صلاحیت کیفری در فضای سایبر

تاریخ دریافت: ۱۳۸۵/۹/۱ تاریخ تأیید: ۱۳۸۵/۱۰/۱۰

امیرحسین جلالی فراهانی*

چکیده

سوء استفاده‌های فراوان از فضای سایبر باعث پیش‌بینی تدابیری شده است که از جملهٔ آنها جرم‌انگاری عناوین مجرمانه از سوی کشورهای مختلف است. بدیهی است اعمال مجازات قانونی در بستر صلاحیت کیفری آن قانون رخ می‌دهد و در این میان ویژگیهای متمایز و منحصر به فرد فضای سایبر نسبت به دنیای فیزیکی باعث شده تا در زمینهٔ صلاحیت کیفری در فضای سایبر مباحث جدی و اساسی صورت گیرد و آرای مختلفی ابراز شود، به گونه‌ای که برخی از آن به فضای فاقد حاکمیت یاد می‌کنند و برخی معتقدند صلاحیت کیفری با جلوه‌های مختلف آن می‌تواند در فضای سایبر همانند دنیای فیزیکی حاکمیت داشته باشد. مقالهٔ حاضر تلاش می‌کند با نقد و بررسی دیدگاههای موجود، زمینهٔ بحث و بررسی بیشتر را فراهم آورد.

واژگان کلیدی: *فضای سایبر، قلمرو حاکمیتی، صلاحیت سرزمینی، صلاحیت تابعیتی، صلاحیت حمایتی، صلاحیت جهانی.*

---

* کارشناس ارشد حقوق کیفری و جرم‌شناسی، پژوهشگر در حقوق کیفری سایبری (jalalyfarahany 1979@gmail.com).
این مقاله خلاصه‌ای از کار پژوهشی با عنوان «درآمدی بر صلاحیت کیفری در فضای سایبر» است که توسط نگارنده در سال ۱۳۸۵ برای معاونت حقوقی و توسعهٔ قضایی قوهٔ قضائیه انجام شده است.

مقدمه

به شهادت تاریخ، یکی از اساسی‌ترین شیوه‌های حکمرانی دولتها بـر ملتهـای خـویش، وضع قواعد الزام‌آوری با نام کُد یا قانون‌نامه بوده که تخطی از آنها مـستوجب مجازاتهـایی بود که تصور آن هم برای بشر امروز بسیار دردناک و وحشتناک است. از نمونـه‌هـای بـارز آنها، قانون‌نامهٔ حمورابی است که حدود سه هزار سـال پـیش از مـیلاد مـسیح بـر سـاکنان بین‌النهرین اعمال می‌شد. حمورابی در این زمینه می‌گوید:

> بگذارید هر آنکه را ظلمی رفته و دعوایی دارد، سنگ‌نوشتهٔ مـرا بخوانـد، شـاید کـه کـلام گهربار مرا گوش جان سپرد و سنگ‌نوشته‌ام مشکل او را مرتفع سازد. شاید که حکم خـود را در آن یافته و ذهنش آرام گیرد ... (وست‌بروک، ۱۳۸۳: ۱٦۱).

به تدریج، دوران اعمال فراگیر آن کدها به سرآمد و هیأتهای حاکمه دریافتنـد کـه تنهـا باید به آنچه در مفهوم عام قلمرو حاکمیتی‌شان می‌گنجد بسنده کنند و از تعرض به دیگران بپرهیزند. لذا با توجـه بـه اهمیـت ایـن موضـوع در برقـراری صـلح و ثبـات بـین‌المللـی، صاحب‌نظران و سیاستگذاران حقوق بین‌المللی، طی سالهای ۱٦٤۸ تا ۱۸۱۵ تلاش خـود را مصروف ترسیم قواعد عدم دخالت دولتها کردند و نظریهٔ حاکمیت دولتها را بر سه اصل بنا نهادند: ۱. حاکمیت در قلمرو خـود از آزادی عمـل و قـدرت بلامنـازع برخـوردار اسـت؛ ۲. دولتها از لحاظ حقوق، تعهدات و آزادی عمل، قانونـاً در وضـعیت یکـسانی نـسبت بـه یکدیگر قرار دارند؛ و ۳. به عنوان نتیجهٔ منطقی دو اصل فوق، دولتها جز قوانینی که با ارادهٔ آنها و از طریق قراردادها، عرف و اصول کلی شناخته شده از سوی آنان پدیـد آمـده، تـابع هیچ قانون برتری نیستند (شیایزری، ۱۳۸۳: ۱٦).

در این اثنا، نیاز مبرم بشر به تعامل با دیگر نقاط جهان ایجاب کـرد ابزارهـایی را ابـداع کند و به خدمت گیرد که مفهوم مطلق و گزندناپذیر قلمرو حاکمیتی را دستخوش تحولاتی قرار داد. توسعه و ارتقای سیستم حمل و نقل زمینی، به ویژه ریلی، دریایی و در قرن اخیـر هوایی، موجب شد عملاً جزیره‌های شناوری (Floating Islands) از کشورها جدا شده و با خیلی از جمعیت به قلمرو دیگران وارد شوند که بالطبع موضوعات جدیدی را مطرح ساخت.

همچنین، در این حین، صنعت ارتباطات نیز با تحولاتی اساسی مواجه شد. اختراع تلفن آرزوی دیرینهٔ بشر در برقراری ارتباطـات غیرحـضوری را محقـق کـرد و بهبـود تـدریجی

کارکردهای آن، مانند امکان ارسال متن از طریق خطوط مخابراتی، ابتکار عملهـای بیـشتری را فراهم آورد. اما آنچه باعث بازآفرینی اساسی این حوزه شـد، دسـتیابی بـشر بـه فنـاوری رایانهٔ الکترونیکی (Electronic Computer) است. این فناوری نه تنها خود تحولی عظیم را در عرصهٔ ذخیره‌سازی نامحدود، پردازشهای گوناگون و ارائهٔ مطلـوب اطلاعـات بـا حفـظ تمامیت و صحتشان فراهم ساخت و به تبع آن دانش به عنوان محور توسعهٔ پایدار در هزارهٔ جدید را به مرحلهٔ جدیدی وارد کرد (یزدان‌پور، ۱۳۸٤: ۳۳)، بلکه مخابرات آنـالوگ را بـه دیجیتال تبدیل کرد و پس از مدت نسبتاً کوتاهی پیوندی میان این دو رقم خورد که ماحصل آن دنیایی کاملاً متمایز با ویژگیهای منحصر به فرد به نام فضای سایبر (Cyber Space) است و با اینکه بیش از یک دهه از حضور جدی آن در عرصهٔ جهانی نمی‌گذرد، اما تقریباً حوزه‌ای نمانده که به آن وارد نشده یا مقدمات ورود به آن فراهم نشده باشد.

برای پی بردن به این موضوع کافی است امور پیرامون خود را از نظـر بگـذرانیم. از ساده‌ترین شکل ارتباطات الکترونیکی، مانند ارسال پیامهای کوتاه یا پـست الکترونیکـی گرفته تا اموری مانند تجارت و داد و ستد و به تبع آن پول و بانکـداری الکترونیکـی و حتی خدمات بهینه شده‌ای مانند درمان و دادرسی الکترونیکی، همگی در این بستر رتق و فتق می‌گردند. حتی دولتها نیز با احراز مزایای فوق‌العادهٔ آن در تلاش‌اند امور دولتـی را نیز به شیوهٔ الکترونیکی به پیش ببرند و در حال حاضر یکی از مباحث اصلی و جدی آنها دولت الکترونیکی و تسهیل و تسریع تحقق آن است. آیا این دگردیسی الکترونیکـی (E-transformation) پرشتاب جز انعطاف‌پذیری بی‌نظیر این فناوری است، به نحوی کـه بـا حداقل دانش و مهارت فنی می‌توان آن را به کاربرد و از همه مهم‌تر اینکه در بهینه‌سـازی و بهره‌وری امور بسیار مؤثر است؟

با این حال، نکتهٔ بسیار مهمی که شـاید بـه دلیـل جلـوه‌گـری بـیش از حـد قابلیتهـای شگفت‌انگیز بی‌شمار این فضا باعث شده کمتر به آن توجه شود، این است که در این فـضا حد و مرز به معنای آنچه در دنیای فیزیکی ادراک می‌شـود وجـود نـدارد. در واقـع، بـستر مشترکی با گستره‌ای لایتناهی شکل گرفته که هـرکس بـه قـدر شـناخت نیازهـای خـود و قابلیتهای راهگشای این فضا در آن حضور می‌یابد و این‌گونه نیست که در آنجا بـر اسـاس معیارهای گوناگون، مانند وسعت سرزمینی، میـزان جمعیـت، درآمـد سـرانه و ... مرزبنـدی

صورت گرفته باشد. حتی فراتر از آن، برای اینکه هیچ مانعی بر سـر راه توسـعه و ارتقـای این بستر مشترک جهانی به وجود نیاید، ابداع‌کننـدگان و همچنـین گردانندگان فعلـی آن، اصول تحدیدناپذیرش را پذیرفته‌اند و عملاً نیز به اجرا می‌گذارند (کاشیان، ۱۳۸٤: ۱۱۰).

اگر حد و مرزی برای فعالیتهای سایبری ترسیم می‌شد، تا این حد امکـان شـکوفایی آن وجود نداشت، اما این باعث نمی‌شود موضوع اساسی مذکور در ابتدای بحث، یعنی اعمـال حاکمیت بر قلمرو، به مفهوم عام آن، تحت‌الشعاع قرار گیرد. با اینکه بسیاری به اشتباه ایـن فـضا را مجـازی (Virtual Space) تلقـی مـی‌کننـد و در واقـع قابلیـت مجـازی‌سـازی‌اش (Virtualization) را به مجازی بودن ماهیتش پیوند می‌زنند، اما همانها این واقعیت را انکار نمی‌کنند که تبعات ناشی از سوء استفاده‌های گوناگون از این فضا، به تهدیدی برای جامعـهٔ بشری تبدیل شده است. به ویژه آنکه این سوء استفاده‌ها به انـدازهٔ نفـوذ فـضای سـایبر در شئون خرد و کلان، گستردگی و تنوع دارند و بدتر آنکه پیامدهای به وجود آمده، به مراتب از نظایر فیزیکی زیانبارتر و خطرناک‌تر هستند. این در حالی است که حاکمیت بـرای مبـارزه بـا این هنجارشکنیها در توسل به کیفر با محدودیتهای بسیاری از جمله و به ویژه مشخص نبودن حدود و ثغور قلمرو حاکمیتی‌اش مواجه است. همچنین اگـر بخواهـد بـه قواعـد صـلاحیت فرامرزی استناد کند نیز محرز است که آنها در موضع استثنا قرار دارند و چندان ابتکار عملـی ایجاد نمی‌کنند، مگر اینکه شرایط و اوضاع و احوال جدید اسباب موجهه‌ای را فراهم آورد.

همان‌طور که ملاحظه می‌شود، موضوع این نوشتار مسائل صلاحیت کیفری در فضای سایبر است. موضوعی به واقع اساسی و بنیادی که بدون اغراق دروازهٔ تدابیر کیفری محسوب می‌شود. به ویژه اگر همانند بسیاری از صاحب‌نظران حقوقی، چه از نظام حقوق عرفی چه رومی ـ ژرمنی، مفهوم موسعی از آن مد نظر قـرار گیـرد و بـه موجـب آن جـرم‌انگـاری، صـلاحیت در وضـع (Jurisdiction to Prescribe)، محاکمه، صلاحیت در قـضا (Jurisdiction to Adjudicate)، و اجرای حکم کیفری، صلاحیت در اجرا (Jurisdiction to Enforce) تعبیر شـود کـه بـه ایـن ترتیب، هیچ اقدامی در عرصـهٔ نظـام عـدالت کیفـری صـورت نمـی‌گیـرد، مگـر از سـوی مرجع ذی‌صلاح آن (European Committee on Crime Problems, 1990: 7).

بدیهی است غور در هر یک از این مباحث و همچنین بررسی قوانین و مقررات مربوط داخلی مجال موسعی می‌طلبد و لذا در اینجا تنها به ذکر کلیات و مبانی این حوزه پرداختـه

می‌شود. به این منظور، در فصل اول موضوعات راجع بـه صـلاحیت سـرزمینی در فـضای سایبر و در فصل دوم نحوهٔ اعمال قواعد صلاحیت فراسرزمینی مورد بررسی قـرار خواهـد گرفت و در نهایت نتیجه‌گیری به عمل خواهد آمد.

فصل اول. صلاحیت سرزمینی و فضای سایبر

مهم‌ترین اصل در اعمال صلاحیت کیفری، اتکا به قلمرو حاکمیتی است که مصداق بارز آن قلمرو سرزمینی است و به همین دلیل، عموماً آن را به جای مفهوم موسع‌تر خود به کار می‌برند. اما این دلالت تضمنی، نباید دیگر مصادیق را تحت‌الشعاع قرار دهـد. لـذا در ایـن فـصل ابتـدا اجمالاً به تبیین مفهوم قلمرو سرزمینی پرداخته می‌شود تا بر اساس آن امکان طرح مسائل راجع به تعیین محل ارتکاب جرم فراهم آید. سـپس در گفتـار دوم صـحت و سـقم مفهـوم قلمـرو سرزمینی سایبری و به تبع آن راههای تعیین محل ارتکاب جرائم سایبری مطرح خواهد شد.

گفتار اول: تعیین محل ارتکاب جرم بر اساس قلمرو سرزمینی

مبنایی‌ترین و قدیمی‌ترین قاعده‌ای که برای اعمال قوانین جزایی مـورد اسـتناد محـاکم کیفری قرار می‌گیرد، صلاحیت سرزمینی اسـت. بـه عقیـدهٔ برخـی صـاحب‌نظـران، مبنـای پذیرش این اصل این است که:

> حاکمیت سرزمینی، بیشترین منفعت، مؤثرترین امکانات و راحت‌ترین وضعیت را برای مقابله با جرائمی که در قلمرو سرزمینی ارتکاب می‌یابند فراهم می‌کند (August, 2002: 536).

به عبارت دیگر، اصولاً جرم ماهیتی محلی دارد که بهتـرین شـیوهٔ مجـازات آن، اجـرای محلی‌اش است. البته سهولت جمع‌آوری دلایل، قرائن و امارات محکمه‌پسند، در کنار تأمین اهداف ارعاب‌انگیزی و عبرت‌آموزی مجازات را نبایـد فرامـوش کـرد. در ادامـه مفهـوم و گسترهٔ قلمرو سرزمینی مورد بررسی قرار می‌گیرد. برای پی بردن بـه جایگـاه تعیـین کننـدهٔ قلمرو سرزمینی در حکمرانی کیفری و همچنین ملاحظات مصلحت‌آمیز عـصر حاضـر، بـه رأی دیوان دادگستری بین‌المللی در دعوای فرانسه علیه ترکیه به سال ۱۹۲۷ که بـه دعـوای لوتوس معروف است، اشاره می‌شود:

> حقوق بین‌المللی، بر روابط بین کشورهای مستقل حاکم است. از این رو، قواعد و نظامات حاکم بر این روابط که با هدف ساماندهی مناسبات این جوامع هم‌زیست و به امید دستیابی

به اهداف مشترک وضع گردیده، ناشی از ارادهٔ آزاد آنهاست که در معاهدات بین‌المللی و عرفی که مبین اصول حقوقی پذیرفته شده از سوی همگان می‌باشد، به منصهٔ ظهور رسیده است. از این رو، اعمال هر گونه محدودیت نسبت به استقلال و آزادی عمل دولتها، فرضی محال و غیرممکن خواهد بود. در این شرایط نخستین و بارزترین محدودیتی که توسط حقوق بین‌الملل علیه هر دولت اعمال می‌گردد، آن است که ــ در صورت فقدان قاعده روادارنده‌ای (Permissive Rule) که بر خلاف این حکم مقرر نماید ـ یک کشور تحت هیچ شرایطی مجاز به اعمال قدرت خود در قلمرو کشوری دیگر نمی‌باشد. از این منظر، صلاحیت بی‌هیچ تردیدی امری سرزمینی است و اعمال آن توسط یک کشور در خارج از قلمرو خود، جز از طریق یک قاعدهٔ روادارندهٔ ناشی از عرف یا معاهدهٔ بین‌المللی میسر نمی‌باشد. با وجود این، آنچه گفته شد، هرگز به این معنا نیست که حقوق بین‌المللی مانع از آن می‌گردد که کشوری در سرزمین خود در قبال وقایعی که خارج از قلمرو آن رخ داده است، با تکیه بر پاره‌ای قواعد روادارندهٔ حقوق بین‌الملل در این زمینه اعمال صلاحیت نماید. برعکس، حقوق بین‌الملل به جای وضع یک بازداری کلی دایر بر ممنوعیت توسعهٔ اعمال قوانین و صلاحیت محاکم کشورها بر اشخاص، اموال و اعمال خارج از قلمرو آنها، میزان گسترده‌ای آزادی عمل به آنها اعطا می‌نماید که جز از طریق پاره‌ای قوانین بازدارنده (Prohibitive Rules) محدود نمی‌گردد ... (شیایزری، همان: ۱۷).

۱. مفهوم و گسترهٔ قلمرو سرزمینی

برخلاف آنچه ظاهراً این اصطلاح نشان می‌دهد، تنها به خاک یک کشور اشاره ندارد و به تبع آن جو فوقانی و همچنین بخشی از آبهای مجاور خاک کشور که در معاهدات بین‌المللی حدود آن مشخص شده نیز به حساب می‌آیند (Law Reform Commission of Canada, 1984: 12). هر چند پرواضح است که این حوزه‌ها و فضاها فی‌نفسه نقشی ندارند و آنچه به آنها هویت می‌بخشد، مصنوعاتی هستند که بشر با ابداع آنها توانسته آنها را به تسخیر خود درآورد. اما اینکه این مصنوعات جزئی از قلمرو سرزمینی هستند که به صورت موقتی از آن منفصل شده‌اند و پس از انجام مأموریت به اصل خویش بازمی‌گردند یا اینکه مفهوم قلمرو سرزمینی در مورد آنها صدق نمی‌کند و باید به دنبال اتخاذ دیگر راهبردهای صلاحیت بود، مسائلی جدی را برانگیخته است.

برای حل این مسئله، عده‌ای اصل صلاحیت سرزمینی شناور (Floating Territorial Principle)

را مطرح کرده‌اند که مطابق آن کشور صاحب پرچم هواپیما، کشتی یا قطار می‌تواند با تلقی آن به عنوان بخشی از قلمرو سرزمینی خود به اصل مربوط استناد کند (میر محمدصادقی، ۱۳۷۷: ۲۵). زیرا در واقع اینها جزایر شناوری هستند که جزء قلمرو سرزمینی محسوب می‌شوند. با پذیرش این اصل، هرکس با هر تابعیتی، در هواپیما، کشتی یا قطار مرتکب یکی از جرائم مندرج در مجموعهٔ قوانین کیفری کشور صاحب پرچم شود، دادگاههای آن صالح به رسیدگی خواهند بود.

با این حال، اگر به این ضابطه با دید منطقی و متعارف نگریسته شود، ملاحظه می‌گردد اجرای ساماندهی نشدهٔ آن می‌تواند مشکلاتی را ایجاد کند. برای مثال، در جایی که بخش خصوصی این صنایع را در اختیار دارد، به ویژه در خصوص کشتیها، مسلماً پرچم کشوری را حمل خواهد کرد که امتیازات بیشتری را به آن اعطا می‌کند. همین امر باعث شده اکنون حمل پرچمهای مصلحتی (Flags of Convenience) به یکی از معضلات اصلی این حوزه تبدیل شود و عملاً کشورها به اصول و موازین دیگری برای اعمال صلاحیت کیفری متوسل شوند (Menthe, 1998: 93). اما در جایی که این صنایع دولتی هستند، پرچم نصب شده جنبهٔ واقعی دارد و این قاعده قابل اجرا خواهد بود.

در پایان، شایان ذکر است گروهی از صاحب‌نظران قواعد حاکم بر صلاحیت تابعیتی را بر این مصنوعات جاری می‌دانند که البته در برخی اسناد و کنوانسیونهای بین‌المللی که به ویژه راجع به فضاها و دریاهای بین‌المللی به تصویب رسیده‌اند نیز بر آن تأکیدهایی شده، اما به آن منحصر نگردیده است. زیرا نسبت به صلاحیت سرزمینی محدودیتهایی دارد که اجرای کامل و بدون استثنای قوانین کیفری در قلمرو سرزمینی از عهدهٔ آن خارج است. برای مثال، اتکای صرف به صلاحیت تابعیتی باعث خواهد شد اتباع دیگر کشورها که در کشتی، هواپیما یا قطار حضور دارند، مصون بمانند (Ibid: 92).

۲. شاخصهای تعیین محل ارتکاب جرم

رایج‌ترین و در عین حال ساده‌ترین شیوهٔ تعیین محل ارتکاب جرم، شناسایی محل حضور مجرم است. قاعدتاً هرجا که او حضور داشته، فرایند گذار از اندیشه به عمل (Acting Out) شکل گرفته و عنصر معنوی در عنصر مادی جرم متجلی شده است.

اما با کمی دقت در ماهیت انواع جرائمی که در قوانین جزایی منعکس شده، محرز می‌گردد که صرف اتکا به این مؤلفه نمی‌تواند به شایستگی اهداف حقوق کیفری را برآورده سازد و ضرورت اقتضا می‌کند ضوابط دقیق‌تری در قالب تفکیکهای منطقی و قابل اجرا تدوین شود. در این زمینه، با امعان نظر به کیفیت ارتکاب تمامی جرائم، به طور کلی اصل صلاحیت سرزمینی به دو شاخهٔ صلاحیت سرزمینی شخصی (Subjective Territorial Principle) و صلاحیت سرزمینی نوعی (Objective Territorial Principle) تقسیم شده است.

۲ـ۱. صلاحیت سرزمینی شخصی

شایع‌ترین حالتی که برای اعمال صلاحیت سرزمینی مورد استناد قرار می‌گیرد، با عناوین پیوند شروع به ارتکاب (Commencement Nexus) و دکترین عناصر متشکلهٔ جرم (The Constituent Elements Doctrine) نیز شناخته می‌شود. منظور از تمامی این اصطلاحات این است که از هر جا فرایند ارتکاب جرم آغاز شود، محکمهٔ کیفری همان قلمرو سرزمینی صالح به رسیدگی است، حتی اگر دیگر عناصر متشکلهٔ آن در خارج از قلمرو محقق و تکمیل گردد. در واقع چون نقطهٔ آغاز فرایند گذار از اندیشه به عمل، این محل بوده است، این اصل به آن تسری یافته است. این قاعده جهان‌شمول است و در اصل آن تردیدی وارد نشده، مگر در مصادیق جدید که احراز آن را با مشکلات عدیده‌ای مواجه کرده است (میر محمدصادقی، همان: ۲٤).

۲ـ۲. صلاحیت سرزمینی نوعی

اما حالت دیگری که به ویژه از سوی کشورهای تابع نظام حقوق عرفی، به ویژه امریکا، با اقبال مواجه شده و برای اعمال اصل سرزمینی مورد استناد قرار می‌گیرد، به محل تحقق نتیجهٔ جرم اشاره دارد (August, op.cit: 537). بعضی جرائم به محض وقوع محقق می‌شوند که در این صورت، محل شکل‌گیری عناصر متشکله و محل تحقق نتیجهٔ جرم یکی خواهد بود و به همین دلیل به آنها جرائم رفتاری (Conduct Crimes) یا مطلق گفته می‌شود. اما جرائمی که در آنها این مراحل از یکدیگر منفک هستند، مقید (Result Crimes) نامیده می‌شوند. برای مثال، جرم جعل به محض خدشه وارد آمدن به سند یا سرقت به محض خارج کردن مال از حرز محقق می‌شود. اما تحقق جرمی مثل قتل زمانی است که قربانی بمیرد. حال ممکن است میان فعل ارتکابی، مانند شلیک و وقوع نتیجه، یعنی مردن،

کیلومترها و یا چند روز فاصله باشد و همین امر باعث شود در دو قلمرو سرزمینی تکون یابد (Law Reform Commission of Canada, op.cit: 108).

به این ترتیب، با توجه به اهمیتی که نتیجهٔ جرم (Fruit of Crime) دارد، بر فعل ارتکابی تفوق یافته و به عنوان شق دیگر صلاحیت سرزمینی پذیرفته شده است. به ویژه آنکه از برخی جهات، موجه نیز به نظر می‌رسد. اولاً علی‌القاعده محل اصلی ارتکاب جرم، محل وقوع نتیجهٔ آن است و تا آن زمان از لحاظ عنوان مجرمانه‌ای که در قانون تعریف شده، جرمی به وقوع نپیوسته است. ثانیاً جامعه‌ای که شاهد تحقق نتیجه بوده، اگر بیشتر نباشد، حداقل به اندازهٔ جامعه‌ای که شاهد مقدمات بعیده و شروع به جرم بوده، احساساتش جریحه‌دار شده و البته لازم است ضوابط ارعاب‌انگیزی و عبرت‌آموزی را هم در مورد آن مکان رعایت کرد و در نهایت اینکه، از لحاظ ادلهٔ جرم نیز مهم‌ترین ادلهٔ مثبته که راجع به نتیجهٔ فعل مجرمانه می‌باشد نیز در این مکان وجود دارد و از این لحاظ هم توجیه‌پذیر است. هرچند معضلاتی جدی مانند دسترس به مجرم و رعایت ضوابط استرداد و دیگر مسائل را نمی‌توان انکار کرد (Xingan, 2004: 10).

اما در خصوص نحوهٔ تعیین محل ارتکاب جرم مطابق قوانین ملی، برای مثال در قسمت دوم از بخش نهم قانون مجازات عمومی آلمان چنین آمده است:

> در شرایط ذیل ارتکاب فعل در قلمرو سرزمینی مفروض انگاشته می‌شود: ۱) در هر مکان که مباشر آنچه را مرتکب شود که عنصر جرم تلقی می‌شود یا در ترک فعل باید آن را انجام می‌داد یا نتیجهٔ آن با آگاهی وی محقق شود یا باید محقق می‌شد؛ ۲) تحریک یا معاونت نه تنها در محلی که فعل ارتکاب یافته، بلکه نسبت به هر محلی که تحریک کننده یا معاون عمل کرده یا در حالت ترک فعل باید عمل می‌کرده یا از نظر آگاهی او، آن فعل باید به انجام می‌رسیده نیز صادق است. اگر تحریک کننده یا معاون در خصوص یک فعل فرامرزی، فعل خود را در داخل مرتکب شده باشد، در اینجا نیز قانون کیفری آلمان در مورد تحریک یا معاونت قابل اجرا خواهد بود، حتی اگر آن فعل، مطابق قانون محل ارتکاب فعل مباشر قابل مجازات نباشد (Brenner, 2004: 14).

گفتار دوم: تعیین محل ارتکاب جرائم در فضای سایبر

برای تعیین محل ارتکاب جرائم در فضای سایبر، ابتدا باید قلمرو سرزمینی در این فضا مشخص شود. اما پیش از آن، گفتنی است که در اینجا جرائمی مورد توجه قرار گرفته‌اند

که عنصر مادی آنها در این فضا تحقق یابد. لذا به طور کلی آن دسته از جرائمی که این فضا در حکم ابزار ارتکابی آنها بوده، از حوزهٔ شمول این بحث خارج خواهد بود (خرم‌آبادی، ۱۳۸۳: ٥٤).

۱. مفهوم قلمرو سرزمینی در فضای سایبر

برای درک مفهوم قلمرو سرزمینی در فضای سایبر، ابتدا لازم است بستر تشکیل دهنده و ابزار دسترس به آن شناسایی گردد.

۱ـ۱. بستر ارتباطات و مبادلات الکترونیکی

منظور از بستر ارتباطات و مبادلات الکترونیکی، مجموعه‌ای عظیم از صفر و یکهایی است که داده‌های الکترونیکی را تشکیل می‌دهد و آنها نیز در قالبهای مختلف، مفاهیم را به شکل الکترونیکی منعکس می‌کنند. در واقع، فضای سایبر همین بستر است که داده‌های الکترونیکی در آن، ذخیره، به انحای گوناگون پردازش و در نهایت به شیوهٔ مورد نظر منعکس می‌شوند.

به این ترتیب، شاید بتوان چنین نتیجه‌گیری کرد که هرجا مراکز تولید کنندهٔ بسترهای الکترونیکی قرار داشته باشند، که اصطلاحاً به آنها مراکز دادهٔ اینترنتی (Internet Data Center) گفته می‌شود، و از لحاظ فنی به ارائهٔ خدمات میزبانی (Hosting) و ملزومات تبعی آن می‌پردازند (دبیرخانهٔ شورای عالی اطلاع‌رسانی، ۱۳۸٤: ۲۰)، جزء قلمرو حاکمیتی آن کشور به شمار می‌روند. با اذعان به اینکه چنین استدلالی از مبنای قابل دفاعی برخوردار است، اما در حال حاضر بیش از هشتاد درصد مراکز اینترنتی دنیا در امریکای شمالی و شمال اروپا واقع هستند و بعید است آنها به اعمال چنین صلاحیتی برای رسیدگی به طیف بسیار متنوع و عظیم جرائم ارتکابی در فضای سایبر از سراسر جهان، که به مجرمانه بودن بعضی از آنها نیز اعتقاد ندارند، تن در دهند.

۱ـ۲. ابزار دسترس به بستر ارتباطات و مبادلات الکترونیکی

آنچه در اینجا از ابزار دسترس به فضای سایبر مورد توجه قرار گرفته، خدمات دسترس نیست که در لایه‌های مختلف تأمین، توزیع و عرضهٔ خدمات اینترنتی به فعالیت می‌پردازند و مثال بارز آنها ارائه دهندگان خدمات اینترنتی (ISP) هستند (مرکز پژوهشهای مجلس

شورای اسلامی، ۱۳۸۵: ٤)، بلکه ابزارهای هویت‌بخش فضای شبکه‌ای با عنوان نام دامنه (Domain Name) است که از سوی عوامل مربوط ارائه می‌شوند. این نامها اصالتاً مجموعه‌ای دوازده رقمی از شمارگان هستند که به صورت سه‌تایی تقسیم شده‌اند و برای راحتی کاربران به صورت نام به نمایش درمی‌آیند. برای مثال، شمارهٔ ۱۹۳,۰,۰,۱۹۹ به postman.ripe.net تعلق دارد (کاشیان، همان: ۲۲).

اما آن قسمت از این نام که به این بحث مربوط می‌شود، دامنهٔ مرتبهٔ بالا نام دارد که به طور کلی به دو قسمت تقسیم می‌شود: دامنهٔ مرتبهٔ بالای عمومی (Generic Top Level Domain Name) مانند (.com,.net) و دامنهٔ مرتبهٔ بالای کد کشوری (Country Code Top Level Domain Name) مانند (.ir). با اینکه تمامی این دامنه‌ها از سوی یک شرکت آمریکایی با نام (ICANN) صادر می‌شود، اما طبق روال ایجاد شده، کدهای کشوری تنها به دولتها واگذار می‌شود تا آنها نسبت به تخصیص آن سیاستگذاری و اقدامات لازم را انجام دهند. لذا عملاً این کدها به مصداق بارزی از اعمال حاکمیت کشورها در فضای سایبر تبدیل شده است (همان: ۲۸۳).

با توجه به این توضیحات، به نظر می‌رسد نقش این نامها در یافتن راه حلی منطقی، کاربردی و قابل اجماع در عرصهٔ جهانی روشن شده باشد. بر خلاف گزینهٔ بستر مبادلات و ارتباطات الکترونیکی، در اینجا حاکمیت در حوزه‌هایی مداخله می‌کند که واقعاً نسبت به آنها احساس تعلق دارد و این مسئله به خوبی با ضابطهٔ متعارف بودن (Reasonableness Standard) که امروزه در اعمال ضمانت اجراهای کیفری به طور ویژه مورد توجه قرار گرفته نیز هماهنگ است (Brenner, Ibid: 29). هر چند باید اذعان کرد که این راه حل جامع نیست و بخش محدودی از مسئلهٔ فراگیر صلاحیت در این فضا را پوشش می‌دهد.

۲. شاخصهای تعیین محل ارتکاب جرائم سایبری

پیش از شروع این بحث یادآور می‌شود، به رغم لزوم تسریع تصمیم‌گیری و حل و فصل مسائل جهانی راجع به این حوزه، تاکنون هیچ اقدامی در عرصهٔ بین‌المللی صورت نگرفته است. نمونهٔ بارز آن کنوانسیون اروپایی جرائم سایبر (European Convention on Cybercrime) است که به واقع بی‌تأثیرترین ضوابط آن را مقررات راجع به صلاحیت کیفری به خود

اختصاص داده‌اند. در این زمینه، مادّهٔ ۲۲ ذیل بخش سوم (صلاحیت) از فصل دوم (اقداماتی که باید در سطح ملی انجام شود) چنین مقرر می‌دارد:

۱. هر یک از اعضا باید به گونه‌ای اقدام به وضع قوانین و دیگر تدابیر کنند که در صورت لزوم، صلاحیت رسیدگی به هر یک از جرائم مصوب مندرج در مواد ۲ تا ۱۱ این کنوانسیون را داشته باشند: الف. جرم در قلمروش ارتکاب یابد؛ یا ب. جرم در کشتی‌ای ارتکاب یابد که پرچم آن کشور برافراشته است؛ یا پ. جرم در هواپیمایی ارتکاب یابد که مطابق مقررات آن عضو به ثبت رسیده است ... .

همان‌طور که ملاحظه می‌شود، هیچ نکتهٔ مرتبطی راجع به فضای سایبر بیان نگردیده است. البته انزوای کامل این مادّه در بند ۵ آن به اوج می‌رسد که اشعار می‌دارد:

در جایی که بیش از یک عضو ادعای صلاحیت رسیدگی به جرم مقرر در این کنوانسیون را دارد، در صورت صلاحدید به شور نشسته و شایسته‌ترین عضو جهت تعقیب و پیگرد را تعیین کنند (مرکز پژوهشهای مجلس شورای اسلامی، ۱۳۸٤: ۲٦).

بدیهی است ضرورتی برای ذکر چنین مقرره‌ای نبود، زیرا در صورت بروز چنین وضعیتی، کشورها به این امر مبادرت می‌کردند.

اما بر خلاف حوزهٔ بین‌المللی و منطقه‌ای، در میان کشورها طیف متنوعی از دیدگاهها بروز یافته است. برخی مانند کشور آلمان نیازی به تصویب ضوابط جدید احساس نکرده‌اند و همان ضوابط موجود را بر مسائل مستحدثهٔ سایبری جدید تسری داده‌اند. برای مثال، در پرونده فردریک توبن، دیوان عالی فدرال آلمان (The Bundesgrerichtshof) تفسیر جالبی را ارائه داد. این تبعهٔ استرالیایی به خاطر نقض قانون جنگ جهانی دوم آلمان تحت تعقیب قرار گرفت. در این قانون، حزب نازی غیرقانونی اعلام و هر گونه تجلیل آن منع شده است. پیش از سال ۱۹۹۹، توبن از طریق پست، اعلامیه‌هایی را به آلمان ارسال کرد که در آن ارتکاب هولوکاست از سوی نازیها به کلی انکار شده بود. او همچنین همان اطلاعات را روی وب‌سایت استرالیایی قرار داد. به این ترتیب، هنگامی که در آوریل ۱۹۹۹ وارد آلمان شد، دستگیر و به خاطر تحریک تنفر نژادی (Racial Hatred) و لکه‌دار کردن حیثیت ملی محکوم شد. برای محکومیت، دادگاه رسیدگی کننده به ارسال اعلامیه‌ها از طریق پست به آلمان ترتیب اثر داد، اما اتهامات راجع به ارسال محتوا به اینترنت را نپذیرفت و رأی داد که قانون آلمان نسبت به محتوای وب‌سایت خارجی قابلیت اجرا

ندارد. هم توبن و هم مقام تعقیب تجدید نظرخواهی کردند. در این مرحله، دیوان عالی نـه تنها محکومیت توبن را به خاطر ارسال اعلامیه‌ها به آلمان تأیید کرد، بلکه نظر دادگاه بدوی را در خصوص عدم تسری قانون ضد نازی آلمان به اینترنت رد کرد. مطـابق نظـر دیـوان، واقعیت این است که محتوای تمجید کنندهٔ حزب نازی، چیزی که کـشور آلمـان در مـسیر منافع ملی خود آن را یکی از جرائم شدید تلقی می‌کند، در اینجا دسترس‌پـذیر بـود و ایـن کافی است تا دیوان عالی آلمان رأی دهد دادگاههای ایـن کـشور صـلاحیت بـه رسـیدگی دارند. به عبارت دیگر، آن‌قدر پیوند میان این فعل با قلمرو سرزمینی آلمان محکم بـوده کـه دادگاهها حق رسیدگی به آن را داشته باشند (August,op.cit: 538).

اما در خصوص کشورهایی که مبادرت به تصویب قوانین جدید کرده‌اند، به طـور کلـی می‌توان تبعیت از دو رویّهٔ کلی را ملاحظه کرد: ۱. محـل اسـتقرار سیـستمهای رایانـه‌ای؛ و ۲. محل حضور بارگذار و پیاده‌ساز شبکه‌ای.

۲ـ۱. محل استقرار سیستمهای رایانه‌ای به عنوان محل ارتکاب جرائم سایبری

منظور از سیستم رایانه‌ای تنها رایانه‌های شخصی یا مستقل نیستند، هر چند مثال بارز آن را شامل می‌شوند و باید مفهوم موسع آنها را مورد توجه قرار داد. بر این اساس، کنوانسیون جرائم سایبر در تعریفی از این سیستمها اشعار می‌دارد:

> مادّهٔ ۱. تعاریف: در راستای اهداف این کنوانـسیون: الـف ـ منظـور از «سیـستم رایانـه‌ای» (computer system)، هر دستگاه یا مجموعه‌ای از دستگاههای مرتبط یا متصل به هـم اسـت که یک یا چند تا از آنها مطابق یک برنامه، پردازش خودکار داده‌ها را انجام می‌دهد (مرکـز پژوهشهای مجلس شورای اسلامی، ۱۳۸٤: ۱٦).

اما از لحاظ نحوهٔ انعکاس این ضابطه در قوانین و مقررات ملی، صرف نظر از رویکـرد عامی که برخی کشورها، به ویژه کشورهای تابع نظام رومی ـ ژرمنی، اتخاذ کـرده‌انـد و در فوق به کشور آلمان اشاره شد، بررسی قوانین کشورهای جنوب شرق آسیا، مانند سـنگاپور به عنوان یکی از کشورهای اتخاذ کننده رویکرد موسع، جالب توجه است. مطابق مـادّهٔ ۱۰ قانون سوء استفاده کامپیوتری سنگاپور:[*]

۱. هر شخصی که در ارتکاب جرائم مندرج در این قانون معاونت یـا شـروع بـه ارتکـاب

---

* Art. 10 Singapore Computer Misuse Act.

نماید یا مقدمات آن را انجام دهد یا در مسیر ارتکاب آن عمل کند، مجرم شناخته و به مجازات مقرر محکوم خواهد شد؛ ۲. در خصوص جرائمی که مطابق این بخش ارتکاب می‌یابند، محل ارتکاب هیچ تأثیری ندارد.

این کشور با نفی هر گونه موقعیت فیزیکی و توجه کامل به ماهیت فضای سایبر، محل وقوع این جرائم در دنیای فیزیکی را به کلی نادیده گرفته است. به این ترتیب، فقط کافی است یک ویروس رایانه‌ای یا هرزه‌نگاری کودک در فضای سایبر منتشر شود تا محاکم سنگاپور صالح به رسیدگی گردند.

اما نکتهٔ اصلی در مادهٔ ۱۱ این قانون آمده است:

حوزهٔ قلمرو جرائم مطابق این قانون عبارت است از: ۱. مطابق زیربخش دو، مقررات این قانون در خصوص هر شخص، چه تابعیت یا شهروندی سنگاپور را داشته چه نداشته باشد و چه در داخل چه خارج از این کشور حضور داشته باشد، قابل اجرا خواهد بود. ۲. در جایی که جرم مطابق این قانون توسط هر شخص در هر محل خارج از این کشور ارتکاب می‌یابد، فرض بر این است که وی جرم را در داخل سنگاپور مرتکب شده است. ۳. در جهت اهداف این بخش، این قانون نسبت به جرائم زیر نیز قابل اجرا خواهد بود: الف. متهم در مدت مقتضی در سنگاپور باشد؛ ب. کامپیوتر، برنامه یا داده‌ها در مدت مقتضی در سنگاپور باشد (Brenner, op.cit: 21).

اما کشور مالزی، در مادهٔ ۹ قانون جرائم رایانه‌ای خود* رویکردی نسبتاً محدودتر را اتخاذ کرده است:

۱. مقررات این قانون نسبت به هر شخص، چه تابعیت یا شهروندی مالزی را داشته چه نداشته باشد، نسبت به داخل و خارج از این کشور قابل اجرا خواهد بود. در جایی که جرم مندرج در این قانون توسط هر شخص در هر مکان خارج از مالزی ارتکاب یابد، با وی به مثابهٔ ارتکاب جرم در مالزی برخورد خواهد شد. ۲. در جهت اهداف زیربخش یک، این قانون در صورتی اجرا خواهد شد که کامپیوتر، برنامه یا داده‌های واقع در مالزی در ارتکاب جرم نقش داشته باشند یا اینکه بتوان در مهلت مقتضی از طریق یک کامپیوتر در مالزی به آنها متصل شد یا آنها را ارسال یا از آنها استفاده کرد (Ibid: 16).

* Malaysia Computer Crimes Act.

۲ـ۲. محل حضور بارگذار و پیاده‌ساز شبکه‌ای به عنوان محل ارتکاب جرائم سایبری

به طور کلی، کنشگران اصلی فضای سایبر از دو حالت اصلی خارج نیستند: یا داده‌ها را در آن می‌گنجانند که در این صورت به آنها بارگذار (Uploader) می‌گویند و یا اینکه داده‌ها را از این فضا دریافت می‌کنند که به آنها پیاده‌ساز (Downloader) گفته می‌شود. در اینجا بارگذار، اطلاعات مورد نظر خود را در فضای تخصیص یافته از سوی خدمات میزبانی قرار می‌دهد تا متعاقباً پیاده‌ساز به آنها دسترس یابد. هیچ نیازی نیست که آنها از هویت یکدیگر آگاهی داشته باشند، لذا نباید آنها را با فرستنده (Sender) و گیرنده (Receiver) که معمولاً هویتشان در ارتباطات الکترونیکی معلوم است اشتباه گرفت. زیرا در اینجا آن هدف خاص از مبادلهٔ اطلاعات که در ارتباطات طرفینی وجود دارد مشاهده نمی‌شود (Xingan, op.cit: 29).

با این حال، نباید ضابطهٔ بارگذار و پیاده‌ساز را بر روی بزهکار و بزهدیده پیاده کرد. همان‌قدر که احتمال دارد بارگذار مرتکب جرم باشد، بزهدیده بودن آن دور از انتظار نیست. برای مثال، در جایی که بارگذار محتوای مجرمانه‌ای را نظیر تصاویر وقیح، هتک حرمت یا توهین یا حتی ویروس خطرناک بر روی شبکه قرار می‌دهد، وی مرتکب جرم است. اما هنگامی که داده‌های مشروعی که بارگذاری کرده، به طور غیرمجاز توسط یک پیاده‌ساز مورد سوء استفاده قرار می‌گیرد، بزهدیده است. همچنین هنگامی که یک پیاده‌ساز ویروس زیانباری را دریافت می‌کند، بزهدیدهٔ جرم نشر ویروس محسوب می‌شود، اما هنگامی که تصاویر غیرمجازی مانند هرزه‌نگاری کودکان را دریافت می‌کند، مطابق قوانین بسیاری از کشورها مرتکب جرم است و این ربطی به فعل بارگذار ندارد.

اما در خصوص انعکاس این ضابطه در میان کشورها، شایان ذکر است در میان ایالتهای امریکا می‌توان نمونه‌هایی از آن را یافت. برای مثال، قانون جرائم رایانه‌ای آرکانزاس* مقرر کرده است: «چه ارتباطات رایانه‌ای از این ایالت نشأت گیرد و چه به آن ختم گردد، مراجع قضایی این ایالت صالح به رسیدگی خواهند بود.» همچنین ایالت کارولینای شمالی** مقرر داشته است: «جرائم ارتکابی از طریق ارتباطات الکترونیکی، چه از این ایالت ارسال و چه در آن دریافت شده باشد، ارتکاب یافته در این ایالت تلقی خواهد شد» (Brenner, op.cit: 11).

* Ark. Code Ann. Sec 5-27-606 (2003).

** N.C. Gen. Stat. Sec 14-453.2 (2002).

فصل دوم. صلاحیت فراسرزمینی و فضای سایبر

در این فصل نکات راجع به ضوابط صلاحیت فراسرزمینی مطرح می‌گردد. در اینجا با توجه به ماهیت فراسرزمینی این فضا اقبال بیشتری در مورد به کارگیری این ضوابط ایجاد شده و از آن حالت استثنا و انزوای دنیای فیزیکی خارج شده‌اند.

بر این اساس، مطالب این فصل در سه گفتار مطرح خواهند شد و به ترتیب، صلاحیتهای فراسرزمینی تابعیتی، حمایتی (واقعی) و جهانی مورد بررسی قرار خواهند گرفت.

گفتار اول: صلاحیت تابعیتی

هنگامی که قانونگذار کیفری به جای تأکید بر قلمرو سرزمینی اعتباری‌ای که مطابق قوانین و معاهدات بین‌المللی به رسمیت شناخته شده است، اتباعش را هدف قرار می‌دهد، دیگر تفاوتی نمی‌کند آن فعل سرزنش‌آمیزِ جرم‌انگاری شده، در کدام نقطه از کرهٔ خاکی ارتکاب یابد. شایان ذکر است، این اصل بیشتر از جانب کشورهای تابع نظام حقوق رومی ـ ژرمنی یا نوشته مورد توجه قرار گرفته است (European Committee on Crime Problems, op.cit: 10). اما به هنگام اعمال آن در مجموعهٔ قوانین جزایی، کم و بیش یک مقررهٔ مهم تکمیلی را هم در کنار آن قید کرده‌اند و آن اینکه کشور محل ارتکاب نیز آن را جرم‌انگاری کرده باشد یا اینکه نتواند نسبت به آن اعمال صلاحیت کیفری کند. برای مثال، کد کیفری آلمان مقررهٔ مشابهی را دارد. اما کشور هلند این مقررهٔ تکمیلی را منحصر به جنایات (Felony) دانسته و جنحه‌ها (Misdemeanor) را مستثنا کرده است (Brenner, op.cit: 24).

همچنین، گاهی اوقات، قانونگذار کیفری تصمیم می‌گیرد برای اجرای شایستهٔ عدالت، حوزهٔ صلاحیت تابعیتی کیفری را به بزهدیدگان نیز تسری دهد. اما از آنجا که این اقدام چندان با اقبال مواجه نشده است، از آن به صلاحیت تابعیتی منفعل (Passive Nationality Jurisdiction) یاد می‌شود که در مقابل صلاحیت تابعیتی فعال (Active Nationality Jurisdiction) که نسبت به مرتکبان جرائم مصداق دارد قرار می‌گیرد. هر چند در مورد برخی جرائم که وجدان جامعه را تحریک می‌کند و جریحه‌دار می‌سازد یا اینکه تعداد زیادی از شهروندان از جرم ارتکابی متضرر می‌شوند و در واقع یک مطالبهٔ ملی برای برخورد با مرتکب جرم شکل می‌گیرد، اعمال این نوع صلاحیت نه تنها غیرمنطقی و نامتعارف نخواهد بود، بلکه ضروری و اجتناب‌ناپذیر است (Xingan, op.cit: 17).

با این حال، قرن اخیر، علاوه بر افراد، شاهد تکاپوی خیل عظیم شخصیتهای جدیدی به نام اشخاص حقوقی بوده که به طور روزافزونی سیطرهٔ آنها بـر امـور خـرد و کـلان بیـشتر می‌شود. صرف نظر از ماهیت و هویت این اشخاص و اینکه مستقل از افراد مؤسس خود یا وابسته به آنها هستند، در این مسئله تردیدی وجود ندارد که بایـد تحـت ضـوابط حقـوقی خاصی قرار گیرند و حتی آنهایی که هویت و موجودیت تبعی برای این گروه از اشـخاص قائل‌اند، اذعان دارند که باید برای آنها ضوابط لازم‌الاجرای قـانونی متمـایزی حتـی در حوزهٔ کیفری تدوین کرد. این حرکت جدی را به خوبی می‌توان در اسـناد بـین‌المللـی کیفری مشاهده کـرد. از جملـه کنوانـسیونهای ملـل متحـد بـرای مبـارزه بـا جنایـات سازمان‌یافتهٔ فراملی (پالرمو، ۲۰۰۱) و مبارزه با فـساد (مریـدا، ۲۰۰۳) کـه صـراحتاً از دول عضو خواسته‌اند به تصویب قوانین کیفری دربرگیرندهٔ این اشـخاص اقـدام کننـد (United Nations Office on Drugs and Crime, 2004: 24). حتی با وجود نوپا بـودن جرائم سایبر، در اولین سند رسمی منطقه‌ای با ماهیت بین‌المللی کنوانسیون جرائم سایبر نیز به آن پرداخته شده است. در مادّهٔ ۱۲ این کنوانسیون آمده است:

مادّهٔ ۱۲. مسئولیت اشخاص حقوقی: ۱. هر یک از اعضا باید بـه گونـه‌ای اقـدام بـه وضـع قوانین و دیگر تدابیر کنند که در صورت لزوم اطمینان دهند چنانچه اشـخاص حقـوقی در راستای منافع خود مرتکب جرائم مصوب ایـن کنوانـسیون شـدند، آنهـا را تحـت تعقیـب کیفری قرار خواهند داد. این جرائم توسط یک شخص حقیقـی کـه شخـصاً یـا بـه عنـوان بخشی از ارگان شخص حقوقی فعالیت می‌کند و مدیریت آن را به عهده دارد و اختیـارات ذیل را داراست ارتکاب مـی‌یابـد: الـف. اختیـار نماینـدگی شـخص حقـوقی؛ ب. اختیـار تصمیم‌گیری از جانب شخص حقـوقی؛ پ. اختیـار اعمـال نظـارت بـر شـخص حقـوقی. ۲. علاوه بر موارد مذکور در بند یک، اعضا باید تدابیری وضع کنند کـه در صـورت لـزوم اطمینان دهند در جایی که خلأ سرپرستی یا نظارت شـخص حقیقـی منـدرج در بنـد یـک وجود دارد و این امکان فراهم آمده که جرائم مصوب این کنوانسیون را شخص حقیقی دیگری بر اساس اختیارات خود و در راستای منافع آن مجموعه مرتکب شود، امکان اعمال مـسئولیت بر آن مجموعه همچنان وجود دارد.۳. با توجه به اصول قانونی حاکم بر اعضا، اتصاف مسئولیت شخص حقوقی می‌تواند به صورت کیفری، مدنی یا اداری باشد. ٤. اعمال این‌گونه مـسئولیتها بر شخص حقوقی نباید موجب تحت‌الشعاع قرار گرفتن مسئولیت اشخاص حقیقی مرتکب این جرائم شود (مرکز پژوهشهای مجلس شورای اسلامی، ١٣٨٤: ١٢).

اما آنچه راجع به فضای سایبر در مورد صلاحیت تابعیتی به طور خاص جلوه‌گر شده است، مطرح ساختن آن به عنوان فضای چهارم بین‌المللی است. به طور کلی، مطابق نظریهٔ فضاهای بین‌المللی (The Theory of International Spaces)، تابعیت و نه قلمرو سرزمینی، مبنای صلاحیت در مفهوم عام (صلاحیت تقنینی، قضایی و اجرایی) در فضای ماورای جو (Outer Space)، قطب جنوب (Antarctica) و دریاهای بزرگ (High Seas) است (Menthe, op.cit: 83).

این پیش‌فرض کلی را باید به همراه ملاحظاتی مورد توجه قرار داد. در فضای ماورای جو، تابعیت محل ثبت سفینه، چه همراه آن کسی باشد چه نباشد، ملاک عمل محسوب می‌شود. در قطب جنوب، تابعیت پایگاه و در دریاهای آزاد نیز تابعیت کشتی، یعنی قانون پرچم، تعیین کننده است. در فصل اول ملاحظه شد برای توجیه این نوع صلاحیت، آن را جزیرهٔ شناوری از قلمرو سرزمینی می‌دانند که به طور مستمر از آن جدا می‌شود و مجدداً به آن می‌پیوندد. هر چند برخی مراجع در اتصاف قلمرو سرزمینی به آنها اشکال کرده‌اند. برای مثال، دیوان عالی ایالات متحده، تفسیری مغایر آن را ارائه داده و بر این نکته تأکید کرده که «گام گذاشتن به کشتی یا هواپیمای صاحب پرچم ایالات متحده، با ورود به این کشور یکسان نیست» (Ibid: 84).

اما در خصوص فضای سایبر، باید دید تا چه اندازه می‌توان از نظریه‌پردازیها و رویه‌های حقوقی سه فضای فوق، یعنی فضای ماورا، قطب جنوب و دریاهای بزرگ بهره‌برداری کرد. البته یک تفاوت اصلی میان آنها و فضای سایبر وجود دارد و آن این است که آنها ماهیت فیزیکی دارند. البته این ویژگی تنها یکی از ابعاد قابل ذکر برای این فضاهاست. حتی میان این سه حوزهٔ فیزیکی نیز تفاوتهای بسیاری وجود دارد، چرا که یکی اقیانوس، دیگری قاره و آخری آسمان است. در واقع آنچه میان آنها وجه اشتراک محسوب می‌شود، فیزیکی بودنشان نیست، بلکه بین‌المللی بودنشان به مفهوم بدون حاکمیت بودنشان (Sovereignless) است. به همین دلیل است که می‌توان میان آنها و فضای سایبر ارتباط برقرار کرد (Ibid: 85).

به این ترتیب، ارائه دهندگان این نظریه نیز تلاش کرده‌اند با اتخاذ یک دیدگاه واقع‌بینانه بحث فضای سایبر را در چارچوب کاملاً متمایزی مورد توجه قرار دهند. البته باید

خاطرنشان کرد با اینکه به نظر آنها این چهار فضا در بی‌حاکمیت بودن وجه اشتراک دارند، اما با توجه به توضیحاتی که در بخش قبل راجع به مفهوم قلمرو سرزمینی سایبری بیان و ملاحظه شد، کشورها حتی و به ویژه کشورهای در حال توسعه که این فناوری را مرهون کشورهای توسعه‌یافته به ویژه ایالات متحده هستند، راجع به نحوهٔ راهبری ارکان آن بحثهای جدی‌ای را مطرح کرده‌اند که بی‌تردید اگر با حوزهٔ حاکمیتشان تداخل نداشت، این‌گونه وارد میدان نمی‌شدند، در حالی که در مورد قطب جنوب و فضای ماورای جو چنین جبهه‌گیری‌ای صورت نگرفته، زیرا نیازی احساس نشده است.

اولین عقبگرد پیشگامان این نظریه، راجع به فرایند ثبت در فضای سایبر است. آنها اذعان دارند این فرایند قابل اجرا نیست، هرچند الزام به ثبت تابعیتی تمامی فایلها و پیامها به موجب معاهدات بین‌المللی نشدنی نیست. اما تا آن زمان، باید مطابق قواعد و وضعیت موجود عمل کرد. اشخاص در فضای بین‌المللی سایبر از طریق افعالشان هویت می‌یابند. یک بارگذار صفحهٔ خودش را با تابعیتش ممهور می‌کند. ممکن است موقعیت یک صفحهٔ وب معلوم نباشد، اما مسئول آن مشخص است. تابعیت موضوعات در فضای سایبر را می‌توان از روی تابعیت شخص یا مجموعه‌ای که آنها را قرار داده یا حتی کنترل کنندهٔ آنها، یعنی متصدی شبکه‌های (System Operator) مربوط شناسایی کرد (Ibid: 93).

به نظر می‌رسد این تحلیل برای ساماندهی صفحات وب پاسخگو باشد. عموماً شناسایی تابعیت یک صفحهٔ وب مشکل نیست و معمولاً نام ایجاد کنندهٔ آن در خود صفحه درج شده که یک فرد یا سازمان است. اما آنچه در اینجا اهمیت می‌یابد، وضعیت افراد یا سازمانهایی است که چنین صفحاتی را برای دیگران ایجاد می‌کنند و در واقع بسیار اتفاق می‌افتد که مالکان واقعی سایتها، حتی در جریان بارگذاری محتوای مورد نظرشان نیستند و کلیهٔ امور توسط متخصصان فنی و حرفه‌ای مربوط انجام می‌شود. لذا هنگامی که می‌خواهیم بر روی فاعل یک وب‌سایت متمرکز شویم تا بر اساس آن صلاحیت تابعیتی را پیاده کنیم، اول سؤالی که باید به طور صحیح به آن پاسخ دهیم این است که مالک واقعی وب‌سایت چه کسی است. آیا ایجاد کنندهٔ محتوا و ساختار وب‌سایت است، یا پشتیبان مالی و سفارش دهندهٔ آن یا در نهایت کسی که بارگذاری می‌کند یا حتی متصدی سرور و پشتیبان فنی آن؟

به هر حال، هر یک از اینها نقش تعیین کننده‌ای در دسترس‌پذیر کردن محتوای یک وب‌سایت دارند و به راحتی می‌توان به آنها به مثابهٔ یک فاعل نگریست و بالتبع قواعد

صلاحیت تابعیتی را اعمال کرد. هرچند باید دید این قاعده تا چه اندازه قابل اجراست. به طور حتم، ابداع کنندگان این نظریه به هدفی که از محدود کردن حوزهٔ تعارضات صلاحیت با انتقال آن از سرزمین به تابعیت اشخاص دنبال می‌کردند نائل شده‌اند، اما باز هم واقعیات فنی و اجرایی حاکم بر این فضا به گونه‌ای است که معضلات جدی همچنان پابرجاست. مضافاً اینکه وب‌سایتها حداکثر یک پنجم فضای سایبر را اشغال می‌کنند و این قاعده، بر فرض قبول، تنها برای گسترهٔ محدودی راهگشاست.

از سوی دیگر، نکات راجع به پیوندها (Links) نیز مطرح است. شخصی که یک پیوند ایجاد می‌کند، نسبت به محتوایی که دسترس‌پذیر می‌سازد، موضوع قوانین لازم‌الاجرای کشورش خواهد بود. همچنین اشخاص موضوع صلاحیت سرزمینی که از آنجا بارگذاری را انجام می‌دهند هم قرار می‌گیرند که بدیهی است یکی از آنها ایجاد پیوند است. همچنین دنبال کنندهٔ پیوندها کسی جز پیاده‌ساز نیست و بالطبع موضوع صلاحیت محل استقرار سیستم رایانه‌ایش قرار می‌گیرد، هر چند از قوانین حاکم بر تابعیتش هم گریزی ندارد.

تمامی این مسائل پیچیده باعث شده در اینجا نیز نویسندگان کنوانسیون جرائم سایبر کاملاً موضوع را مسکوت بگذارند. قسمت ت از بند ۱ مادهٔ ۲۲ کنوانسیون جرائم سایبر بر لزوم اعمال صلاحیت کشورها بر اتباعشان، البته فقط مرتکبان جرائم، تأکید کرده است:

> مادهٔ ۲۲. صلاحیت: ۱. هر یک از اعضا باید به گونه‌ای اقدام به وضع قوانین و دیگر تدابیر کنند که در صورت لزوم، صلاحیت رسیدگی به هر یک از جرائم مصوب مندرج در مواد ۲ تا ۱۱ این کنوانسیون را داشته باشند ... ت. در جایی که جرم مورد نظر مطابق قوانین جزایی قابل مجازات شناخته شده، توسط تبعه‌اش ارتکاب یافته ... باشد (مرکز پژوهشهای مجلس شورای اسلامی، ۱۳۸٤: ۲٦).

اما در سطح قوانین ملی، تحرکاتی به چشم می‌خورد. در این میان، همانند صلاحیت سرزمینی، بعضی کشورها خود را مستغنی از وضع قوانین جدید دانسته‌اند، اما بعضی دیگر حداقل در خصوص جرائم خاصی به حوزهٔ سایبر نیز وارد شده‌اند. از گروه اول، کشور آلمان اعمال صلاحیت کیفری علیه اتباع خود را مشروط به قابل مجازات بودن فعل مورد نظر در محل ارتکاب یا اینکه تحت شمول هیچ حوزهٔ صلاحیت کیفری قرار نگیرد دانسته است.* البته کشور بلژیک تا حدی پا را فراتر نهاده و اجازهٔ تعقیب اتباع خارجی‌ای

* Sec. 7 Nr (2)(1) StGB. Strafgeseztbuch (German CC).

را که در ارتکاب جرم اتباع بلژیکی در خارج از این کشور معاونت کرده‌اند نیز می‌دهد. اما دولت هلند، علاوه بر قواعد عام صلاحیتی خود، جهت اعمال صلاحیت تابعیتی بر مجرمان سایبر، قواعد خاصی نیز وضع کرده است. برای مثال، چنانچه جعل رایانه‌ای توسط کارمندان دولت یا کارمندان سازمانهای بین‌المللی مستقر در هلند در خارج از این کشور ارتکاب یابد، در هلند قابل تعقیب کیفری هستند. البته به شرطی که قواعد حاکم بر مجرمیت متقابل (Double Criminality) رعایت شده باشد.* همچنین چنانچه اتباع هلند با دسترس به یک کامپیوتر، اسرار شرکتی یا هرزه‌نگاری کودکان را منتشر کنند، طبق قانون این کشور قابل محاکمه خواهد بود. البته همان‌طور که پیش از این اشاره شد، قانونگذار هلند مقرر کرده حتی اگر پس از ارتکاب جرم، مجرم تابعیت هلندی اخذ کند، باز هم محاکم این کشور صالح به رسیدگی خواهند بود** (Brenner, op.cit: 24).

اما در خصوص صلاحیت تابعیتی منفعل، دولت آلمان بر اساس همان قواعد عام خود مقرر کرده اگر جرمی علیه اتباع آلمان ارتکاب یابد، چنانچه در محل ارتکاب قابل مجازات باشد یا اینکه تحت صلاحیت هیچ مرجعی قرار نگیرد، مراجع آلمان صالح به رسیدگی خواهند بود.*** در بلژیک نیز ارتکاب جرم علیه یک بلژیکی به محاکم این کشور حق صلاحیت اعطا می‌کند، مشروط به اینکه فعل ارتکابی در کشور محل ارتکاب، جرم شناخته شده و مجازات مقرر برای آن حداقل پنج سال حبس باشد. کشور هلند نیز در خصوص دو جرم سایبری مهم، یعنی خرابکاری کامپیوتری (Computer Sabotage) و تخریب داده‌ها (Data Damage)، برای بزهدیدگان خود صلاحیت قائل شده است؛**** مشروط به اینکه فعل ارتکابی تحت شمول مادهٔ ۲ کنوانسیون بین‌المللی مقابله با بمب‌گذاری تروریستی (International Convention for the Suppression of Terrorist Bombings (15 Dec 1997)) یا مادهٔ ۲ کنوانسیون بین‌المللی مقابله با تأمین مالی تروریسم (International Convention for the Suppression of the Financing of Terrorism (9 Dec 1999)) قرار گیرد (Ibid: 25).

* Art. 4(11) jo. 225 (Dutch CC).

** Art. 5(2) (Dutch CC).

*** Sec. 7 Nr. (2)(1) StGB.

**** Art. 4(13) & Art. 4(14) jo (Dutch CC).

در ایالات متحده نیز این رویکرد تنها در جایی پیاده شده که بزهدیده خود دولت باشد. بخش 1030(a)(3) عنوان هجدهم قانون فدرال که جرائم سایبر را در خود جای داده، مقرر کرده چنانچه هر شخص عالماً و بدون مجوز به کامپیوتر غیرعمومی (Nonpublic Computer) یک نهاد یا عامل ایالات متحده دسترس یابد، قابل پیگرد خواهد بود. همچنین در قسمت (a)(6)(B) همین بخش، قاچاق متقلبانهٔ عمدی و آگاهانهٔ هر گونه گذرواژه‌ای (Traffic In Password) که امکان دسترس به کامپیوتر مورد استفاده توسط یا برای دولت ایالات متحده را فراهم می‌آورد، مشمول این قانون قرار گرفته است. شایان ذکر است بسیاری از ایالات امریکا به تبع این قانون مقررات مشابهی را وضع کرده‌اند (Ibid: 25). برای مثال، ایالت میشیگان در مجموعهٔ قوانین کامپیوتری خود آورده هر گاه قربانی جرم یا کارمند یا عامل واحد دولتی به عنوان قربانی جرم در این ایالت ساکن باشد یا در زمان وقوع جرم در این ایالت حاضر باشد، محاکم آن صالح به رسیدگی خواهند بود.*

گفتار دوم: صلاحیت حمایتی (واقعی)

کشورهای تابع نظام حقوق نوشته برای اعمال صلاحیت کیفری خود به قاعدهٔ دیگری نیز متوسل می‌شوند و آن در جایی است که یک فعل مجرمانه امنیت و منافع ملی کشور را تهدید کند (Protective Principle). البته این سخن به این معنا نیست که کشورهای تابع نظام حقوق عرفی به آن متوسل نشوند، اما میزان اتکا متفاوت است. به هر حال، این اصل در جایی نظر قانونگذار کیفری را به خود جلب می‌کند که قربانی فعل مجرمانه، دولت یا حتی خود حاکمیت باشد (August, op.cit: 540).

اما نکتهٔ قابل توجه این است که بر خلاف صلاحیت جهانی که در گفتار بعد به آن اشاره خواهد شد، هیچ وحدت ملاکی برای جرم‌انگاری وجود ندارد و هر کشور می‌تواند متناسب با سیاستها و خط‌مشیهای خرد و کلانی که دنبال می‌کند، طیفی از اقدامات را مغایر با امنیت و منافع ملی تلقی کند. برای مثال، در دعوای ایالات متحده علیه رودریگز،** متهمان به ارتکاب اظهارات خلاف واقع به هنگام درخواست مهاجرت در

* Mich. Comp. Laws Sec. 762.2(1)(d) (2004).

** United States v. Rodriguez (1960).

خارج از ایالات متحده محکوم شدند. به این ترتیب، در رویّهٔ قضایی آمریکا ثبت شد که جرائمی از این قبیل جهت مهاجرت به امریکا، مغایر با امنیت و منافع ملی این کشور است (Menthe, op.cit: 72). در کشور آلمان نیز، اگر جرائم در فراسوی مرزها توسط هر شخص علیه امنیت یا اقتصاد ملی ارتکاب یابد، دادگاههای این کشور صالح به رسیدگی خواهند بود. در فرانسه نیز اعمالی از قبیل جعل اسکناس رایج کشور یا خدشه‌دار کردن امنیت دولت، حتی اگر در خارج از مرزهای فرانسه رخ داده باشد، به دادگاههای این کشور صلاحیت لازم را اعطا می‌کند (میر محمدصادقی، همان: ۲۹).

در هر حال، همان‌طور که ملاحظه می‌شود، به لحاظ اهمیت این مسئله در قوانین کشورها، دیگر نه محل ارتکاب فعل و نه تابعیت مرتکب مورد توجه قرار گرفته است و هر کس در هر جای دنیا چنین اعمالی را مرتکب شود، تحت شمول قوانین جزایی کشور بزهدیده قرار خواهد گرفت. لذا نتیجه‌ای که می‌توان از این رویکرد حاکمیتی گرفت این است که در اینجا بار اصلی بر دوش قانونگذاران است و محاکم همانند دو اصل سرزمینی و تابعیتی ملزم نیستند در اعمال آن، ضوابط قانونی و اجرایی بسیاری را مورد بررسی و تجزیه و تحلیل قرار دهند. در اینجا فقط باید به مُرّ قانون عمل کرد، فارغ از اینکه چه شخصی و با چه هویتی و در چه محلی مرتکب چنین جرائمی شده است (August, op.cit: 542).

با این حال، اگر قانونگذار کیفری بنا به دلایلی به ذکر کلیات در قانون جزا اکتفا کند، که البته اگر از حدود خود خارج شود و ناقض اصول مسلّم حقوق جزا باشد فاقد اعتبار و مشروعیت خواهد بود، این مهم به عهدهٔ مراجع کیفری است که با ارائهٔ تفسیری صحیح و منطقی از آنها، از یک سو حمایت مدبرانه و قانونمندی از امنیت و منافع ملی به عمل آورند و از سوی دیگر خود را درگیر مسائل غیرضروری ننمایند، به ویژه آنکه این اصل، مرتبه و جایگاه ضعیف‌تری نسبت به صلاحیت سرزمینی و تابعیتی دارد.

اما در خصوص فضای سایبر باید دید آیا محملی برای اعمال این نوع صلاحیت وجود دارد. برای پاسخ به این سؤال، باید موضوعی را یافت که بتواند تحت شمول چنین حمایتی قرار گیرد. در مقدمه به دگردیسی الکترونیکی جهانی و ورود اکثریت قریب به اتفاق امور خرد و کلان به فضای سایبر اشاره شد. در این میان، تحقق دولت الکترونیکی یکی از اولویتهای اصلی کشورها در ورود به هزارهٔ نوین محسوب می‌شود. لذا به نظر نمی‌رسد این

سخن ناصحیح باشد که از این پس تجلی امنیت و منافع ملی را باید در فضای سایبر جست‌وجو کرد. آیا به خطر افتادن امنیت زیرساختهای حیاتی از این واضح‌تر که اگر اطلاعات موجود در سیستم کنترل برق کشور دستکاری یا حذف شود، خسارات احتمالی آن ممکن است از حمله به یکی از نیروگاههای بزرگ بیشتر باشد؟ یا در فرایند بانکداری الکترونیکی، آیا از کار انداختن برنامه‌های شبکه‌ای یک بانک یا از آن مهم‌تر تخریب یا سرقت اطلاعات واجد ارزش مالی متعلق به صاحبان حساب، نمی‌تواند منافع کشور را در معرض خطر قرار دهد؟

این مثالها و دهها نمونهٔ دیگر، همگی به خوبی نشان می‌دهند منافع و امنیت ملی کشورها تا چه حد با این فضا گره خورده و این در حالی است که آسیب‌پذیری آنها به طور قابل توجهی افزایش یافته است. این فضا و به تبع آن هر آنچه در خود جای داده برای تمامی جهانیان دسترس‌پذیر است که این به معنای خطرپذیری حداکثری خواهد بود. زیرا اگر تا به حال زیرساختهای حیاتی و دیگر امور موضوع و مربوط به امنیت و منافع ملی در معرض تهدیدات محیطی قرار داشتند، اکنون با برداشته شدن تمامی موانع و محدودیتها از یک سو و در دسترس بودن بهترین ابزارهای تعرض با کاربرد آسان از سوی دیگر و از همه مهم‌تر، دور بودن از مجریان قانون بهترین شرایط را مهیا کرده است. در این میان، به نظر می‌رسد تهدیدات تروریستی موضوعیت خاصی داشته باشند. این فضا چه در مفهوم خاص آن، که زیرساختهای این فضا را هدف قرار می‌دهند و چه از لحاظ بهره‌برداریهای رسانه‌ای که به نوبهٔ خود رگ حیات تروریستها محسوب می‌شود، آن‌قدر مطلوبیتهای منحصر به فرد دارد که آنها را بر آن داشته هرچه زودتر از دنیای فیزیکی به این فضا کوچ کنند (جلالی فراهانی: ۱۳۸۵).

گفتار سوم: صلاحیت جهانی

گروهی از افعال هستند که فارغ از هر چیز، برای حمایت از جامعهٔ ملل و برای اینکه یک اقدام سرزنش‌آمیز جهانی محسوب می‌شوند، از سوی قانونگذاران کیفری مورد توجه قرار گرفته‌اند. البته این نکته به این معنا نیست که چنین افعالی در قوانین داخلی جرم‌انگاری شوند، بلکه تنها جایی است که می‌توان گفت جرم‌انگاری از حوزهٔ حاکمیت و قلمرو سرزمینی کشورها فراتر رفته و در واقع این مهم را حقوق بین‌المللی به عهده گرفته

است. لذا پرواضح است که به موارد بسیار خاصی محدود می‌شود که اجماع جهانی در مورد آنها شکل گرفته است. از جمله نمونه‌های بارز می‌توان به برده‌داری، جنایات جنگی، جنایات علیه بشریت، نسل‌کشی، نژادپرستی، هواپیماربایی و گروگان‌گیری اشاره کرد (Law Reform Commission of Canada, op.cit: 154).

البته طی سالهای اخیر کنوانسیونهای بین‌المللی متعددی از سوی اکثریت کشورها به تصویب رسیده که نشانهٔ شکل‌گیری یک عزم جهانی جدی برای مبارزه با برخی پدیده‌های شوم است. از مهم‌ترین آنها می‌توان به کنوانسیون مواد مخدر و روانگردان در سال ۱۹۸۸، کنوانسیون ملل متحد برای مبارزه با فساد و کنوانسیون ملل متحد برای مبارزه با جنایات سازمان‌یافتهٔ فراملی اشاره کرد که بسیاری از کشورها آن را امضا کرده‌اند.

همچنین، در سال ۱۹۹۶، کمیسیون حقوق بین‌الملل، پیش‌نویس قانون (کُد) کیفری جنایات علیه صلح و امنیت بشری را تهیه کرده و در آن طیف وسیعی از جنایات علیه بشریت را تحت شمول قرار داده که ملاحظه می‌شود طی سالهای اخیر برای بسیاری از آنها اسناد بین‌المللی خاصی به تصویب رسیده است. این جنایات عبارت‌اند از: قتل عمد، نابودی، برده‌کشی، شکنجه، زجر و آزار شدید (به دلایل سیاسی، نژادی، مذهبی یا قومیتی)، تجاوز به عنف، روسپی‌گری اجباری و سوء استفادهٔ جنسی، در جایی که به شکل نظام‌مند یا گسترده انجام می‌شود و از سوی یک دولت یا سازمان یا گروه پشتیبانی یا هدایت می‌شود. در خصوص جنایات جنگی نیز علاوه بر موارد فوق اقدامات تروریستی نیز تحت شمول قرار گرفته است (August, op.cit: 542).

البته برخی کشورها نیز رأساً مبادرت به جرم‌انگاریهای بعضاً موسعی در این حوزه کرده‌اند که در این میان موارد مذکور در قانون مجازات عمومی آلمان قابل توجه است: جرائم مربوط به انرژی هسته‌ای، مواد منفجره و رادیو اکتیو؛ حمله به هواپیما؛ تشویق به فحشا؛ دست داشتن در معاملات مواد مخدر؛ هرزه‌نگاری و جعل (میر محمدصادقی، همان: ۲۹).

در هر حال، همانند صلاحیت حمایتی، تنها وظیفهٔ محاکم این است که تابع قانون جزای ماهوی باشند و البته رویّهٔ حاکم بر حقوق بین‌الملل را نیز مورد عنایت قرار دهند. زیرا این جرائم ماهیتی جهانی و بین‌المللی دارند و به نظر نمی‌رسد استناد به رویّهٔ قضایی دیگر کشورها برای اعمال صلاحیت خالی از وجههٔ قانونی باشد و می‌تواند اعتبار آن را نیز تقویت کند.

اما در خصوص میزان کاربرد این اصل در رسیدگی به جرائم ارتکابی به فضای سایبر، با وجود اینکه صراحتاً بر استثنا بودن آن تأکید و تصریح شده و می‌شود، اما به نظر می‌رسد زندگی اجتناب‌ناپذیر در این فضای مشترک، به مراتب بالقوه بودن بیشتری را ایجاد کرده است. در این فضا به راحتی هر جرمی صبغهٔ جهانی می‌یابد و حفظ انسجام جامعهٔ جهانی سایبری اقتضا می‌کند در سریع‌ترین و راحت‌ترین شکل تدابیر کیفری لازم اعمال گردد. هم‌اکنون اشتراک نظرهای بسیاری راجع به برخی مصادیق مجرمانه، نظیر هرزه‌نگاری کودکان، نشر ویروس (به ویژه از منظر تروریستی آن)، پول‌شویی الکترونیکی و ... به وجود آمده است که به تدریج بر نوع و میزان آنها افزوده خواهد شد. به همین دلیل، کنوانسیون جرائم سایبر علاوه بر آخرین بند از مادهٔ ۲۲ خود که اشعار داشته است:

مادهٔ ۲۲. صلاحیت: ۱. هر یک از اعضا باید به گونه‌ای اقدام به وضع قوانین و دیگر تدابیر کنند که در صورت لزوم، صلاحیت رسیدگی به هر یک از جرائم مصوب مندرج در مواد ۲ تا ۱۱ این کنوانسیون را داشته باشند ... ت. در جایی که جرم مورد نظر مطابق قوانین جزایی قابل مجازات شناخته شده، توسط تبعه‌اش ارتکاب یافته یا جرم ارتکابی از جمله جرائم واقع در حوزه صلاحیت جهانی حقوق جزا باشد ... .

در مقدمه نیز بر لزوم اتخاذ سیاست جنایی مشترک جهت مقابله با این طیف از جرائم تأکید کرده است (مرکز پژوهشهای مجلس شورای اسلامی، ۱۳۸٤: ١٤).

نتیجه‌گیری

امروزه اعمال ضمانت اجراهای کیفری در فضای سایبر به یکی از معضلات جدی کشورها تبدیل شده است. البته ریشهٔ این معضلات عمیق‌تر و گسترده‌تر از قواعد و سازوکارهای شکلی است و گزافه نیست اگر منشأ عدم شکل‌گیری اجماع جهانی در اعمال صلاحیت کیفری قضایی را در صلاحیت تقنینی کیفری سایبری یا همان جرم‌انگاری در فضای سایبر بدانیم. کما اینکه تدوین کنندگان کنوانسیون جرائم سایبر نیز نتوانستند بر آن فائق آیند و در نهایت ۹ عنوان مجرمانه که همگی به اتفاق از حق شرط (Reservation) برخوردار بودند ارائه گردید که این خود ضرورت کار جمعی بیشتر را برای نزدیک‌تر کردن دیدگاههای ملی در شکل‌گیری یک سیاست جنایی مشترک سایبری نشان می‌دهد (مرکز پژوهشهای مجلس شورای اسلامی، ۱۳۸۵: ۱۵).

آثار تبعی این مسائل بنیادین را می‌توان در لایه‌های بعدی صلاحیت کیفری نیز ملاحظه کرد. در این نوشتار مجال طرح مسائل راجع به تعارض منفی (Negative Conflict) و تعارض مثبت (Positive Conflict) در صلاحیت، منع محاکمهٔ دوباره (Double Jeopardy) و راههای رفع آنها فراهم نبود. بی‌تردید با توجه به شرایط خاص و منحصر به فرد فضای سایبر، ضروری است هر یک از این مسائل با نگاهی جامع و در عین حال موشکافانه مورد بررسی و تجزیه و تحلیل قرار گیرد تا بتوان با مبنا قرار دادن ضابطهٔ متعارف بودن، به یک راه حل منطقی و کاربردی، به ویژه برای همکاری قضایی بین‌المللی کشورها به عنوان تنها راه حل‌وفصل معضلات حاکم بر اعمال صلاحیت کیفری دست یافت.

منابع

الف. فارسی

۱. جلالی فراهانی، امیرحسین، «تروریسم سایبری»، *فصلنامهٔ تخصصی فقه و حقوق*، شماره ۱۰، پاییز ۱۳۸۵.

۲. خرم‌آبادی، عبدالصمد، «سابقهٔ پیدایش، تعریف و طبقه‌بندی جرائم رایانه‌ای»، *مجموعه مقالات همایش بررسی ابعاد حقوقی فناوری اطلاعات*، معاونت حقوقی و توسعهٔ قضایی قوهٔ قضائیه، نشر سلسبیل، ۱۳۸٤.

۳. دبیرخانهٔ شورای عالی اطلاع‌رسانی، *مجموعه مقالات همایش نقش مراکز داده در توسعهٔ فناوری اطلاعات و ارتباطات*، ۱۳۸٤.

٤. شیایزری، کریانگ ساک کیتی، *حقوق بین‌المللی کیفری*، ترجمهٔ بهنام یوسفیان و محمد اسماعیلی، نشر سمت، ۱۳۸۳.

۵. کاشیان، علیرضا و دیگران، *راهبری اینترنت (مشارکت فراگیر)*، دبیرخانهٔ شورای عالی اطلاع‌رسانی، ۱۳۸٤.

٦. مرکز پژوهشهای مجلس شورای اسلامی، *بررسی آئین‌نامهٔ تأمین، توزیع و عرضهٔ خدمات اینترنت و اینترانت ملی*، شمارهٔ ۸۲٦۹، اسفند ماه ۱۳۸۵.

۷. مرکز پژوهشهای مجلس شورای اسلامی، *قانون جرائم رایانه‌ای «خلأها و ضرورتها»*، شمارهٔ ۷۸۸٤، ۱۳۸۵.

۸. مرکز پژوهشهای مجلس شورای اسلامی، *کنوانسیون جرائم سایبر و گزارش توجیهی آن*، شمارهٔ ۷٦٤٦، بهمن ماه ۱۳۸٤.

۹. میر محمدصادقی، حسین، *حقوق جزای بین‌الملل (مجموعه مقالات)*، نشر میزان، ۱۳۷۷.

۱۰. وست‌بروک، ریموند، «کدهای باستانی و قداست‌بخشی به آنها، داستان پیدایش مفهوم قانون‌محوری»، ترجمهٔ محمد صدر توحیدخانه، مجلهٔ *حقوقی دادگستری*، شمارهٔ ٤٧، تابستان ١٣٨٣.
۱۱. یزدان‌پور، اسماعیل (مترجم)، *علم در جامعهٔ اطلاعاتی*، کمیسیون ملی یونسکو، دبیرخانهٔ شورای عالی اطلاع‌رسانی، ١٣٨٤.

ب. لاتین

12. August Ray, International Cyber-Jurisdiction: A Comparative Analysis, *American Business Law Journal*, 2002.
13. Council of Europe, European Committee on Crime Problems, *Extraterritorial Criminal Jurisdiction*, Strasbourg, 1990.
14. Law Reform Commission of Canada, *Extraterritorial Jurisdiction (Working Paper 37)*, 1984.
15. Li Xingan, *Theories and Practices of International Jurisdiction of Cyber Crime*, LEX Publications, 2004.
16. Menthe, Darrel C., *Jurisdiction in Cyberspace: A Theory of International Spaces*, Michigan Telecommunications and Technology Law Review, Vol. 4:69, 1998.
17. United Nations Office on Drugs and Crime, *The Global Program against Corruption, UN Anti-Corruption Toolkit*, Third Edition, Vienna, September 2004.
18. W. Brenner, Susan & Koops, Bert-Jaap, *Approaches to Cyber Crime Jurisdiction*, 4 J. High Tech. L. 1, 2004.