فصلنامهٔ مطالعات حقوق عمومی، دورهٔ ۴۹، شمارهٔ ۴، زمستان ۱۳۹۸: ۱۳۵۱-۱۳۷۲
DOI: 10.22059/jplsq.2019.208109.1271

ضرورت ایجاد نظام هماهنگ حقوقی بین‌المللی در مقابله با جرائم در فضای مجازی

محمود جلالی[1*]، سعیده توسلی اردکانی[2]

چکیده

عرصهٔ حقوق مانند سایر ابعاد زندگی بشری از پدیدهٔ جهانی شدن تأثیر می‌پذیرد و در مسیر این فرایند گام‌های تغییر را پشت سر می‌گذارد؛ گام‌هایی که لاجرم در بعضی از حوزه‌ها باید با سرعت بیشتری برداشته شوند تا از فواید جهانی شدن بهره گیرند. عرصهٔ حقوق کیفری و به‌ویژه حقوق فضای سایبر و جرائم ارتکابی در آن از جمله حوزه‌هایی است که به‌دلیل جهانی شدن و آثار آن، تصویب قوانین و مقررات متحدالشکل یا هماهنگ ملی و بین‌المللی در آن به‌شدت احساس می‌شود. فضای بی‌مرز سایبر، جهانی موازی با جهان فیزیکی را به‌وجود آورده است که در واقع کنترل و ادارهٔ حقوقی آن از حیطهٔ اعمال قدرت یک حاکمیت برنمی‌آید. بنابراین، برای حاکمیت بر این فضا و مقابله با جرائم روزافزون و پیچیدهٔ ارتکابی در آن همکاری و معاضدت جامعهٔ بین‌المللی برای قاعده‌مندی نیاز است، به‌گونه‌ای که هیچ مجرمی بدون مجازات نماند و این مهم به‌دست نمی‌آید مگر با تدوین مقررات هماهنگ و متحدالشکل، زیرا جرائم ارتکابی در این فضا مرزهای جغرافیایی و سنتی را پشت سر می‌گذارند و به‌سبب ویژگی‌هایی که دارند، می‌توان برخی از این‌گونه جرائم را در زمرهٔ آن دسته جرائمی به‌شمار آورد که برای مقابله با آنها اعمال صلاحیت جهانی ضرورت دارد. با وجود فعالیت‌های گوناگون سازمان‌های بین‌المللی جهت ارائهٔ مقررات پیشنهادی در جهت یکسان‌سازی و هماهنگ‌سازی مقابله با جرائم در فضای مجازی، هنوز هم جامعهٔ جهانی به هدف خود دست نیافته است، بنابراین، وجود مقررات مدونی که کاستی‌های سایر مقررات را برطرف کند، لازم‌الاجرا باشد و بتواند مقبولیت جهانی را به‌دست آورد، ضروری است.

کلیدواژگان

جرائم رایانه‌ای، حقوق بین‌الملل کیفری، جهانی شدن حقوق، فضای مجازی، متحدالشکل‌سازی حقوقی.

---

۱. دانشیار گروه حقوق، دانشکده علوم اداری و اقتصاد، دانشگاه اصفهان، اصفهان، ایران (نویسنده مسئول).
Email: m.jalali@ase.ui.ac.ir

۲. دانش‌آموختهٔ کارشناسی ارشد حقوق جزا و جرم شناسی، گروه حقوق، دانشگاه اصفهان، اصفهان، ایران.
Email: saeedetavassoli.ar@gmail.com

تاریخ دریافت: ۱۳۹۵/۰۳/۰۷، تاریخ پذیرش: ۱۳۹۵/۱۰/۱۳

مقدمه

با تولد اینترنت و پاگذاشتن آن به عرصهٔ استفاده از فناوری کامپیوتری، تحولی عظیم در کارامدی، انعطاف‌پذیری، سرعت عمل و توسعهٔ این بخش ایجاد شده است. امروزه فناوری ارتباطات حول همین موضوع گردش دارد و فناوری اطلاعات بدون در نظر گرفتن دنیای شگفت‌انگیز آن چیزی جز یک شیء بی‌محتوا نخواهد بود. غرایز و اهداف انسان‌ها مختلف است و همان‌طورکه همیشه اشخاصی هستند که با به خدمت گرفتن علوم در جهت آسایش و رفاه انسان گام برمی‌دارند، برخی افراد نیز وجود تنها به استفاده از علوم و بهره‌برداری از آن برای دستیابی به منافع شخصی حتی به بهای وارد آمدن خسارات بسیار به عموم جامعه می‌اندیشند. در مورد استفاده از فناوری کامپیوتر و به‌تبع آن فضای اینترنت و سایبر نیز همین سخن صادق است.

فضای سایبر یا فضای مجازی که جرائم موردنظر این مقاله در آن ارتکاب می‌یابد و امروزه این جرائم در شاخهٔ نسبتاً مستقل و در حال شکل‌گیری تحت عنوان حقوق سایبر[1] یا نظام حقوقی فضای مجازی مطالعه می‌شود، به دنیایی گفته می‌شود که با استفاده از فناوری اطلاعات و تکنولوژی‌های نوین ارتباطات و علوم رایانه، اینترنت و امکانات مجازی همانند دنیای واقعی در کیفیت زندگی افراد جامعه تأثیرگذار است. فضای مجازی در این معنا «به مجموعه‌هایی از ارتباطات درونی انسان‌ها از طریق کامپیوتر و وسایل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی گفته می‌شود. در این فضا مرز بین دنیای درون و بیرون تقریباً ناپدید می‌شود و دیگر زمان معنایی ندارد. در واقع می‌توان گفت فضای مجازی گستره‌ای از ذهن است که می‌تواند تمامی اشکال زندگی واقعی را بسط و معنا دهد» (پورنقدی، ۱۳۹۳: ۱۱). بنابر این، جرائم موضوع این مقاله در دنیای کامپیوترها و به‌ویژه اینترنت و بیشتر با ماهیت بین‌المللی موضوعیت دارد و مواردی مانند دسترسی غیرمجاز، شنود غیرقانونی، اعمال علیه محرمانگی، تولید و توزیع برنامه‌های رایانه‌ای ارتکاب جرم، تمامیت و در دسترس بودن سیستم‌های رایانه‌ای، شبکه‌ها و داده‌های رایانه‌ای، انتشار مطالب نژادی و تنفرانگیز، فحشا، هرزه‌نگاری و هتک حرمت، نقض حریم خصوصی و سوء استفاده از تصاویر شخصی افراد، حملات اینترنتی، افشای اسرار تجاری، جاسوسی، سرقت و کلاهبرداری اینترنتی، نقض حقوق مالکیت معنوی در فضای مجازی و تعرض به حق نشر، ایجاد خرابکاری کامپیوتری در سیستم حرکت قطارها، هواپیماها و کشتی‌ها و امنیت سیستم‌ها را در برمی‌گیرد.

با روش توصیفی-تحلیلی، هدف مقالهٔ حاضر تبیین اهم دستاوردهای جامعهٔ بین‌المللی در مبارزه با جرائم فضای مجازی و برجسته کردن خلأهای موجود در این زمینه برای رویارویی با

---

۱. واژهٔ حقوق سایبر که فناوری اطلاعات و ارتباطات را قانونمند می‌کند، در دههٔ ۱۹۹۰ جایگزین عناوینی چون حقوق انفورماتیک، حقوق کامپیوتر و فناوری اطلاعات و ارتباطات شده است. ن.ک:

جرائم موصوف است. بدین‌منظور ابتدا به جهانی شدن حقوق کیفری و خصایص جهانی ارتکاب جرائم در این فضا پرداخته می‌شود. سپس اقدامات هماهنگ‌کنندهٔ برخی نهادهای فعال در این زمینه بررسی و به‌طور ویژه به مفاد کنوانسیون ۲۰۰۱ بوداپست پرداخته می‌شود و در پایان ضرورت توجه بیشتر جامعهٔ بین‌المللی به پدیدهٔ جهانی جرم در فضای سایبر و در نتیجه نیاز به وضع مقررات هماهنگ و حتی‌الامکان متحدالشکل مقابله با جرائم در این فضا بررسی می‌شود.

جهانی شدن حقوق کیفری و فضای مجازی

جهانی شدن حقوق واقعیتی انکارناپذیر است؛ واقعیتی که هم از منظر نهادها، مفاهیم و ارزش‌های حقوقی شایان توجه است و هم از منظر شکلی و الگوبرداری تقنینی. «همهٔ اینها در حالی است که به‌طور سنتی، حقوق کیفری بخشی از حقوق عمومی و در صلاحیت دولت‌ها بوده است و هیچ دولتی نمی‌توانست در هیچ‌یک از مراحل فرایند کیفری، از جرم‌انگاری تا مجازات در امور داخلی دولت دیگر دخالت کند و گاه این صلاحیت نشانه‌ای بارز و دلیلی بر حاکمیت ملی شناخته می‌شد» (دلماس مارتی[1]، ۱۳۷۶: ۴۵). اما امروزه قواعد حقوق بشردوستانه حتی به مخاصمات مسلحانهٔ داخلی نیز تسری یافته و دیوان بین‌المللی کیفری نیز مانند مخاصمات مسلحانهٔ بین‌المللی در رسیدگی به این‌گونه موارد دارای صلاحیت است. «برای پاسداشت حساسیت‌های مربوط به حاکمیت که مشروع نیز هست، جهانی شدن حقوق کیفری، تنها با رضایت قانونگذاران محلی محقق می‌شود. نزدیک شدن نظام‌های حقوقی را نمی‌توان از خارج تحمیل کرد و اگر در گذشته همواره به این ترتیب نبوده است، اما امروزه چنین است» (پرادل[2]، ۱۳۸۳: ۱۶۲).

شاید بتوان گفت مهم‌ترین مسئله یا به‌عبارت بهتر، چالشی که مجریان قانون در زمینهٔ جرائم در فضای مجازی با آن مواجه‌اند، «بین‌المللی بودن» این جرائم است. همین مسئله سبب شده از همان زمان که وجههٔ بین‌المللی جرائم رایانه‌ای مورد توجه کشورهای جهان قرار گرفته، اقدامات گسترده‌ای به‌منظور ساماندهی، پی‌جویی و تعقیب جرائم تبادل اطلاعات در عرصهٔ بین‌الملل صورت گیرد و از کشورها خواسته شده بر مبنای موازین حقوق داخلی خود، به‌ویژه توافقنامه‌های دوجانبه یا چندجانبه‌ای که با سایر کشورها منعقد کرده یا اسناد بین‌المللی یا منطقه‌ای که به آن ملزم شده‌اند، زمینه‌های همکاری متقابل در این حوزه را تقویت کنند؛ و این چیزی نیست جز حرکت کردن در مسیر جهانی شدن به‌ویژه جهانی شدن حقوق کیفری و قلمرو زدایی سرزمینی از امور کیفری (جوانمردی صاحب، ۱۳۹۴).

جرائم فضای مجازی نیز از جمله جرائمی اند که قابلیت ایراد صدمه به «نظم عمومی

1. Delmas Marty
2. Pradel

جهانی» را دارند و به کل جامعهٔ بین‌المللی مربوط می‌شوند. همچنین به دلیل ویژگی‌هایی که دارند، مرتکبان این جرائم اغلب بدون مجازات می‌مانند.

ماهیت و خصایص جرائم ارتکابی در فضای مجازی

در واقع از عمر رواج اصطلاح «جرم سایبری» کمتر از دو دهه می‌گذرد و پیش از آن نمی‌توان چنین واژه‌ای را در هیچ لغت‌نامه‌ای پیدا کرد. «اما امروزه در همهٔ لغت‌نامه‌های به‌روزآمد شده اعم از اینترنتی و معمولی می‌توان چنین واژه‌ای را به‌راحتی پیدا کرد» (کلانتری،۱۳۹۳: ۱۴۹). اما بدیهی است «جرم سایبری به رفتارهایی که ضد این فضا یا بستر بی‌مرز و بی‌کران یا توسط آن ارتکاب می‌یابد، اطلاق می‌گردد» (عالی‌پور، ۱۳۹۰: ۱۳۰).

در تعاریف گوناگونی که از جرائم سایبری یا جرائمی که در فضای مجازی به‌وقوع‌پیوسته وجود دارد، می‌توان به برخی ویژگی‌های مشترک آنها دست یافت، اما برای روشن‌تر شدن ماهیت فضای سایبر و جرائم قابل ارتکاب در آن معرفی انواع این جرائم ضروری است؛ جرائمی که می‌توان در یک دسته‌بندی کلی آنها را به دو دسته «جرائم رایانه‌ای وسیله‌محور» و «جرائم رایانه‌ای موضوع محور» تقسیم کرد؛ جرائم رایانه‌ای وسیله‌محور شامل جرائم ضداشخاص، ضدعفت و اخلاق عمومی و جرائم علیه اموال، و جرائم موضوع‌محور شامل جرائم ضدمحرمانگی داده‌ها و سامانه‌های رایانه‌ای و مخابراتی، جرائم ضدصحت و تمامیت داده و سامانه‌های رایانه‌ای و مخابراتی و جرائم ضدقابلیت دسترسی، می‌شود.

طرق ارتکاب این جرم راه را برای تعریف جامع و مانع از آن بسته است؛ این امر به‌علت طبع این‌گونه جرائم است.

۱. ماهیت بین‌المللی جرائم ارتکابی در فضای مجازی

متمایزترین و مهم‌ترین ویژگی دنیای سایبر از دنیای خاکی یا فیزیکی، برچیده شدن مفهوم ماده و مختصات مکانی آن است. همین توانمندی سبب شده همه‌چیز یک‌جا باهم باشد و همزمان به کاربری‌های متفاوتی پرداخته شود. برای مثال «در کنار آموزش الکترونیکی، مایحتاج خود را خریداری، امور بانکی را انجام، گفت‌وگوی روزانه را در محیط‌های ارتباطی خصوصی و شبکه‌های اجتماعی، غیرعمومی و عمومی برقرار و با همهٔ اینها، پایگاه‌های خبری و سرگرمی‌های مورد علاقه را هم مرور و بررسی کنیم» (کیسی،[1] ۱۳۸۶: ۷).

1. Casey

۲. ارتباطات بدون مرز

در دنیای مجازی افراد می‌توانند فارغ از محدودیت‌هایی چون مرزهای ملی، حاکمیت سیاسی و نظارت سازمان‌ها، مراجع مختلف، زبان، ملیت، نژاد، جنسیت و ... از هر کجای دنیا و در هر زمان با جوامع مختلف ارتباط برقرار کنند؛ با آنها وارد گفتمان شوند و از نظرهای آنها مطلع شوند. پس از انقلاب صنعتی که «با بهره‌گیری از ابزارها و وسایل پیشرفتهٔ صنعتی، در امر تولید کالا تحولات شگرفی در سطح دنیا به‌دنبال داشت و عصر صنعتی را رقم زد، اکنون پس از گذشت قرن‌ها دچار انقلاب اطلاعات شده‌ایم که تأثیرات آن نسبت به انقلاب صنعتی بیشتر است که در مقابل، عواقب این دگرگونی اطلاعات شامل یک ایالت یا یک سرزمین مشخص نیست بلکه شامل تمام جوامع ملل می‌گردد» (حسنی و همکاران، ۱۳۹۳: ۱۶).

۳. تحول مفهوم زمان و مکان در دنیای مجازی

مفهوم زمان و مکان به‌صورت ساختاری و در فضای سایبری و فیزیکی با یک‌دیگر متفاوت است. در جرائم رایانه‌ای علاوه‌بر طرق مختلف ارتکاب یک جرم، جهان بعضاً با جرائم جدیدی روبه‌رو می‌شود که حتی شناخت مفهومی این جرائم برای حقوقدانان و قضات دشوار است. «این امر ناشی از سرعت بالای پیشرفت فناوری و تکنولوژی اطلاعات و ارتباطات است. شاید بتوان گفت به‌دلیل سرعت بالای این پیشرفت‌ها و همچنین سرعت بالای این‌گونه ابزارها، قانونگذار کیفری همیشه یک گام عقب‌تر از فناوری است و پس از قربانی شدن شهروندان بسیاری توسط مجرمین باهوش رایانه‌ای، به پیشگیری یا جرم‌انگاری می‌پردازد» (سلیمی، ۱۳۹۱: ۱۷). ازاین‌رو فضای سایبر، فضای یک محل در همهٔ جهان و همهٔ جهان در یک محل است. وسعت آن به اندازهٔ تمام جهان است و لامکان و بدون مرز بودن، آن را به بزرگی جهانی که سرعت و فرامرزی بودن آن را کوچک کرده، تبدیل ساخته است (عاملی، ۱۳۹۰: ۲۸). زمان در این فضا معنایی نو یافته و مکمل معنای نو و جدید مکان در فضای سایبر شده است؛ بدین‌نحو که در زمانی ناچیز می‌توان با دورترین نقاط جهان ارتباط برقرار کرد.

۴. موقعیت متفاوت مجرمان در فضای مجازی

مجرمان تبادل اطلاعات برخلاف مجریان قانون برای ارتکاب انواع جرائم خود، با حد و مرزی مواجه نیستند و به‌راحتی می‌توانند از هر نقطهٔ این کرهٔ خاکی سیستم‌ها و داده‌های رایانه‌ای موردنظر خود را مورد تعرض قرار دهند یا دیگر جرائم تبادل اطلاعات را مرتکب شوند (جلالی فراهانی، ۱۳۸۹: ۲۰۶). این دسته از جرائم، بعضاً از لحاظ مرتکبان هم با جرائم سنتی تفاوت دارند؛ برخلاف جرائم سنتی که معمولاً حضور مجرم در محل وقوع جرم ضروری است، در

فضای مجازی چنین ضرورتی وجود ندارد و شاید مجرم فرسنگ‌ها با محل وقوع جرم یا نتیجهٔ آن فاصله داشته باشد. به‌طور مثال در جرمی مانند انتشار ویروس می‌توان گفت با پخش ویروس، جرم در تمام جهان انجام شده است. همچنین «جرم سایبری مستلزم مجاورت فیزیکی میان قربانی و مرتکب نیست. برعکس جهان واقعی، در جهان سایبر جرم به‌صورت اتوماتیک از طریق فناوری واقع می‌شود، چون جرم در جهان واقعی اتفاق نمی‌افتد، از محدودیت‌های جهان فیزیک هم برخوردار نیست» (جوان جعفری، ۱۳۹۰: ۲۶).

تصویب قوانین متحدالشکل بین‌المللی

متحدالشکل‌سازی بین‌المللی حقوق، شامل تمام سعی و تلاش‌هایی است که با هدف غلبه بر تفاوت‌های میان نظام‌های حقوقی داخلی متعدد، از طریق بسط سیستمی از قوانین که جایگزین قوانین ملی موجود در تنظیم یک موضوع معین می‌شود، صورت می‌گیرد، این فرایند به وضوح متفاوت از متحدالشکل‌سازی قانون داخلی است (کارولیس، ۲۰۱۰: ۹۱).

در اغلب تعاریف موجود از متحدالشکل‌سازی حقوقی، بر فرایند نزدیک شدن نظام‌های حقوقی تأکید شده است، فرایندی که در آن سعی می‌شود تفاوت‌های موجود میان نظام‌های حقوقی برداشته شده و معیار مشترکی برای تدوین، تنظیم و تصویب قوانین در نظر گرفته شود، معیاری که گاه الزام‌آور و گاه اختیاری هستند. ازاین‌رو «نظریهٔ متحدالشکل‌سازی حقوقی، آینده‌ای را رقم می‌زند که دستیابی به آن از اهم اهداف برخی مجامع و سازمان‌های بین‌المللی است؛ در حقیقت، هدف این نظریهٔ بین‌المللی، دستیابی به نظام واحد جهانی در تمامی گرایش‌های حقوقی است و شکل‌گیری آن از ثمرات اندیشهٔ یگانه‌انگاری حقوق محسوب می‌شود؛ اما به‌دلیل واکنش منفی دولت‌ها در قبال پذیرش قانونگذاری‌های فراملی، تحقق کامل آن همواره با مشکلاتی مواجه بوده است. مخالفان، آن را تهدیدی برای حاکمیت می‌دانند و در مقابل موافقان آن را ارزشمند و از اقتضائات شرایط جدید تجاری، قلمداد می‌کنند» (شکوری، ۱۳۸۹: ۴).

برخی مؤسسات معتبر و متخصص در جهان به تهیه و تدوین «قوانین نمونه» در زمینهٔ تخصصی خود می‌پردازند و مشکل مواضع حساس و مدرن و به‌روز نبودن یافته‌های علمی جهان را تا حدودی حل کرده‌اند. این مؤسسات بهترین متخصصان و حقوقدانان را به‌کار می‌گیرند تا ضمن رعایت اصول قانونگذاری و توجه به نیازهای جامعهٔ جهانی، نتیجهٔ مطالعات و تحقیقات علمی و تطبیقی خود را به‌صورت مقررات نمونه منتشر سازند و آن را در اختیار نهادهای قانونگذاری کشورهای مختلف قرار دهند. این قوانین نمونه به‌دلیل داشتن برخی ویژگی‌ها مورد استقبال بعضی کشورهای مختلف قرار گرفته‌اند. اولین ویژگی این است که چون این مقررات به حکومت خاصی مربوط نیستند، پس هر کشوری که بخواهد از آنها استفاده کند، احساس

نمی‌کند حاکمیت ملی خود را به‌وسیلهٔ مقررات کشور دیگری زیر سؤال برده است. ویژگی دیگر این است که مقررات نمونه از ایدئولوژی خاصی ناشی نشده‌اند که دیگر کشورها در استفاده از آنها با چالش روبه‌رو شوند و آن را تهدیدی علیه ایدئولوژی ملی خود بدانند. ویژگی سوم این است که این قوانین به‌صورت منظم، بسیار دقیق و به‌طور تخصصی تنظیم شده‌اند. این مقررات با این ویژگی‌هایی که دارند، از طرف اکثریت حکومت‌ها مورد پذیرش قرار می‌گیرند و این حرکت به‌طور مستقل، خود سبب نوعی هماهنگی و یکسان‌سازی قوانین در آن زمینه خاص می‌شود. اگرچه در زمینهٔ فضای مجازی هنوز صحبت از چنین قوانین نمونه‌ای به نظر زودهنگام است، نقش چشمگیر انجمن‌ها و نهادهای غیردولتی فعال مانند ایکان (ICANN)[1] و آیسوک (ISOC)[2] در زمینه‌سازی ایجاد این‌گونه مقررات انکارناپذیر است.

فعالیت‌های هماهنگ‌ساز سازمان‌های بین‌المللی در خصوص جرائم در فضای مجازی

همان‌طورکه گفته شد، جرائم در فضای سایبر اغلب دارای ابعاد بین‌المللی‌اند. «پست‌های الکترونیکی با محتوای غیرقانونی عموماً از میان تعدادی کشور تا رسیدن به مقصود عبور می‌کند و چند نظام حقوقی مختلف را درگیر چنین موضوعی می‌کند. یکی از راه‌هایی که می‌توان به‌وسیلهٔ آن بر این مشکل فائق آمد توافقات دوجانبهٔ رسمی بین کشورهاست. اما در این رابطه مشکلاتی وجود دارد مبنی‌بر اینکه پروسهٔ رسمی دستیابی به توافقات رسمی بین کشورها معمولاً زمان‌بر و دشوار است و با ذات جرم رایانه‌ای که یکی از ویژگی‌های اصلی آن سرعت می‌باشد، همخوانی ندارد. این موضوع بدان معنی نیست که هیچ توافقی در رابطه با چنین جرائمی وجود ندارد، بلکه برخی در همهٔ کشورها جرم انگاشته می‌شود» (گرک[3]، ۱۳۸۹: ۲۴). نمونه‌ای از این موارد سرقت است. با وجود اختلاف بین نظام‌های حقوقی مختلف در تعریف و تشخیص جرائم، روش‌های استفاده از فناوری رایانه در همه جای جهان یکسان است. از همین رو می‌توان این را فرصتی دانست که به‌دلیل متحدالشکل بودن سبک استفاده از رایانه، نظام‌های حقوقی در این مورد در کشورها با سرعت بیشتری به هماهنگی برسد.

نقش جامعهٔ بین‌المللی در جایی پررنگ‌تر می‌شود که بر سر امور مهمی همچون اعمال صلاحیت در مورد یک جرم از سوی کشورها باید تعیین تکلیف شود. مثلاً ممکن است در فضای سایبر جرمی علیه یک کشور در خاک کشور دیگری تحقق یابد و حتی کشورهای بیشتری

1. Internet Corporation for Assigned Names and Numbers
2. Internet Society
3. Gerck

درگیر این جرم شوند. از سویی حتی ممکن است به‌واسطهٔ یک جرم بین‌المللی امنیت و صلح بین‌المللی به مخاطره افتد. بنابر مطالب گفته‌شده، سازمان‌های بین‌المللی تاکنون اقدامات مختلفی انجام داده‌اند، درگیر جرائم رایانه‌ای شده و فعالیت‌های مفیدی را انجام داده‌اند.

مقررات ۱۹ سند چندجانبه در حال حاضر به جرائم سایبر پرداخته‌اند که اغلب محصول کار شورای اروپا یا اتحادیهٔ اروپا، جامعهٔ مشترک‌المنافع کشورهای مستقل یا سازمان همکاری شانگهای، سازمان‌های بین‌الدولی آفریقایی، جامعهٔ کشورهای عربی و بالاخره سازمان ملل متحد است. در ادامه به چند نمونه از برخی سازمان‌های بین‌المللی که در زمینهٔ جرائم رایانه‌ای به فعالیت پرداخته‌اند، اشاره شده و به‌اجمال بخشی از فعالیت‌های آنها در راستای متحدالشکل کردن قوانین حاکم بر جرائم رایانه‌ای تبیین می‌شود.

۱. سازمان همکاری و توسعهٔ اقتصادی

سازمان همکاری و توسعهٔ اقتصادی[1] به‌عنوان یکی از تأثیرگذارترین نهادهای اقتصادی جهانی، مجمعی را برای کشورهای همفکر به‌منظور بحث و بررسی و ایجاد و پالایش سیاست‌های اقتصادی و اجتماعی آنها فراهم آورده است. این سازمان با ارزیابی تجارب مشترک اعضا و جست‌وجوی راه‌حل برای مشکلات مشترک از طریق هماهنگ کردن سیاست‌های داخلی و بین‌المللی به آنها کمک می‌کند. توصیه‌های سازمان همکاری و توسعهٔ اقتصادی به اعضا در شکل موافقت‌نامه‌های الزام‌آور حقوقی همچون موافقت‌نامه‌های مربوط به مبارزه با رشوه و جریان آزاد سرمایه و خدمات یا از طریق سازوکارهای غیرالزام‌آور، صورت می‌گیرد (حسنی و همکاران، ۱۳۹۳: ۲۹-۲۸).

سازمان مذکور در سال ۱۹۷۷ رهنمودهای ناظر بر حمایت از حقوق فردی، حریم خصوصی و گردش فرامرزی داده و اطلاعات شخصی را اتخاذ و در سال ۱۹۷۹ منتشر کرد. کمیتهٔ تخصصی این سازمان کار خود را در زمینهٔ ایجاد هماهنگی بین‌المللی بین قوانین کیفری برای مبارزه با جرائم اقتصادی رایانه‌ای آغاز و در سال ۱۹۸۶ رهنمود جرائم مرتبط با کامپیوتر را منتشر کرد که در آن پس از بررسی قوانین موجود کشورها پیشنهادهایی برای اصلاح مقررات کشورهای عضو ارائه شد. در سال ۱۹۸۹ فهرستی از سوءاستفاده‌های رایانه‌ای ارائه کرد. سازمان در سال ۱۹۸۹ کارش را در خصوص امنیت سیستم‌های رایانه‌ای ادامه داد (گرکی، ۲۲۰ :۱۳۸۹). بنابراین، سازمان همکاری و توسعهٔ اقتصادی اولین سازمانی است که در سال ۱۹۸۳ به مطالعه و بررسی مسئلهٔ جرم یا سوءاستفاده‌های رایانه‌ای پرداخت و در همین زمینه در سال ۱۹۸۶ گزارشی نیز با عنوان جرم رایانه‌ای و تحلیل سیاست‌های قانونی منتشر کرد. در این

1. Organization for Economic Cooperation and Development(OECD)

گزارش تعریف جرم رایانه‌ای و فهرستی از جرائم رایانه‌ای محتمل را ارائه کرد و از کشورها درخواست کرد که در قوانین کیفری‌شان این‌گونه رفتارها را ممنوع گردانند (حسنی و همکاران، ۱۳۹: ۲۹). به‌نظر می‌رسد این سازمان با فهرست پیشنهادی خود گام مؤثری در راستای هماهنگ‌سازی یا متحدالشکل ساختن مقررات جرائم رایانه‌ای برداشته است، اما به‌دلیل عدم پیگیری مستمر و فقدان دایرهٔ نظارت بر اقدامات دول عضو، در زمینهٔ تصویب قوانین جرائم رایانه‌ای هماهنگ، چندان توفیق نیافته است. در هر حال، این سازمان به‌عنوان شروع‌کنندهٔ جریان هماهنگ‌سازی، زمینهٔ فعالیت سایر نهادهای بین‌المللی را که در حال حاضر در عرصهٔ جرائم فضای سایبر تلاش می‌کنند، فراهم آورده است.

۲. سازمان ملل متحد

سازمان ملل متحد با توجه به رسالت اصلی خود (ایجاد صلح و دوستی، تأمین امنیت بین المللی و حمایت از حقوق و آزادی‌های بنیادین بشر) الزاماً می‌بایست به مسائل جدید که امور مختلف جهانی را تهدید می‌کند، توجه کند. در سال ۱۹۸۵ کمیسیون سازمان ملل متحد در مورد حقوق تجارت بین‌الملل (آنسیترال)[1] توصیه‌نامه‌ای را برای اصلاح قوانین کشورها صادر کرد تا اطلاعات الکترونیکی را به‌عنوان دلیل در سیستم قضایی و اداری خود به رسمیت بشناسند. همین کمیسیون در تکمیل توصیه‌نامهٔ مذکور در سال ۱۹۹۶ به‌منظور جلوگیری از فضای ناامن در مبادلهٔ اطلاعات در اینترنت قانون نمونهٔ تجارت الکترونیک و در سال ۲۰۰۱ قانون نمونهٔ امضاء الکترونیکی را برای سرمشق قراردادن قانونگذاران ملی انتشار داد. در سال ۱۹۸۹ کمیسیون حقوق بشر سازمان رهنمودهایی برای قانونگذاری فایل‌های دادهٔ شخصی کامپیوتری اتخاذ کرد و در کنگرهٔ هشتم در سال ۱۹۹۰ نمایندهٔ کشور کانادا متن پیش‌نویس یک قطعنامه را در خصوص پیشگیری از جرائم رایانه‌ای و رفتار با مجرمان پیشنهاد کرد که در اجلاس سیزدهم پذیرفته شد و در سال ۱۹۹۴ به‌صورت کتابچه ای منتشر شد. شایان ذکر است که این قطعنامه برای کشورهای عضو الزام‌آور نبوده و اجرای آن برای دول عضو اختیاری است (شیرزاد، ۱۳۸۸: ۱۷۵-۱۷۳). با این حال، این سند اصولی که کشورها در قانونگذاری باید بدان توجه کنند، همچون اصل عدم تبعیض در داده‌های حساس نژادی و قومی، اصل ایجاد استثنا به دلایل امنیتی، سلامت و اخلاق عمومی و اصل نظارت و ضمانت بی‌طرفانه حمایت از داده‌ها را ذکر کرده است. در سال ۲۰۰۳ به ابتکار سازمان، نشست جهانی سران جامعهٔ اطلاعاتی[2] برگزار شد که از نتایج آن دو سند «اعلامیهٔ اصول»[3] و «طرح عملیات»[4] بود. اسناد مذکور با هدف

1. United Nations Commission on International Trade Law(UNCITRAL)
2. World Summit Information Society(WSIS)
3. Declaration of Principles
4. Plan of Action

ایجاد اطمینان و امنیت در استفاده از فناوری اطلاعات و ارتباطات، بر حکمرانی چندجانبهٔ بین‌المللی بر اینترنت تأکید دارند. مجمع عمومی سازمان ملل متحد در قطعنامهٔ ۹۱/۵۲ دسامبر ۱۹۹۷ و قطعنامهٔ ۱۱۰/۵۳ دسامبر ۱۹۹۸ کارگاه‌هایی را طراحی کرد تا به موضوع پیشگیری از جرائم و عدالت کیفری در فضای مجازی بپردازند. پس از برگزاری کنگرهٔ یازدهم سازمان در سال ۲۰۰۵ حاصل کار کارگاه‌ها را به‌صورت توصیه‌های سازمان منتشر کرد که از جملهٔ آنها توصیه به کشورها در به‌روز کردن قوانین کیفری خود به‌نحوی که جرائم سایبری را پوشش دهد، بوده است. البته از سازمان ملل به‌عنوان بزرگ‌ترین و مؤثرین‌ترین سازمان بین‌المللی انتظار می‌رود اقدامات بیشتری در این زمینه انجام دهد، زیرا امکانات بیشتری در اختیار دارد و تقریباً زمینهٔ اعمال نفوذ در تمامی کشورهای جهان را داراست.

در سال ۲۰۱۳ سازمان ملل متحد سند مهمی را در مورد جرائم در فضای مجازی با عنوان «مطالعهٔ جامع در خصوص جرم سایبری» منتشر کرد که در آن به انقلاب جهانی ارتباطات، رشد سریع جرم سایبری به‌عنوان چالشی جهانی، مرتکبان جرائم سایبری، نقش قانون در مقابله با این جرائم، ضرورت هماهنگ سازی قوانین، نگاهی به اسناد منطقه‌ای و بین‌المللی جرائم سایبری، دعوت از کشورها برای اجرای مقررات چندجانبه در حقوق ملی، ارتباط بین جرم‌انگاری این جرائم با حقوق بشر، ادلهٔ الکترونیک و مرزهای دیجیتال، همکاری بین‌المللی، سیاست‌های ملی جلوگیری از ارتکاب جرائم سایبری و آگاهی‌رسانی در مورد این‌گونه جرائم پرداخته است.[1] انتظار می‌رود این سازمان در روند هماهنگ و یکسان‌سازی مقررات فضای مجازی نقش فعال‌تری را ایفا کند.

۳. انجمن بین‌المللی حقوق جزا

انجمن بین‌المللی حقوق جزا[2] مؤسسهٔ حقوقی غیردولتی است که در ۱۴ مارس ۱۹۲۴ در پاریس تأسیس شد و اکنون قریب یک قرن از عمر آن می‌گذرد. انجمن که اکنون در ۳۸ کشور جهان از جمله در ایران دارای گروه ملی است، هر پنج سال یک‌بار در یکی از کشورهای داوطلب اجلاسیهٔ خود را برگزار می‌کند و از ۱۹۲۶ تاکنون ۱۹ کنگره برگزار کرده و قرار است کنگرهٔ بعدی خود را در سال ۲۰۱۹ تشکیل دهد. در جلسات انجمن فرصت‌هایی حاصل می‌شود تا در مورد موضوعات جدید حقوق جزا و آخرین تحولات این رشته از حقوق با حضور بسیاری از متخصصان کشورهای مختلف بحث و بررسی شود. در سال ۱۹۹۰ انجمن چهار موضوع را مطرح کرد که از جملهٔ آن جرائم علیه فناوری اطلاعات و جرائم رایانه‌ای بود (شیرزاد، ۱۳۸۸: ۱۷۶).

همچنین در سال ۱۹۹۲ انجمن نشستی مقدماتی در زمینهٔ جرم رایانه‌ای در دانشگاه

1. https://www.unodc.org/...crime/...4.../CYBERCRIME_STUDY_210213.pdf
2. International Association of Penal Law(IAPL)

ورتسبورگ[1] آلمان برگزار و قطعنامه‌ای در مورد فهرست جرائم رایانه‌ای صادر کرد. در سال ۱۹۹۴ در نشست خود در ریودوژانیرو[2] نیز در بخش دوم قطعنامهٔ خود با عنوان «جرائم کامپیوتری و دیگر جرائم علیه فناوری اطلاعات» مصوباتی در این خصوص داشته است.[3] انجمن در آخرین نشست خود در ریودوژانیرو در سال ۲۰۱۴ با عنوان «جامعهٔ اطلاعاتی و حقوق کیفری»[4] ضمن تأیید مجدد فهرست‌های حداقلی و اختیاری شورای اروپا عناوینی را به‌عنوان جرائم رایانه‌ای نام برد که برخی از آنها به قرار ذیل است: ۱. قاچاق کلمات رمز، ۲. انتشار ویروس یا برنامه‌های مشابه، ۳. دسترسی به اسرار برخلاف قانون و ۴- به‌کارگیری و انتقال و دگرگونی داده‌های شخصی (حسنی و همکاران، ۱۳۹۳: ۳۲-۳۰).

درحالی‌که انجمن متخصصان بسیاری در این زمینه دارد و می‌تواند اقدامات تخصصی تأثیرگذاری در مورد جرائم در فضای مجازی انجام دهد، به‌نظر می‌رسد بیشتر در پی بررسی فعالیت دیگر سازمان‌ها برآمده و آنها را تأیید کرده است. البته توجه این انجمن به جرائم رایانه‌ای و نشست‌های سالانهٔ آن در این زمینه را نباید نادیده گرفت. در بند ۱۳ قطعنامهٔ ۲۰۱۴ انجمن به‌صراحت قید شده که «خط‌مشی‌های حمایت از شبکه‌های فناوری ارتباطات و اطلاعات و فضای مجازی و منافع کاربران باید به‌صورت جهانی هماهنگ گردد تا بتوان از تعارضات جدی قانونگذاری در خصوص موضوعات مشابه خودداری کرد و همکاری بین‌المللی را توسعه بخشید و از تعارض صلاحیت دادگاه‌ها اجتناب ورزید».[5] چه‌بسا نتایج به‌دست آمده از همین نشست‌ها الگوی دیگر نهادهای بین‌المللی در طراحی یک قانون هماهنگ، جامع و مفید در رابطه با موضوع باشد.

۴. شورای اروپا و کنوانسیون بین المللی بوداپست

شورای اروپا کار متحدالشکل‌سازی در زمینهٔ حفاظت از داده‌ها را از از سال ۱۹۶۸ در منطقهٔ اروپا آغاز کرد و آن را به سایر مناطق جهان نیز پیشنهاد می‌دهد. هرچند فهرست های حداقل و اختیاری شورای اروپا حالت پیشنهادی دارند، مناسب‌تر این است که برای شکل‌گیری چنین مقررات هماهنگ و متحدالشکل بین‌المللی، تمامی دول جهان در روند شکل‌گیری و تدوین شرکت داشته باشند تا قانون شکلی و ماهوی که قرار است در زمینهٔ جرائم رایانه‌ای تدوین و تصویب شود، مناسب با شرایط همهٔ کشورها و همچنین همراه با رعایت قواعد حقوقی حاکم بر دول جهان باشد. همان‌طورکه بیان شد، کشورهایی به این توصیه‌نامه پیوسته و آن را امضا

1. Wurzburg
2. Rio de Janeiro
۵. برای ملاحظهٔ قطعنامه‌های انجمن ر.ک: http://www.penal.org/en/resolutions-aidp-iapl-congresses
4. Information Society and Penal Law
5. http://www.penal.org/en/resolutions-last-congress

کرده‌اند که تقریباً شرایطی همچون کشورهای اروپا دارند و از طرف کشورهای آسیایی و خاورمیانه چندان مورد اقبال و پذیرش نبوده است. دستورالعمل‌های اتحادیهٔ اروپا مانند دستورالعمل شمارهٔ ۴۶ مورخ ۱۹۹۵ در زمینهٔ حمایت از داده و کنوانسیون‌های شورای اروپا مثل کنوانسیون ۱۹۸۵ شورا در خصوص حمایت از حریم خصوصی، دو منبع اصلی حقوق فضای مجازی کشورهای عضو اتحادیه است. این اسناد حداقل تعهدات دولت‌های عضو برای هماهنگی را بیان می‌کنند و قوانین ملی کشورهای عضو نیز کم و بیش از این طریق الهام می‌گیرند.

در پی پیشنهاد کمیتهٔ منتخب جرائم رایانه‌ای شورای اروپا، کمیتهٔ وزرای شورای اروپا فهرست حداقل و فهرست اختیاری طبقه‌بندی‌شده‌ای را طی توصیه‌نامهٔ سال ۱۹۸۹ خود ارائه کرد تا کشورهای عضو بر مبنای آن به جرم‌انگاری جرائم رایانه‌ای بپردازند.

متعاقب تصمیمات کمیته، در سال ۲۰۰۱ در اجلاس بوداپست[1] توصیه‌نامهٔ شورای اروپا به امضای کشورهای عضو شورای اروپا و چهار کشور آمریکا، ژاپن، کانادا و آفریقا رسید. در این اجلاس جرائم سایبری طبقه‌بندی شد و نتایج آن تحت عنوان «کنوانسیون بوداپست جرائم سایبری»[2] نام گرفت (شیرزاد، ۱۳۸۸: ۱۳۶).

در میان فعالیت‌های بین‌المللی صورت‌گرفته در خصوص جرائم سایبر و هماهنگ کردن مقررات بین‌المللی در این زمینه، کنوانسیون بوداپست بیشتر از همه خودنمایی می‌کند (ن.ک: زندی، ۱۳۹۳: ۶۵۷ به بعد)، چراکه این کنوانسیون چکیده‌ای از فعالیت‌های تمام نهادهای پیش‌گفته است. در واقع این کنوانسیون با بررسی و نقد تمامی فعالیت‌ها در سطح ملی و بین‌المللی مقرراتی را تدوین و سعی کرده است که ضعف‌های موجود در گزارش‌ها و مقررات پیشنهادی سایر نهادها را برطرف کند، هرچند در حال حاضر این کنوانسیون نیز ضعف هایی دارد، اما می‌توان گفت کنوانسیون به‌طور تخصصی فعالیت می‌کند و جایگاه خاصی را در میان سایر نهادهای فعال در این زمینه به خود اختصاص داده است. از زمانی‌که این کنوانسیون و گزارش توجیهی آن در یکصدونهمین جلسهٔ وزرای شورای اروپا در هشتم نوامبر ۲۰۰۱ به تصویب رسید، از بیست‌وسوم همان ماه، در شهر بوداپست، در کنفرانس بین‌المللی جرائم سایبر، جهت امضا مفتوح مانده است و در حال حاضر علاوه‌بر کشورهای عضو شورای اروپا بیش از شصت کشور دیگر در سراسر جهان این سند را امضا کرده و به تصویب رسانده اند. هرچند ایران به این کنوانسیون نپیوسته و آن را امضا نکرده است، اما با مطالعه و تدقیق در جرائم رایانه ای مصوب ۱۳۸۸، به‌راحتی ردپای مقررات کنوانسیون جرائم سایبر و تأثیراتش به‌وضوح دیده می‌شود. البته این تأثیرپذیری و الگوبرداری نه‌تنها در قوانین کشور ایران، بلکه در بیشتر مقررات مربوط به جرائم فضای سایبر مصوب سایر دول جهان قابل مشاهده است. با وجود کاستی‌هایی

1. Budapest
2. Budapest Convention on Cybercrime of 23 November 2001.

که این کنوانسیون دارد، در حال حاضر کامل‌ترین سند به‌منظور حل مسائل و تعارضاتی است که جهان امروزه از جهت جرائم مربوط به فضای سایبر خود را با آن روبه‌رو می‌بیند. کنوانسیون بوداپست مشتمل بر فصل‌های مختلفی است که کشورها ترغیب به الگو قرار دادن جرم‌انگاری‌های آن شده‌اند. از کشورهایی که به این کنوانسیون ملحق می‌شوند، خواسته شده تا در حوزهٔ قوانین ماهوی خود جرم‌انگاری‌هایی را صورت دهند، در حوزهٔ شکلی نیز توصیه‌هایی در متن این کنوانسیون مشاهده می‌شود.

ضرورت تصویب مقررات کیفری جهانی حاکم بر فضای مجازی و وضعیت ایران

با توجه به مطالب ذکرشده، «مفهوم مرزهای جغرافیایی و فیزیکی در تعیین مرزها در فضای مجازی نقشی ندارند. پس در این زمینه و برای تعیین حدود اعمال صلاحیت جزایی در فضای سایبر و جرائم رایانه‌ای به چه طریقی می‌توان تصمیم گرفت و تعیین صلاحیت کرد؟ دکترین سنتی در زمینهٔ حاکمیت، شبکه را یک دنیای خاص نمی‌داند، بلکه رابط انتقال پیام از یک مکان به مکان دیگر می‌داند (فراندا،[1] ۲۰۰۱: ۱۰۹). با این حال، با توجه به طبع این ارتباطات، اعمال حاکمیت داخلی نسبت به معاملات اینترنتی یا جرائم اینترنتی و تحلیل عواقب آن با استفاده از این دکترین ممکن نیست (حسنی و همکاران، ۱۳۹۳: ۷۰-۶۸).

تحلیل مشکلات عمدهٔ ایجادشده به‌وسیله جرائم رایانه‌ای نشان می‌دهد که فناوری اطلاعات مستلزم تلاش‌های تقنینی جدید در زمینه‌های مختلف حقوقی است. این تلاش‌ها باید در سطح بین‌المللی هماهنگ شود.

علاوه‌بر خلأهای ماهوی موجود در مورد جرائم رایانه‌ای در سطح بین‌المللی، مشکلات شکلی زیادی نیز بروز می‌کند. «برای نمونه احتمال ارتکاب جرم از طریق پردازش از راه دور داده‌ها در یک کشور با نتایج حاصل در کشور دیگر، ممکن است سبب شود دادگاه‌های چند کشور با استناد به اصل سرزمینی بودن به‌طور همزمان خود را برای رسیدگی به این جرم صالح بدانند. برای اجتناب از آثار تعقیب مضاعف شاید بازنگری تعاریف مربوط به دادگاه صالح (به‌خصوص اصل سرزمینی بودن) و کنوانسیون‌های بین‌المللی مربوط به احاله دعاوی ضروری باشد.

به‌درستی گفته می‌شود که «آیین دادرسی پلی است برای رساندن مجرم به سزای اعمال مجرمانه‌اش. این پل باید مستحکم باشد. اصول آیین دادرسی کیفری همچون محاکمهٔ عادلانه و حق دفاع در حال حاضر جزء حقوق اساسی بشر قرار گرفته‌اند. مسئلهٔ تحقیق جرائم رایانه‌ای

1. Franda

مشکلات خاص خود را دارد. این مشکلات ناشی از طبع خاص فضای مجازی است. برای پیگیری این جرائم و تحقیق دربارهٔ آنها سطح خاصی از تخصص مورد احتیاج است، همان‌گونه‌که برای ارتکاب آنها هم به تخصص احتیاج است. کمیسیون اروپا راهکارهایی برای تحقق تخصص در امر تعقیب جرائم رایانه‌ای پیش‌بینی کرده است که شامل آموزش‌هایی برای پلیس‌ها می‌گردد» (شیرزاد، ۱۳۸۸: ۱۳۴). ازاین‌رو مسئلهٔ تحقیق و تعقیب جرائم رایانه‌ای با تصویب یک قانون شکلی هماهنگ یا متحدالشکل نیز امکان‌پذیر می‌شود، قانونی که حاوی راه‌حل‌های گسترده‌ای برای گشایش مشکلات تحقیق، تعقیب و رسیدگی باشد، تحقیق جرائم رایانه‌ای به‌دلیل ویژگی منحصربه‌فردشان بسیار پیچیده است و لاجرم قوانین شکلی را از حالت سنتی خارج می‌کند و حاکمیت‌ها را مجبور به معاضدت در سطح گسترده می‌نماید تا جایی که جهانیان به این نکته پی ببرند که معاضدت در حد کنوانسیون‌های دوجانبه یا چندجانبه کافی نیست و تنها قانون واحد و متناسب با شرایط این نوع جرائم پاسخگوی امر تحقیق خواهد بود.

بنابراین، هر مکانی که مراکز تولیدکنندهٔ بسترهای الکترونیکی که به‌اصطلاح مراکز دادهٔ اینترنتی خوانده می‌شود، درون آن قرار داشته باشد و از لحاظ فنی به ارائهٔ خدمات میزبانی و ملزومات تبعی آن می‌پردازد و توانایی بیشتری برای تحقیق و پیگرد این جرائم را دارد، جزء قلمرو حاکمیت کشور به‌شمار می‌رود و تحت صلاحیت سرزمینی قرار می‌گیرد، زیرا دسترسی بیشتری به مجرم و ابزارهای او وجود دارد. هنگامی‌که بر مبنای یکی از معیارهای تعیین صلاحیت، کشور صالح به رسیدگی تعیین شد، طبعاً آیین دادرسی همان کشور هم برای رسیدگی به این جرائم به‌کار خواهد رفت. اما به‌رغم لزوم تصمیم‌گیری و حل‌وفصل مسائل جهانی در زمینهٔ صلاحیت در حوزهٔ جرائم فضای مجازی، تاکنون هیچ اقدام عملی و لازم‌الاجرایی در عرصهٔ بین‌المللی صورت نگرفته است. نمونهٔ بارز آن کنوانسیون اروپایی جرائم سایبر است که به‌واقع بی‌تأثیرترین ضوابط آن را به مقررات راجع به صلاحیت کیفری اختصاص داده است (حسنی و همکاران، ۱۳۹۳: ۱۵۹). به‌منظور تشخیص کشور صالح به رسیدگی در جرائم سایبر و اعمال یکی از اصول صلاحیت باید به طبع این جرائم و نحوهٔ ارتکاب آنها توجه کرد. در خصوص کشورهایی که مبادرت به تصویب قوانین جدید کرده‌اند، می‌توان تبعیت از دو رویهٔ کلی را ملاحظه کرد: «اول، محل استقرار سامانه‌های رایانه‌ای و دوم، محل حضور بارگذار و پیاده‌ساز شبکه‌ای. در بحث از محل استقرار سامانه‌های رایانه‌ای به‌عنوان محل ارتکاب جرائم در فضای مجازی، منظور از سامانه‌های رایانه‌ای تنها رایانه‌های شخصی نیستند، هرچند نمونهٔ بارز آن به‌شمار می‌آیند، اما باید مفهوم موسع آن را مورد توجه قرار داد. اما در اعمال رویهٔ دوم یعنی محل حضور بارگذار و پیاده‌ساز شبکه‌ای برای اعمال صلاحیت باید دانست که به‌طور کلی کنشگران اصلی فضای سایبر از دو حالت کلی خارج نیستند؛ بدین‌صورت که یا داده‌ها را در قالب فایل‌های مختلف با پسوندهای متفاوت در آن می‌گنجانند که در این صورت به آنها بارگذار

می‌گویند یا اینکه داده‌ها را از این فضا دریافت می‌کنند که به آنها پیاده‌ساز می‌گویند. در اینجا بارگذار، اطلاعات موردنظر خود را در فضای تخصیص‌یافته از سوی ارائه‌کنندهٔ خدمات میزبانی قرار می‌دهد تا متعاقباً پیاده‌ساز به آنها دسترسی یابد. هیچ نیازی نیست که آنها از هویت یکدیگر آگاهی داشته باشند. بنابراین نباید آنها را با فرستنده و گیرنده که معمولاً هویت آنها در ارتباطات الکترونیکی معلوم است، اشتباه گرفت؛ زیرا در اینجا آن هدف خاص از مبادلهٔ اطلاعات که در ارتباطات طرفینی وجود دارد مشاهده نمی‌شود» (خداقلی، ۱۳۸۳: ۳۲). هر کشوری که قصد اعمال صلاحیت سرزمینی بر این نوع از جرائم را دارد، باید به این مسئله توجه خاص کند. اما هنگامی‌که بحث تعارض صلاحیت‌ها پیش می‌آید، برای حل مسئله باید صلاحیت غیرمبتنی بر حیطه‌بندی‌های جغرافیایی، سیاسی و طبیعی انتخاب شود. ازاین‌رو برخی بیان می‌کنند که ملاک تعیین مرجع قضایی صالح، فقط عبور از قواعد سنتی و در نظر گرفتن موقعیت بزه‌دیده است؛ یعنی چنانچه بزه‌دیده‌های جرائم فضای سایبر 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 می‌توان تحقیقات مقدماتی را از آنجا آغاز کرد و امکان جمع‌آوری آثار جرم در آنجا وجود دارد، محلی است که بزه‌دیده در آن اقامت داشته، دست‌کم نمایی از جرم در فضای مجازی علیه داده‌ها یا سامانه‌های او رؤیت‌پذیر است (میسن[1]، ۱۹۹۶: ۲۱).

برای تعیین صلاحیت رسیدگی به جرائم رایانه‌ای، «کنوانسیون جرائم سایبر» در مادهٔ ۲۲ مقرر می‌دارد: ۱. هر یک از اعضا باید به‌گونه‌ای اقدام به وضع قوانین و مقررات کنند که در صورت لزوم، صلاحیت رسیدگی به هر یک از جرائم مندرج در مواد ۲ تا ۱۱ این کنوانسیون را در موارد ارتکابی زیر داشته باشند: الف) جرم در قلمروش ارتکاب یابد؛ ب) جرم در کشتی‌ای ارتکاب یابد که پرچم آن کشور را برافراشته است؛ ج) جرم در هواپیمایی ارتکاب یابد که مطابق مقررات آن عضو، ثبت شده است؛ د) جرم موردنظر مطابق قوانین جزایی توسط تبعه‌اش ارتکاب یا جرم در خارج از قلمرو سرزمینی کشورها ارتکاب یافته است. به‌نظر می‌رسد حتی تدابیری که در این کنوانسیون برای برداشتن موانع شکلی اندیشیده شده است، جامع نیست و در شرایطی که تعارض صلاحیت پیش می‌آید، چندان کارگر نمی‌افتد. با این همه حتی اگر چنین راه‌حل‌هایی بتواند بخشی از مشکلات را حل‌وفصل کند، باز هم ضمانت اجرای بسیار قوی در سطح جهانی را می‌طلبد که این کنوانسیون فاقد چنین ضمانت اجرایی است و مفاد آن برای کشورهایی که عضو این کنوانسیون هستند، حالت پیشنهادی دارد و صرفاً سعی دارد الگویی به نهاد قانونگذاری کشورهای عضو جهت تدوین و تصویب مقررات حاکم بر جرائم در فضای مجازی ارائه دهد. بنابراین، نمی‌توان انتظار داشت که کشورهای عضو حاکمیت خود را به نفع مقررات مربوط به صلاحیت که در «کنوانسیون جرائم سایبر» آمده است، کنار بگذارند. اما

1. Meessen

زمانی‌که قانون متحدالشکلی در سطح بین‌المللی به تصویب برسد، قانونی که نیازها و مناسبت‌های این فضای رو به رشد را لحاظ کرده و دارای ضمانت اجرای قوی باشد، بدون شک اعضای جامعهٔ بین‌المللی که هر روز بیش از گذشته خود را با مشکلات این فضا درگیر می‌بینند و نیازمند قانونی جامع‌اند، بدان خواهند پیوست و حتی حاضرند از بخشی از حاکمیت خود به نفع اجرای این مقررات، بگذرند.

در سال‌های اخیر علاوه‌بر اسناد مذکور، اقدامات مثبت دیگری در زمینهٔ مبارزه با این‌گونه جرائم در نقاط مختلف جهان انجام گرفته است. برای مثال می‌توان از دستورالعمل سال ۲۰۰۰ اتحادیهٔ اروپا در خصوص تجارت الکترونیک، دستورالعمل آن اتحادیه در سال ۲۰۱۳، کنوانسیون عربی ۲۰۱۰ مبارزه با جرائم فناوری اطلاعات، موافقت‌نامهٔ شانگهای ۲۰۱۰ در مورد همکاری در زمینهٔ امنیت بین‌المللی اطلاعات و بالاخره پیش‌نویس کنوانسیون ۲۰۱۲ اتحادیهٔ آفریقا در خصوص تأسیس چارچوبی حقوقی در آفریقا در مورد امنیت در فضای مجازی نام برد.[1] با توجه به خصلت منطقه‌ای این‌گونه اسناد، امید می‌رود با همکاری جامعهٔ بین‌المللی و با الهام از تجربهٔ نظام‌های ملی و تحقیقات مؤسسات غیردولتی مبارزه با جرائم سایبری زمینهٔ تصویب سندی جهانی در رویارویی با جرائم در فضای مجازی فراهم شود.

اگرچه امکان عضویت از طریق دعوت به الحاق مطابق مادهٔ ۳۷ کنوانسیون بوداپست برای کشورهایی چون جمهوری اسلامی ایران وجود دارد، ایران به این کنوانسیون که نخستین معاهدهٔ بین‌المللی است که در جست‌وجوی هماهنگ کردن قوانین ملی، بهبود شیوه‌های تحقیقاتی و افزایش همکاری میان ملت‌ها در زمینهٔ جرائم رایانه‌ای یا اینترنتی (البته فعلاً با قلمرو محدود) است، نپیوسته است. اما ردپای آن و تأثیرات ناشی از تحولات و فعالیت‌های سازمان‌های منطقه ای و بین‌المللی در مورد حقوق سایبر را به‌خوبی می‌توان در کشور مشاهده کرد. تأکید برنامه‌های توسعهٔ پنج‌سالهٔ کشور بر اختصاص شعبه یا شعبی از دادگاه‌ها برای بررسی جرایم االکترونیکی، تصویب قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای سال ۱۳۷۹ (به‌خصوص مواد ۱۳، ۱۴ و ۱۵ آن)، سیاست‌های کلی شبکه‌های اطلاع‌رسانی رایانه‌ای از سوی مقام رهبری در سال ۱۳۸۰، تصویب قانون تجارت الکترونیک سال ۱۳۸۲ (به‌خصوص باب چهارم آن در مورد جرائم و مجازات‌ها) اقتباس‌شده از قانون نمونهٔ تجارت الکترونیکی آنسیترال[2]، قانون وظایف و اختیارات وزارت ارتباطات و فناوری اطلاعات مصوب ۱۳۸۲، قانون نحوهٔ مجازات اشخاصی که در امور سمعی و بصری فعالیت‌های غیرمجاز می‌کنند مصوب سال ۱۳۸۶، دستورالعمل رئیس قوهٔ

1. E-Commerce Directive 2000/31/CE; EU Directive 2013/40 of 12 August 2013; Arab Convention on Combating Information Technology Offences of 2010; Shanghai Cooperation Organization Agreement on Cooperation in the Field of International Information Security of 2010, and the draft African Union Convention on the Establishment of a Legal Framework Conducive to Cybersecurity in Africa of 2012.
2. United Nations Commission on International Trade Law(UNCITRAL)

قضاییه در مورد توسعهٔ کاربری فناوری اطلاعات و ارتباطات در دستگاه قضایی و استقرار نرم‌افزار مدیریت پروندهٔ قضایی سال ۱۳۸۶، تصویب قانون مبارزه با پولشویی ۱۳۸۶ در پی افزایش جرائم مالی و اقتصادی ناشی از پدیدهٔ جهانی شدن و پیشرفت‌ها در فناوری اطلاعات و ارتباط[1]، الحاق ایران به کنوانسیون سازمان ملل متحد مبارزه با فساد ۱۳۸۷ (مریدا، ۲۰۰۳)، قانون جرائم رایانه‌ای سال ۱۳۸۸، قانون انتشار و دسترسی آزاد به اطلاعات سال ۱۳۸۸ مصوب مجمع تشخیص مصلحت (به‌خصوص مواد ۲۱ و ۲۲ آن در مورد مسئولیت مدنی و کیفری)، تشکیل شورای عالی مجازی در سال ۱۳۹۰ و بخش دهم قانون آیین دادرسی کیفری ۱۳۹۲ در خصوص آیین دادرسی جرائم رایانه‌ای (مواد ۶۶۴ تا ۶۸۷)، از مهم‌ترین موارد تلاش برای تطبیق قوانین و نهادهای داخلی با نظام جهانی فضای مجازی است.

سلاح دیجیتالی کرم اینترنتی «استاکس نت» در سال‌های ۲۰۰۹ و ۲۰۱۰ اولین بار علیه تأسیسات هسته‌ای ایران به‌کار گرفته شد و پیش‌بینی می‌شود که نسل جدید سلاح‌های سایبری پیشرفته‌تر است و در آنها از روشی بسیار متفاوت با استاکس نت و با قدرت تخریبی بسیار بیشتری استفاده شود. اکنون این نگرانی به‌طور جدی وجود دارد که جنگ سایبری ممکن است به نتایج فاجعه باری برای همهٔ کشورها در قرن بیست‌ویکم منجر شود. ازاین‌رو ضرورت دارد دولت جمهوری اسلامی ایران نیز با ایجاد بسترهای مناسب و بالا بردن توان الکترونیکی خود و به‌منظور جلوگیری از چنین فجایعی نسبت به خود یا علیه سایر کشورها در جهت طراحی و تصویب مقررات الزام‌آور بین‌المللی حاکم بر اینترنت و فضای سایبر فعالیت کند.

نتیجه‌گیری

جهانی شدن پدیده‌ای فراگیر است که هر روز بیش از گذشته مرزها را در می‌نوردد و به تمامی عرصه‌های زندگی جهانیان ارتباط می‌یابد. حقوق نیز یکی از عرصه‌هایی است که هم از این فرایند تأثیر پذیرفته و هم بر آن تأثیر گذاشته است. این نوشتار در خصوص تأثیرپذیری حقوق کیفری و به‌طور خاص حقوق کیفری جرائم در فضای مجازی از فرایند جهانی شدن و همچنین ضرورت و نیازی که این عرصه به جهانی شدن و بین‌المللی شدن و تصویب قوانین یکنواخت دارد، به مطالعه پرداخت. یکنواخت‌سازی قانون، همچنین به ساده‌سازی، انسجام قوانین حقوقی پراکنده و نظام‌مند شدن حقوق منجر خواهد شد. به‌علاوه، قانون واحد، میزان اختلافات حقوقی را کاهش می‌دهد و حتی در مواردی به ساده تر شدن سطح اختلافات منجر می‌شود.

تهدیدات و جرائمی در سطح جهان وجود دارد که مقابله با آنها جز با همکاری‌ها و معاضدت‌های ملی، منطقه‌ای، بین‌المللی و جهانی در زمینهٔ جرم‌انگاری، فراهم آوردن امکانات،

---

۱. البته هنوز ایران به کنوانسیون پالرمو مقابله با جرائم سازمان‌یافتهٔ فراملی سال ۲۰۰۰ نپیوسته است.

تبادل اطلاعات، تأمین دلیل و جمع‌آوری ادله، شناسایی متهمان، اعمال صلاحیت کیفری، تعقیب، مجازات و استرداد مرتکبان آنها و بالاخره شناسایی و اجرای دستورها و احکام کیفری در پرونده‌های جرائم سایبری فراهم نمی‌شود، جرائم سایبری در این دسته از جرائم جای می‌گیرند. این نوع جرائم به‌سبب ویژگی‌ها و مختصاتی که دارند، ضرورت این‌گونه همکاری‌ها را هر روز بیش از قبل به جهانیان گوشزد می‌کنند. جرائم فضای سایبر، علیه تمامیت، محرمانگی و دسترس‌پذیری سیستم‌های رایانه‌ای یا شبکه‌های مخابراتی ارتکاب می‌یابند یا اینکه از خدمات چنین شبکه‌هایی برای ارتکاب جرائم سنتی استفاده می‌شود. ویژگی فرامرزی این‌گونه از جرائم، با سرزمینی بودن اختیارات مجریان قانون تعارض دارد، ازاین‌رو کشورهای مختلف با همکاری و مذاکره به این نتیجه رسیده‌اند که این عرصه را تحت قاعده درآورند و بر آن اعمال نظارت کنند. البته نهادها و سازمان‌های بین‌المللی متعددی در زمینهٔ حقوق کیفری و همچنین حقوق کیفری جرائم در فضای مجازی دست به فعالیت زده‌اند و مقررات و قوانینی را به‌صورت پیشنهادی و با هدف الگومداری و نه دقیقاً در جهت متحدالشکل‌سازی، به جهانیان عرضه داشته‌اند تا شاید بتوان با قوایی بین‌المللی و هماهنگ به مقابله با این جرم در حال توسعه و پیشرفت، پرداخت. از میان این نهادهای بین‌المللی کنوانسیون جرائم سایبر برجسته‌تر و کامل‌تر به‌نظر می‌رسد، زیرا علاوه‌بر گنجاندن محتویات پیشنهادی سایر نهادها، با سازوکار جدیدتری روی کار می‌آید. این برجستگی تا جایی پیش می‌رود که ردپای محتویات آن در قوانین داخلی کشورها به‌صورت محسوس دیده می‌شود، اما همچنان جای خالی قانونی متحدالشکل و لازم‌الاجرا در این عرصه خالی است، قانونی که محدودیت‌ها را بردارد، حافظ حقوق حاکمیتی دول عضو باشد و جنبه های مختلف سیاسی، فرهنگی، اجتماعی و اقتصادی کشورها را رعایت کند تا در مسیر هماهنگی کیفری توفیق یابد.

منابع

۱. فارسی

الف) کتاب‌ها

۱. استون، هیک (۱۳۸۶). *حقوق بشر و اینترنت*، ترجمه و تحقیق سید قاسم زمانی و مهرناز بهراملو، تهران: خرسندی.

۲. جاویدنیا، جواد (۱۳۸۸). *جرائم تجارت الکترونیکی*، چ دوم، تهران: خرسندی.

۳. جلالی فراهانی، امیرحسین (۱۳۸۹). *درآمدی بر آیین دادرسی کیفری جرائم سایبری*، تهران: خرسندی.

۴. ---------- (۱۳۸۹). *کنوانسیون جرائم سایبر و پروتکل الحاقی آن*، تهران:

خرسندی.
۵. جوانمرد، بهروز (۱۳۹۳). *آیین دادرسی کیفری اختصاصی(افتراقی) در جرایم سازمان‌یافتهٔ فراملّی*، تهران: جاودانه.
۶. جوانمردی صاحب، مرتضی (۱۳۹۴). *نظریهٔ قلمرو زدایی سرزمینی از حقوق جزا ماهیت، مبانی و ساختار*، تهران: شهردانش.
۷. حسنی، علیرضا؛ پهلوانی‌فرد، احسان (۱۳۹۳). *بررسی تطبیقی قانون جرائم رایانه‌ای در حقوق ایران و حقوق بین‌الملل*، تهران: مجد.
۸. خداقلی، زهرا (۱۳۸۳). *جرائم کامپیوتری*، تهران: آریان.
۹. زندی، محمدرضا (۱۳۹۳). *تحقیقات مقدماتی در جرایم سایبری*، تهران: جنگل.
۱۰. زیبر، اولریش (۱۳۸۳). *جرائم رایانه‌ای*، ترجمهٔ محمدعلی نوری، رضا نخجوانی، مصطفی بختیاروند و احمد رحیمی مقدم، چ دوم، تهران: کتابخانهٔ گنج دانش.
۱۱. شیرزاد، کامران (۱۳۸۸). *جرائم رایانه‌ای از دیدگاه حقوق ایران و حقوق بین‌الملل*، تهران: بهینه فراگیر.
۱۲. شیروی خوزانی، عبدالحسین (۱۳۹۲). *حقوق تطبیقی*، چ دوازدهم، تهران: سمت.
۱۳. عالی‌پور، حسن (۱۳۸۹). *حقوق کیفری فناوری اطلاعات*، تهران: خرسندی.
۱۴. عاملی، سعیدرضا (۱۳۹۰). *رویکرد دوفضایی به آسیب‌ها، جرائم، قوانین و سیاست‌های فضای مجازی*، چ دوم، تهران: امیر کبیر.
۱۵. فضلی، مهدی (۱۳۸۹). *مسئولیت کیفری در فضای سایبر*، تهران: خرسندی.
۱۶. کیسی، اوئن (۱۳۸۶). *دلایل دیجیتالی و جرم رایانه‌ای (علم قانونی، رایانه‌ها و اینترنت)*، ترجمهٔ امیرحسین جلالی فراهانی و علی شایان، معاونت حقوقی و توسعهٔ قضایی قوهٔ قضائیه، تهران: سلسبیل.
۱۷. گرکی، مارکو (۱۳۸۹). *جرائم سایبری: راهنمایی برای کشورهای در حال توسعه*، ترجمهٔ مرتضی اکبری، تهران: نیروی انتظامی جمهوری اسلامی ایران، پلیس امنیت فضای تولید و تبادل اطلاعات(افتا).
۱۸. محمد نسل، غلامرضا (۱۳۸۵). *مجموعه مقررات دیوان بین‌المللی کیفری*، تهران: دادگستر.

ب) مقالات

۱۹. پورنقدی، بهزاد (۱۳۹۱). «پدافند غیرعامل و بررسی تهدیدات نظم و امنیت در فضای سایبری»، *فصلنامهٔ علمی ـ تخصصی دانش انتظامی کردستان*، دورهٔ سوم، ش ۱۱، ص ۸۳-۱۰۴.

۲۰. جلالی فراهانی، امیرحسین (۱۳۸۷). «جنبه‌های حقوقی اقدامات کیفری بین‌المللی مجریان قانون در قبال جرائم سایبری»، *فصلنامهٔ مطالعات پیشگیری از جرم*، سال سوم، ش ۸، ص ۷۶-۵۷.
۲۱. جلالی فراهانی، امیرحسین؛ منفرد، محبوبه (۱۳۹۲). «حمایت قانونی از آسیب‌دیدگان سایبری»، *مجلهٔ مجلس و راهبرد*، سال بیستم، ش ۷۳، ص ۲۰۲-۱۵۵.
۲۲. جلالی، محمود؛ قاسمی، وحید (۱۳۹۴). «قلمرو انطباق رویکرد قانونگذار ایران با مقررات متحدالشکل مقابله با فساد در کنوانسیون مریدا»، *فصلنامهٔ مطالعات حقوق عمومی*، دورهٔ ۴۵، ش ۳، پاییز ۱۳۹۴، ص ۴۰۳-۳۸۱.
۲۳. جلالی، محمود؛ مقامی، امیر (۱۳۸۹). «روند جهانی شدن حقوق کیفری و تأثیر آن بر حقوق ایران»، *فصلنامهٔ حقوق*، مجلهٔ دانشکدهٔ حقوق و علوم‌سیاسی دانشگاه تهران، دورهٔ ۴، ش ۷، ص ۹۷-۷۷.
۲۴. جلالی، محمود؛ مقامی، امیر (۱۳۸۷). «کارکرد حقوق بین‌الملل در فرایند جهانی شدن حقوق»، *فصلنامهٔ حقوق*، مجلهٔ دانشکدهٔ حقوق و علوم سیاسی دانشگاه تهران، دورهٔ ۴۱، ش ۳، ص ۱۱۶-۹۷.
۲۵. جوان جعفری، عبدالرضا (۱۳۸۹). «جرائم سایبر و رویکرد افتراقی حقوق کیفری»، *مجلهٔ دانش و توسعه*، سال هفدهم، ش ۳۴، ص ۱۹۳-۱۷۰.
۲۶. جوان جعفری، عبدالرضا (۱۳۹۰). «جرائم سایبر و چالش‌های نوین سیاست کیفری»، *مجموعه مقالات همایش جهانی شدن حقوق و چالش‌های آن*.
۲۷. دلماس مارتی، میری (۱۳۷۸). «جهانی شدن حقوق، فرصت‌ها و خطرات»، ترجمهٔ اردشیر ارجمند، *مجلهٔ حقوقی بین‌المللی*، ش ۲۴.
۲۸. عالی‌پور، حسن (۱۳۸۳). «جرم‌های مرتبط با محتوا: محتوای سیاه فناوری اطلاعات»، *مجموعه مقالات و سخنرانی‌های ارائه‌شده در همایش بررسی جنبه‌های حقوقی فناوری اطلاعات، معاونت حقوقی و توسعهٔ قضایی قوهٔ قضائیه*، مرکز مطالعات توسعهٔ قضایی با همکاری شورای عالی اطلاع‌رسانی کشور، تهران: سلسبیل.
۲۹. عالی‌پور، حسن (۱۳۹۲). «امنیت ملی و عدالت کیفری»، *فصلنامهٔ مطالعات راهبردی*، ش ۶۱، ص ۸۸-۵۷.
۳۰. لقمانی، سلیم (۱۳۷۶). «تکاپو در جهت مشروعیت دموکراتیک»، ترجمهٔ ابراهیم بیگ‌زاده، *مجلهٔ تحقیقات حقوقی*، ش ۲۰.

ج) پایان‌نامه‌ها

۳۱. شکوری، معصومه (۱۳۸۹). *قلمرو انطباق ایران با قواعد متحدالشکل بین‌المللی در عرصهٔ*

حقوق قراردادها، پایان نامه کارشناسی ارشد رشتهٔ حقوق خصوصی، دانشگاه اصفهان، دانشکدهٔ علوم اداری و اقتصاد، گروه حقوق.

۳۲. عالی‌پور، حسن (۱۳۸۷). *توازن میان امنیت ملی و آزادی‌های فردی در مقابله با جرائم تروریستی*، رسالهٔ دکتری حقوق کیفری و جرم‌شناسی، دانشگاه شهید بهشتی، دانشکدهٔ حقوق و علوم سیاسی.

۳۳. کلانتری، امیرحسین (۱۳۹۳). *امکان‌سنجی پیشگیری از جرم در فضای سایبر*، پایان‌نامهٔ کارشناسی ارشد رشتهٔ حقوق جزا و جرم‌شناسی، دانشگاه اصفهان، دانشکدهٔ علوم اداری و اقتصاد، گروه حقوق.

۳۴. مقامی، امیر (۱۳۸۷). *بین‌المللی شدن حقوق کیفری و تأثیرات آن بر نظام حقوقی ایران*، پایان‌نامهٔ کارشناسی ارشد حقوق بین‌الملل، دانشگاه پیام نور، دانشکدهٔ علوم انسانی، گروه حقوق.

۲. انگلیسی

A) Books

35. Akehurts, Micheal Barton (2005).*A Modern Introduction to International Law*, London, Hyman, 6th ed.

36. Albero, Martin (1999). *A Perspective on Globalization*, Lynne Reinner publisher.

37. Andrev, Jones (2006). *Dictionary of Globalization*, Cambridge: Polity Press.

38. Carey, Peter (1999). *Media Law*, Sweet and Maxwell Publishing, Second Edition, london.

39. Daly, Herman (2005). *Globalization Versus Internationalization*: *Some Implications: Universal Norms in Biotheics.*

40. David, John (1998). *Cases and Materials on International Law*, London, Sweet and Maxwell, 5th ed.

41. Etter, Barbara (2006). Director, Australasian Center for Policing Research, *Computer Crime, Paper Presented at the 4th National Outlook Symposium on Crime in Ausralia*.

42. George B. Delta, Jeffery H. Matsuura (2008). *Law of Internet*, London, Aspen Publishers.

43. Graham. J & H. Smith (2002). *Internet Law and Regulation*, London, Sweet and Maxwell, 4th ed.

44. Herzog J. B (1957). *Les Principes et Les Methodes du Droit Penal Compare*, Revue Internationale de Droit Compare

45. Franda, Marcus (2001). *Governing the Internet*, London, Lynne Rienner Publisher.

46. Norris, Gareth (2005). *Emerging Cyber Threats Reports Australian Internet*

Hate Site, Bond University.
47. Reed Ch., (1993). *Computer Law*, 2nd Ed., Blackstone Press.
48. Stuart, Biegle (2001). *Beyond Our Control? Cofronting the Limits of Our Legal System in the Age of Cyberspace*. The MIT Press. Cambridge, Massachusett, London England.

B) Articles
49. Brenner, Susan (2004). "Toward A Criminal Law for Cyberspace: Product Liability and Other Issues", *Journal of Technology Law and Policy*, Fall, Vol.23, No.2, pp. 65-88.
50. Brenner, Susan (2010). "Cyber Crime Investigation and Prosection: the Role of Panel and Procedural law", *Law Murdooh University Electronic Jornal of Law*, Vol.18, No.2, pp 5-20.
51. Carolis, Daniele De (2010). "Some Features of the Harmonization of International Trade Law in the Third Millennium", *Uniform Law Review*, Vol.15, No.1, pp. 91-105.
52. Keenan, Patric (2006). *The New Deterrence: Crime and Policy in the Age of Globalization*, Law Review, Vol.91, No.5, pp. 68-91.
53. Messen, Karl (1996). "Extraterritorial Jurisdiction in Theory and Practice", *The Hague, Kluwer Law International, Vol. 32, No.1, pp. 19-38.*

C) Websites
54. http://www.penal.org/en/resolutions-aidp-iapl-congresses
55. http://www.penal.org/en/resolutions-last-congress
56. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf