسبت صلاحیت سرزمینی، اعمال این نوع صلاحیت راه کار بهتری برای مقابله با بی کیفی مجرمان سایبری ارائه می دهد چرا که در این حالت بالاخره رسیدگی به جرم در صلاحیت یکی از کشورها قرار خواهد گرفت. فقط تنها مشکلی که ممکن است پیش آید بحث تداخل صلاحیت ها است. اگر جرم رایاه ای علیه فردی اتفاق بیفتد و همزمان هم کشور متبوع مجرم (اصل صلاحیت شخصی فعال) و هم کشور متبوع بزه دیده (اصل صلاحیت شخصی منفعل) ادعای صلاحیت برای رسیدگی به جرم مذکور را نمایند، در واقع تعارض صلاحیت ها پیش آمده است که راه کار حقوقی مشخصی هم برای آن در بین نیست. (شیرزاد، ۱۳۸۸: ۸۴)

۵-۱۳ اصل صلاحیت حمایتی

هر دولتی حق دارد نسبت به جرایمی که علیه امنیت و استقلال و منافع حیاتی اقتصادی صورت می‌گیرد، اعمال صلاحیت کند. این اصل که به اصل صلاحیت حمایتی معروف است در غالب قوانین جزایی کشورهای از جمله ایران، موجود است. توجیه اینگونه صلاحیت، شدت مخاطره و صدمه‌ای است که متوجه امنیت و منافع یک کشور می‌شود به علاوه از آن جا که متخلف، مرتکب نقض مقررات کشور محل ارتکاب جرم نشده است ممکن است از مجازات بگریزد یا به علل سیاسی از استرداد وی خودداری شود، البته اشکال این نوع صلاحیت آن است که هر کشوری ممکن است خطرات و صدمات را طبق سلیقه خود تفسیر و قضاوت کند. (Eric, ۲۰۱۳: ۱۰۳)

در تروریسم سایبری یا هنگام نقض اصل عدم مداخله با بهره‌گیری از ابزارهای رایانه‌ای، اعمال این اصل می‌تواند راه کار خوبی هم برای دفاع باشد و هم برای مقابله با بی‌کیفری.

صلاحیت حمایتی در واقع یکی از استثنای مجاز عدم اعمال فرا سرزمینی صلاحیت است که به موجب آن اصل بر صلاحیت سرزمینی است. این اصل در حوزه جرایم رایانه‌ای احتمال بیشتری کاربرد را داشته باشد چرا که طبعاً این کشور زیان‌دیده است که ابداناً در صدد تعقیب مجرمان بر خواهد آمد.

۵-۱۴ اصل صلاحیت جهانی

جرمی که تابع صلاحیت عام یا جهانی است جرمی است که تحت صلاحیت همه دولت‌ها قطع نظر از محل ارتکاب آن قرار می‌گیرد چون اینگونه جرایم علیه جامعه بین‌المللی تلقی می‌شود، همه دولت‌ها حق تعقیب و مجازات متخلف را دارند هدف صلاحیت عام یا جهانی آن است که اینگونه جرایم بدون مجازات نمانند و از جمله موارد مسلم جرایم جهانی دو مورد زیر است: دزدی دریایی و جرائم جنگی.

جرایم دیگری مانند خرید و فروش مواد مخدر، تجارت زنان و کودکان و جعل اسکناس، موضوع کنوانسیون های دیگر بین المللی قرار گرفته است. طبق این کنوانسیون ها، متخلفین یا توسط دولتی که در قلمرو آنها یافت می شوند مجازات شده یا تسلیم دولتی می گردند که صالح و علاقمند برای اعمال صلاحیت است یک نمونه دیگر ماده ۸ کنوانسیون بین المللی علیه گروگان گیری می باشد که توسط مجمع عمومی در ۱۷ دسامبر ۱۹۷۹ به تصویب رسید. همین معنی در مورد جرم کشتار جمعی نیز صادق است. (Simplified, ۲۰۱۵: ۸۳)

بعید به نظر می رسد که دزدی دریایی و جرایم جنگی قابلیت ارتکاب از طریق رایانه را داشته باشند اما جعل و تجارت کودکان یا تجارت مواد مخدر ممکن است با استفاده از واسطه های الکترونیکی صورت گیرد. برای جرایم رایانه ای تاکنون صلاحیت جهانی پیش بینی نشده است بدان معنا که هیچ یک از جرایم رایانه ای به سان دزدی دریایی تحت صلاحیت همه کشورها قرار نگرفته است. (عالی پور، ۱۳۹۰: ۶۹)

۶. آیین دادرسی و معاضدت قضایی بین المللی

آیین دادرسی، پلی است برای رساندن مجرم به سزای اعمال مجرمانه اش. این پل باید مستحکم باشد. اصول آیین دادرسی کیفری همچون محاکمه عادلانه و حق دفاع در حال حاضر جزء حقوق اساسی بشر قرار گرفته اند.

مسئله تحقیق جرایم جرایمانه ای مشکلات خاص خود را دارد. این مشکلات ناشی از طبع خاص فضای مجازی است. برای پیگیری این جرایم و تحقیق در باره آن ها سطح خاصی از تخصص مورد احتیاج است همانگونه که برای ارتکاب آن ها هم به تخصص احتیاج است.

کمیسیون اروپا راه کارهایی برای تحقق تخصص در امر تعقیب جرایم رایانه ای پیش بینی کرده است که شامل آموزش هایی برای پلیس ها می گردد.

۲۵۰.....تحقیقات حقوقی تطبیقی ایران و بین‌الملل، سال یازدهم، شماره چهل و دوم، زمستان ۱۳۹۷

همانگونه که در بحث صلاحیت مطرح شد، هر جا مراکز تولید کننده بسترهای الکترونیکی قرار داشته باشند که اصطلاحاً به آن‌ها مراکز داده اینترنتی گفته می‌شود از لحاظ فنی به ارائه خدمات میزبانی و ملزومات تبعی آن می‌پردازند، جزء قلمرو حاکمیت آن کشور به شمار می‌روند و تحت صلاحیت سرزمینی قرار می‌گیرند که این کشور توانایی بیشتری برای تحقیق و پیگرد این جرایم دارد چرا که دسترسی بیشتری به مرتکب و ابزارهای او دارد.

هنگامی که بر مبنای یکی از معیارهای تعیین صلاحیت که در بالا بیان شد، کشور صالح به رسیدگی تعیین شد، طبعاً آیین دادرسی همان کشور هم برای رسیدگی به این جرایم به کار خواهد رفت اما به رغم لزوم تصمیم‌گیری و حل و فصل مسائل جهانی راجع به صلاحیت در حوزه جرایم سایبری، تا کنون هیچ اقدام عملی و لازم‌اجرائی در عرصه بین‌المللی صورت نگرفته است. نمونه بارز آن کنوانسیون اروپایی جرایم سایبر است که به واقع بی‌تاثیرترین ضوابط آن را به مقررات راجع به صلاحیت کیفری به خود اختصاص داده است.

به منظور تشخیص کشور صالح به رسیدگی در جرایم سایبر و اعمال یکی از اصول صلاحیت که در بالا توضیح داده شد باید به طبع این جرایم و نحوه ارتکاب آن‌ها توجه نمود. در خصوص کشورهایی که مبادرت به تصویب قوانین جدید کرده‌اند می‌توان تبعیت از دو رویه کلی را ملاحظه نمود: اول، محل استقرار سامانه‌های رایانه‌ای و دوم، محل حضور بارگذار و پیاده‌ساز شبکه‌ای در بحث از محل استقرار سامانه‌های رایانه‌ای به عنوان محل ارتکاب جرایم سایبری منظور از سامانه رایانه‌ای تنها رایانه‌های شخصی نیستند، هرچند نمونه بارز آن به شمار می‌آیند اما باید مفهوم موسع آن را مورد توجه قرار داد. (peter, ۲۰۱۳: ۶۵)

اما در اعمال رویه دوم یعنی محل حضور بارگذار و پیاده‌ساز شبکه‌ای برای اعمال صلاحیت باید دانست که به طور کلی کنش‌گران اصلی فضای سایبر از دو حالت کلی خارج نیستند. بدین صورت که یا داده‌ها را در قالب فایل‌های مختلف با پسوند‌های

متفاوت در آن می گنجانند که در این صورت به آن ها بار گذار می گویند و یا این که داده ها را از این فضا دریافت می کنند که به آن ها پیاده ساز می گویند. در این جا بار گذار، اطلاعات مورد نظر خود را در فضای تخصیص یافته از سوی ارائه کننده خدمات میزبانی قرار می دهد تا متعاقباً پیاده ساز به آن ها دسترسی یابد. هیچ نیازی نیست که آن ها از هویت یکدیگر آگاهی داشته باشند. بنابراین نباید آن ها را با فرستنده و گیرنده که معمولاً هویت آن ها در ارتباطات الکترونیکی معلوم است، اشتباه گرفت. زیرا در این جا آن هدف خاص از مبادله اطلاعات که در ارتباطات طرفینی وجود دارد مشاهده نمی شود. حال هر کشوری که قصد اعمال صلاحیت سرزمینی بر این نوع از جرایم را دارد باید به این مسائل توجه خاص مبذول بدارد. هنگامی که بحث تعارض صلاحیت ها پیش می آید، برای حل مساله باید صلاحیت غیر مبتنی بر مرز یا صلاحیت فرا مرزی جانشین صلاحیت های مبتنی بر حیطه بندی های جغرافیایی، سیاسی و طبیعی شود. پس برخی پیشنهاد می کنند که ملاک تعیین مرجع قضایی صالح، فقط عبور از قواعد سنتی و در نظر گرفتن موقعیت بزه دیده است. یعنی چنانچه بزه دیده های جرایم سایبری به دادسرای محل وقوع جرم اقامت خود شکایت کنند آن دادسرا باید با پذیرش شکایت، اقدام به تعقیب و رسیدگی قضایی کند. زیرا تنها محلی که می توان تحقیقات مقدماتی را از آن جا آغاز کرد و امکان جمع آوری آثار جرم در آن جا وجود دارد محلی است که در آن اقامت داشته دست کم نمایی از ارتکاب جرم سایبری علیه داده ها یا سامانه های او رویت پذیر است. (Susan, ۲۰۱۲: ۳۴)

در هر حال، کشور صالح به رسیدگی باید حداقل موازین رسیدگی های کیفری را که در اسناد بین المللی مقرر شده رعایت نماید. در باب رسیدگی به جرایم و رسیدگی های کیفری به طور کلی، معیارهای حقوق بشری خاصی وجود دارد که باید در رسیدگی به جرایم رایانه ای هم مورد توجه قرار گیرد.

شروع به جرم نیز در فضای سایبر رنگ و بوی جدیدی به خود می گیرد و نمی توان به طور اطلاق قوانین سنتی را در فضای سایبر مجرا ساخت. مثلاً شخصی با ارسال

۲۵۲.....تحقیقات حقوقی تطبیقی ایران و بین‌الملل، سال یازدهم، شماره چهل و دوم، زمستان ۱۳۹۷

نامه‌های الکترونیکی به اشخاص متعدد بیان دارد که طالب قتل شخص معینی است و کسی که پیشنهاد وی را بپذیرد با فشار دادن دکمه مخصوص، قبول این پیشنهاد را اعلام دارد تا مقدماً یک میلیون تومان به حسابش واریز شود؛ آیا می‌توان گفت این عمل، شروع به جرم قتل است و مستحق پیگرد و مجازات؟ آیا فشار دادن یک دکمه مخصوص در حکم دست دادن با شخصی است که برای قتل یک نفر پول می‌پردازد؟ همینطور است در مورد پیشنهاد رابطه جنسی با کودکان از طریق اینترنت و قرار ملاقات گذاشتن با آنها. آیا چنین ملاقاتی قبل از وقوعه در حکم شروع به جرمی است که تحت عنوان «ممنوعیت ارتباط جنسی با کودکان» آمده است. تمام این مسائل حاکی از آن است که سیاست کیفری، چه در زمینه جرم انگاری در فضای سایبر و چه در زمینه آیین دادرسی آن رویه‌های جدیدی در پیش گرفته و جامعه بین‌المللی به صورت صحیح و یکسان با آن برخورد نمایند. (فریرزی، ۱۳۹۰: ۷۹)

ضرورت همکاری بین‌المللی برای برخورد با جرایم رایانه‌ای مسئله‌ای نیست که قابل انکار باشد. مشکلی که در این قضیه پیش خواهد آمد، تعدد بزه‌دیدگان و در نتیجه تعدد مراجع قضایی صالح است. مثلاً انتشار ویروس‌های مخرب رایانه‌ای که هزاران کاربر را در سطح یک کشور یا جهان بزه‌دیده می‌کند. بهترین و کارآمد تری راه حل، تقویت همکاری بین‌المللی یا همان تعاون و معاضدت قضایی است. بدین صورت که یک نقطه تماس بین‌المللی که به طور ۲۴ ساعته و به شکل آنلاین آماده دریافت، پیگیری و ارائه گزارش‌های مربوط به به همکاری کشورها در مبارزه با جرایم سایبری باشد. هم در کنوانسیون جرایم سایبر و هم در قانون ایران راه‌کارهایی برای تقویت معاضدت بین‌المللی پیش‌بینی شده است.

کنوانسیون جرایم سایبر در این زمینه یک فصل کامل را به خود اختصاص داده است. در این فصل از کنوانسیون درباره اصول حاکم بر همکاری دو و چند جانبه دولت‌ها و قواعد استرداد مجرمان و معاضدت قضایی بحث شده است. ماده ۲۳ کنوانسیون با عنوان اصول کلی مربوط به همکاری بین‌المللی مقرر می‌دارد که اعضای کنوانسیون

باید براساس مقررات این فصل و از طریق اعمال ابزارهای بین‌المللی مربوط به همکاری بین‌المللی در زمینه مسائل کیفری، تمهیدات مورد توافق بر پایه قانونگذاری یکنواخت یا متقابل و حقوق داخلی، برای رسیدن به وسیع‌ترین محدوده ممکن به منظور پی‌جویی‌ها یا رسیدگی‌های قضایی راجع به جرایم مرتبط با سیستم رایانه‌ای و داده‌ها یا جمع‌آوری دلایل الکترونیکی در جرایم با همدیگر همکاری کنند.

در قانون جرایم رایانه‌ای ایران هم در ماده ۵۲ به ضرورت همکاری بین‌المللی توجه شده است. این ماده مقرر می‌دارد که به منظور ارتقای همکاری‌های بین‌المللی در زمینه جرائم رایانه‌ای، وزارت دادگستری موظف است با همکاری وزارت ارتباطات و فناوری اطلاعات اقدامات لازم را در زمینه تدوین لوایح و پیگیری امور مربوط جهت پیوستن ایران به اسناد بین‌المللی و منطقه‌ای و معاهدات راجع به همکاری و معاضدت دوجانبه یا چندجانبه قضایی انجام دهد. جرائم رایانه‌ای در بردارنده طیف گسترده‌ای از جرائم هستند که با پیشرفت در زمینه به کارگیری اینترنت گسترده تر هم شده است و در واقع می‌توان گفت دچار تحول در محتوا شده است. چنین جرائمی از سرقت اطلاعات، کلاهبرداری، توهین و افترا و ... گرفته تا استفاده غیر مجاز از نشان‌ها و علائم تجاری را در بر می‌گیرد. (Association, ۲۰۱۳: ۵۶)

از سوی تاریخچه جرائم رایانه‌ای را می‌توان به سه نسل طبقه‌بندی نمود. نسل اول که تا اواخر دهه ۱۹۸۰ می‌باشد شامل سرقت و کپی برداری از برنامه‌ها و جرائم علیه حریم خصوصی اشخاص مانند سرقت از آثار و تحقیقات افراد بود. نسل دوم که تحت عنوان جرائم داده‌ها نامیده می‌شود تا اواخر دهه ۱۹۹۰ ادامه داشته است. در این دهه تمامی جرائم علیه تکنولوژی اطلاعاتی، ارتباطاتی، کامپیوتری، ماهواره‌ای و شبکه‌های بین‌المللی تحت عنوان جرائم علیه داده‌ها اطلاق می‌شود. نسل سوم که از اواسط دهه ۱۹۹۰ شروع می‌شود جرائم کامپیوتری تحت عنوان جرائم سایبر یا جرائم در محیط سایبر معروف گردید. پیشینه تاریخی جرائم کامپیوتری به سال ۱۹۸۵ بر می‌گردد که

۲۵۴.....تحقیقات حقوقی تطبیقی ایران و بین‌الملل، سال یازدهم، شماره چهل و دوم، زمستان ۱۳۹۷

جرایم کامپیوتری در بر گیرنده جرائمی مانند جاسوسی کامپیوتری، سرقت های آثار ادبی و سوء استفاده غیر قانونی از سیستم های کامپیوتری بود.

در دهه ۱۹۸۰ که بعنوان نسل دوم جرائم کامپیوتری محسوب می گردد. جرائم کامپیوتری فقط محدود به جرائم اقتصادی نبوده و سایر زمینه ها را هم که جنبه اقتصادی نداشته مانند دستکاری کامپیوتر بیمارستان ها، جعل اسناد با استفاده از کامپیوتر و ورود به اطلاعات خارجی محرمانه آمریکا، انگلستان و چند کشور دیگر دست یافته و این اطلاعات را به ک . گ . ب بفروشد. در دهه ۱۹۹۰ که شبکه جهانی (اینترنت) فراگیر شد جرائم کامپیوتری از جنبه اقتصادی وسیعتر گردیده و ابعاد جدیدتری به خود گرفته است. (قربان نیا، ۱۳۸۲: ۶۳)

جرایم جدید مانند ورود کرم اینترنتی که برای اولین بار توسط یک دانشجوی آمریکائی ساخته شده بود و باعث شد تا سیستم کامپیوتری حدود ۶۲۰۰ کاربر اینترنت شامل دانشگاهها، سرویسهای نظامی و سایتهای بیمارستانها را مختل نماید و هزینه تعمیرات سیستمها حدوداً به مبلغ ۹۸ میلیون دلار بود که بعد از مدتی این دانشجوی دستگیر و پس از محاکمه محکوم به پرداخت کلیه مبالغ فوق گردید.

به طور کلی می توان گفت جرائم سایبری اغلب دارای ابعاد بین المللی هستند. پست های الکترونیکی با محتوای غیر قانونی عموماً از میان تعدادی کشور تا رسیدن به مقصود عبور می کند و چند نظام حقوقی مختلف را درگیر چنین موضوعی می کند. یکی از راه های که می توان به وسیله آن بر آن مشکل فائق آمد توافقات دوجانبه رسمی بین کشورها است. اما در این رابطه مشکلاتی وجود دارد مبنی بر اینکه پروسه رسمی دست یابی به توافقات رسمی بین کشورها معمولاً زمان بر و دشوار است و با ذات جرائم رایانه ای که یکی از ویژگی های اصلی آن سرعت می باشد هم خوانی ندارد. این موضوع بدان معنی نیست که هیچ توافقی در رابطه با چنین جرائمی وجود ندارد، بلکه برخی جرائم در همه کشورها جرم انگاشته می شود. نمونه ای از چنین موارد سرقت است که می توان ادعا کرد در همه نظام های حقوقی جرم انگاری شده

است. علی‌رغم وجود اختلاف بین نظام‌های حقوقی مختلف در تعریف و تشخیص جرائم، روش‌های استفاده از تکنولوژی رایانه در همه جای جهان یکسان است. بنابراین از همین رو می‌توان این شانس را متصور بود که به دلیل متحدالشکل بودن سبک استفاده از رایانه کشورها با سرعت بیشتری به هماهنگی برسند. با توجه به مطالب مذکور امروزه جرائم سایبری گستره وسیعی از جرائم را در خود جای داده است که همتی جدی را در جهت مقابله با آن طلب می‌کند. این تلاش صرفاً محدود به کشورها نمی‌باشد و جامعه بی‌المللی ناگزیر است که در جهت مقابله با چنین جرائمی از خود واکنشی نشان دهد. نقش جامعه بین‌المللی در جای پررنگ‌تر می‌شود که بر سر امور مهمی همچون اعمال صلاحیت در مورد یک جرم از سوی کشورها و چنین مسائلی می‌بایست تعیین تکلیف گردد. مثلاً ممکن است جرمی سایبری علیه یک کشور در خاک کشور دیگری تحقق یابد و حتی کشورهای بیشتری درگیر این جرم شوند. از سویی حتی ممکن است به واسطه یک جرم بین‌المللی امنیت و صلح بین‌المللی به مخاطره افتد. بنابر مطالب گفته شده، سازمان‌های بین‌المللی مختلفی داده‌اند. درگیر جرائم رایانه‌ای شده و فعالیت‌های مفیدی را انجام داده‌اند. در ادامه به چند نمونه از برخی از سازمان‌های بین‌المللی که در رابطه با جرائم رایانه‌ای پرداخته‌اند اشاره شده و مختصراً فعالیت‌های آنان نیز تبیین می‌گردد. (کرمی، ۱۳۷۵: ۱۳۶)

نتیجه گیری:

سیاست جنایی که چاره‌اندیشی برای معضل جرم را به‌عنوان هدف و چارچوب اصلی خود برگزیده است به مجموعه اصولی گفته می‌شود که هیئت اجتماع بر مبنای آن پاسخ‌دهی به پدیده‌ی مجرمانه را سامان‌دهی خواهد کرد. در این میان نوع نگاه سیاست جنایی و تعیین اهداف آن می‌تواند بر عملکرد سیاست جنایی مؤثر واقع شود و برنامه‌های اجرایی و عملیاتی آن را در یک مسیر دیگر به حرکت وا دارد. لذا اگر سیاست جنایی با هدف تأمین امنیت و تضمین حداکثری آن تشکیل شود لازم است که بر این مبنا تمامی اصول، شرایط، راه‌کارها و سازوکارها و ابزارهای اجرای این هدف، در مجموعه سیاست جنایی تعریف شده و به‌کار گرفته شوند. تأمین امنیت اگر به‌عنوان هدف اولیه و والای سیاست جنایی پذیرفته شود لازم است که فرآیند جرم‌انگاری، انتساب مسئولیت کیفری و اعمال و تحمیل کیفرها نیز متناسب با این موضوع اصلاح شوند و در این صورت دورنمای سیاست جنایی از اصلاح و تربیت و بازپروری بزه‌کاران تبدیل به سزادهی و سرکوبی مجرمین خواهد شد که بر این اساس سیستم کنترل اجتماعی، چه در بُعد مداخله در وضعیت ما قبل جنایی به‌عنوان عملکرد کنشی پیشگیری از جرم و چه در بُعد واکنش کیفری و اعمال مجازات، بر مبنای عدم تسامح و تساهل در قبال رفتارهای مجرمانه و یا بعضاً منحرفانه تعریف و تبیین می‌گردد. کنوانسیون جرایم سایبری درباره اصول حاکم بر همکاری دو و چند جانبه دولت‌ها و قواعد استرداد مجرمان و معاضدت قضایی بحث شده است. ماده ۲۳ کنوانسیون با عنوان اصول کلی مربوط به همکاری بین‌المللی مقرر می‌دارد که عضای کنوانسیون باید براساس مقررات این فصل و از طریق اعمال ابزارهای بین‌المللی مربوط به همکاری بین‌المللی در زمینه مسائل کیفری، تمهیدات مورد توافق بر پایه قانونگذاری یکنواخت یا متقابل و حقوق داخلی، برای رسیدن به وسیع‌ترین محدوده ممکن به منظور پی‌جویی‌ها یا رسیدگی‌های قضایی راجع به جرایم مرتبط با سیستم رایانه‌ای و داده‌ها یا جمع‌آوری دلایل الکترونیکی در جرایم با همدیگر همکاری کنند.

منابع:

۱. ایوانز، گرام و نونام، جفری (۱۳۸۱)، فرهنگ روابط بین الملل، مشیرزاده، حمیرا و شریفی، حسین، چ دوم، انتشارات اطلاعات.
۲. باستانی، برومند (۱۳۸۳)، جرایم کامپیوتری و اینترنتی جلوه ای نوین از بزهکاری، چ دوم، تهران، بهنامی.
۳. پور قهرمان بابک و حسین علی بای (۱۳۸۸)، بررسی فقهی و حقوقی جرایم رایانه ای، قم، انتشارات پژوهشگاه علوم و فرهنگ اسلامی، چاپ اول.
۴. جاویدنیا، جواد (۱۳۸۸)، جرایم تجارت الکترونیکی، چ دوم، تهران، انتشارات خرسندی.
۵. جلالی فراهانی، امیر حسین (۱۳۸۹)، کنوانسیون جرایم سایبر و پروتکل الحاقی آن، چ اول، تهران، خرسندی.
۶. جوان جعفری، عبدالرضا (۱۳۸۹)، جرایم سایبر و رویکرد افتراقی حقوق کیفری، مجله دانش و توسعه، سال هفدهم، شماره ۳۴، صص ۱۷۰-۱۹۳.
۷. حسن بیگی، ابراهیم (۱۳۸۳)، حقوق و امنیت در فضای سایبر، چ اول، تهران، انتشارات موسسه فرهنگی مطالعاتی و تحقیقاتی بین الملل ابرار معاصر.
۸. خداقلی، زهرا (۱۳۸۳)، جرایم کامپیوتری، چ اول، تهران، انتشارات آریان.
۹. خرم آبادی، عبدالصمد (۱۳۸۴)، جرایم فناوری اطلاعات، پایان نامه مقطع دکتری، دانشگاه حقوق و علوم سیاسی دانشگاه تهران.
۱۰. ذاکریان، مهدی (۱۳۸۳). مفاهیم کلیدی حقوق بین الملل بشردوستانه، تهران، نشر میزان.
۱۱. راسخی، افشین (۱۳۹۰)، امنیت اطلاعات در فضای اینترنت، فصلنامه علمی-ترویجی دانش حفاظتی و امنیتی، سال ششم، شماره ۲۱، زمستان، صص ۱۹-۴۸.

۲۵۸.....تحقیقات حقوقی تطبیقی ایران و بین‌الملل، سال یازدهم، شماره چهل و دوم، زمستان ۱۳۹۷

۱۲. زیبر، اولریش (۱۳۹۰)، **جرایم رایانه ای**، مترجمان نوری، محمد علی و نخجوانی، رضا و بختیار وند، مصطفی و رحیمی مقدم، احمد، چ اول، تهران، گنج دانش.

۱۳. زینالی، امیر حمزه (۱۳۸۸)، **حمایت کیفری از کودکان در برابر هرزه نگاری- از واکنشهای جهانی تا پاسخ های نظامی کیفری ملی**، حقوق فناوری اطلاعات و ارتباطات (مجموعه مقالات)، چاپ اول، تهران، انتشارات روزنامه رسمی کشور.

۱۴. سالاری، مهدی، سرقت تعزیری و رایانه ای، چاپ اول، تهران، میزان، ۱۳۸۹.

۱۵. شاهبندرزاده، حمید، شهلا، یوسفی ده بیدی (۱۳۹۱)، **تعیین درجه اهمیت جرائم رایانه ای از دیدگاه صاحب نظران انتظامی استان بوشهر، فصلنامه نظم و امنیت انضباطی**، سال پنجم، بهار، صص ۱۳۷-۱۵۵.

۱۶. شریفی، مرسده، **جرایم رایانه ای در حقوق جزای بین المللی**، پایان نامه کارشناسی ارشد، دانشگاه آزاد اسلامی، ۱۳۷۹

۱۷. شیرزاد، کامران (۱۳۸۸)، **جرایم رایانه ای از دیدگاه حقوق جزای ایران و حقوق بین الملل**، چ اول، تهران، نشر بهینه فراگیر، ص ۳۸.

۱۸. عالی پور، حسن (۱۳۹۰)، **حقوق کیفری فناوری اطلاعات**، چ اول، تهران، نشر خرسندی،

۱۹. فریبرزی، الهام (۱۳۹۰)، **امنیت اطلاعات در فضای اینترنت**، فصلنامه تخصصی فقه و تاریخ تمدن، سال هفتم، شماره بیست و هفتم، صص ۱۸۵-۱۵۸.

۲۰. قربان نیا، ناصر (۱۳۸۲)، **مداخله بشر دوستانه از منظر حقوق بین‌الملل**، نامه مفید (حقوقی)، سال نهم، شماره ۳۷، مرداد و شهریورماه.

۲۱. کرمی، جهانگیر (۱۳۷۵)، شورای امنیت سازمان ملل متحد و مداخله بشر

دوستانه، چ اول، تهران، دفتر مطالعات سیاسی و بین‌المللی.

۲۲. *American Bar Association, section of science and technology, security committee, Digital signature Guidelines tutorial.* ۲۰۱۳.

۲۳. Brenner, susan, toward a criminal law for cyberspace: Disturbed security, university of Dayton school of law, <http://law.bepress.com/expresso/eps/2012>.

۲۴. *Carey, Peter, Media Law, Sweet & Maxwell, second Edition, London, 2013.*

۲۵. *Cyber Law Simplified; Indian Information Technology Act (2015)*

۲۶. *Engle, Eric, Extraterritorial Corporate Criminal Liability A Remedy for Human Rights Violations- 2013.*

۲۷. *European Convention on the Legal Protection of Services Based on or Consisting of Conditional Access- EST 2011.*

۲۸. *M. Gahtan, Alan Electronic Evidence; Carswell; 2011;*

۲۹. *M. Gahtan, Alan; Electronic Evidence; Carswell; 2006.*