

اصول بنیادین مقررات گذاری اینترنت

خدیدجه اکرمی*

هدی غفاری**

ولی رستمی***

چکیده

با وجود این که حقوق اینترنت پدیده‌ی حقوقی نسبتاً جدیدی است؛ اما برخی از اصول آن در حال تکامل است. پنج اصل بنیادین مقررات گذاری اینترنت شامل آزادی ارتباطات اینترنتی، احترام به حریم خصوصی، اصل صلاحیت سرزمینی، مشارکت ذی نفعان و همکاری دولت‌ها است؛ از این رو هدف پژوهش حاضر، تحلیل حقوقی از اصول بنیادین مقررات گذاری اینترنت در چارچوب موازین حقوقی است تا علاوه بر نظریه-پردازی در این زمینه، راهنمایی برای تنظیم‌گری اینترنت از سوی قانون‌گذار ملی کشورمان باشد. این تحقیق از نوع توصیفی-تحلیلی است و اطلاعات لازم نیز با استفاده از روش کتابخانه‌ایی جمع‌آوری گردیده و تنظیم شده است. بر مبنای یافته‌های تحقیق، می‌توان ادعا کرد که اصول بنیادینی در ارتباط با تنظیم-گری اینترنت در سطح بین‌المللی ظهور یافته است که می‌تواند راهنمای عملی کشورها در مقررات گذاری فضای مجازی قرار گیرد. نظام مقررات گذاری اینترنت در ایران در مقایسه با اصول اساسی مقررات گذاری اینترنت، مطلوب نیست. نتیجه این که در وضعیت کنونی، نظام مقررات گذاری اینترنت در بحث آزادی ارتباطات اینترنتی به دنبال حداکثرسازی محدودیت‌ها است. نهاد مقررات‌گذار در این خصوص عموماً نهادهای انتصابی هستند. حریم خصوصی در اینترنت در زمینه‌ی مقررات گذاری با وجود حمایت‌های قانونی؛ اما همچنان کاستی‌هایی دارد. مدل تنظیم‌گری اینترنت یک مدل کاملاً دولتی و بدون مشارکت ذی نفعان است و در زمینه‌ی مشارکت و همکاری‌های بین‌المللی، تمایلی به همکاری با سایر دولت‌ها در زمینه‌ی مقررات گذاری اینترنت وجود ندارد.

کلیدواژه‌ها: آزادی اینترنت، حریم خصوصی، صلاحیت سرزمینی، همکاری دولت‌ها، مشارکت ذی نفعان

*. دانشجوی گروه حقوق عمومی، دانشکده حقوق، الهیات و علوم سیاسی، واحد علوم تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران.
kh_akrami@yahoo.com

** . استادیار، دانشکده حقوق و علوم سیاسی، دانشگاه علامه طباطبائی، تهران، ایران (نویسنده مسئول)
hodaghfari@yahoo.com

***. استاد گروه حقوق عمومی دانشکده حقوق و علوم سیاسی دانشگاه تهران، تهران، ایران
vrostami@ut.ac.ir

مقدمه

اینترنت تغییرات شگفت‌انگیزی در زندگی مردم در سرتاسر جهان ایجاد کرده است و به اصلی‌ترین عنصر زندگی بشر در زمان حاضر تبدیل شده است. امروزه وابستگی مردم جهان به اینترنت، به شکل چشمگیری افزایش یافته است. حوزه‌هایی؛ مانند ارتباطات، آموزش، تجارت و غیره به شکل قابل توجهی متکی به اینترنت است. اینترنت هم‌چنین ابزاری لازم برای اعمال حقوق بنیادین بشر؛ مانند حق دسترسی به اطلاعات و حق بر آزادی بیان است. مقررات‌گذاری فضای مجازی از مسائل مهم و اساسی است که همواره با چالش‌هایی رو به رو است. دولت‌ها بر مبنای اصل صلاحیت سرزمینی، از حق انحصاری تنظیم‌گری اینترنت در قلمرو سرزمینی خود برخوردار هستند؛ با این حال اصول مقررات‌گذاری اینترنت در حال شکل‌گیری است که راهنمای قوانین ملی در زمینه‌ی مقررات‌گذاری اینترنت است و اختیارات مطلق دولت ملی را در این زمینه کاسته است؛ برای مثال در عرصه‌ی بین‌المللی اصول آزادی بیان و آزادی اطلاعات مانع از اعمال محدودیت بر دسترسی به اینترنت با استفاده از ابزار سانسور است.

از این رو، این تحقیق در صدد ارائه‌ی الگویی برای مقررات‌گذاری اینترنت بر مبنای اصول بنیادینی است که در این زمینه ظهور یافته و در حال تکامل است. اهمیت تحقیق از آن جهت است که نتایج این تحلیل‌ها می‌تواند راهنمای قانون‌گذار کشورمان در تنظیم مقررات مرتبط با اینترنت باشد و نیز پیامدهای عدم توجه به این اصول را متذکر گردد. ضرورت انجام تحقیق را می‌توان به این شکل توجیه کرد که تاکنون نظام مقررات‌گذاری اینترنت در ایران از حیث اصول مقررات‌گذاری اینترنت به شکل جامع مورد آسیب‌شناسی و نقد قرار نگرفته است و از این جهت انجام موضوع این تحقیق ضرورت دارد.

سؤالات تحقیق آن است که چه اصولی باید راهنمای مقررات‌گذاری ملی در رابطه با فضای سایبری در عصر اینترنت باشد؟ نظام مقررات‌گذاری اینترنت در ایران در ارتباط با اصول بنیادین مقررات‌گذاری اینترنت چه وضعیتی دارد؟ فرضیه‌ی نخست این که مقررات‌گذاری اینترنت باید بر مبنای اصول بنیادین حقوق بین‌الملل اینترنت که ظهور یافته و در حال تکامل است انجام گیرد. فرضیه‌ی دوم این که مقررات‌گذاری اینترنت در ایران در مقایسه با اصول بنیادین مقررات‌گذاری اینترنت کاستی‌هایی دارد.

در سازمان‌دهی این پژوهش ابتدا پنج اصل اساسی و بنیادین در رابطه با مقررات‌گذاری بین‌المللی اینترنت که عبارت است از: ۱. اصل آزادی اینترنت، ۲. اصل احترام به حریم خصوصی، ۳. اصل صلاحیت سرزمینی به شکل اصلاحی خود در رابطه با فضای سایبری، ۴. اصل همکاری بین‌الدولی، ۵. اصل مشارکت کلیه‌ی ذی‌نفعان بحث خواهد شد و سپس با نظام مقررات‌گذاری اینترنت در ایران مقایسه می‌گردد.

گفتار اول: آزادی ارتباطات اینترنتی

آزادی بیان، یکی از آزادی‌های اساسی در اینترنت محسوب می‌گردد. بند ۲، ماده ۱۹ میثاق حقوق مدنی و سیاسی این آزادی را در سطح جهانی تضمین می‌کند. در اروپا، حق مشابهی در ماده ۱۰ کنوانسیون اروپایی حقوق بشر به رسمیت شناخته شده است. بند ۲، ماده ۱۹ میثاق حقوق مدنی و سیاسی به صراحت به آزادی بیان از طریق هر نوع رسانه به انتخاب خود شخص، اشاره نموده است. اطلاعات و ایده‌هایی که در روی یک صفحه وب بیان می‌گردد در چارچوب ماده ۱۰ کنوانسیون اروپایی، قرار می‌گیرد.^۱

در دعوی روزنامه تایمز علیه دولت بریتانیا، دادگاه اروپایی حقوق بشر بر این عقیده بود که آرشیوهای اینترنتی را می‌توان در قلمرو ماده ۱۰ گنجانده؛^۲ زیرا آزادی بیان، آزادی اطلاعات را نیز شامل می‌گردد؛^۳ بنابراین نه تنها ارائه دهندگان محتوا بلکه هم‌چنین کاربران ساده اینترنت را نیز شامل می‌گردد.^۴ حمایت‌های مقرر در ماده ۱۹ میثاق بین‌المللی حقوق مدنی و سیاسی و ماده ۱۰ کنوانسیون اروپایی حقوق بشر، از آزادی بیان در خصوص مجلات الکترونیکی نیز صادق است. در دعوی فتولایف علیه جمهوری آذربایجان، دادگاه اروپایی حقوق بشر به صراحت شبکه‌های اجتماعی در اینترنت که از محبوبیت بالایی برخوردار هستند را مشابه رسانه‌های چاپی از جهت تأثیرگذاری تلقی کرد.^۵ لازم است خاطر نشان گردد که هر دو رأی صادره، آزادی بیان را صرف‌نظر از مرزها تضمین می‌کند. این امر به‌ویژه در رابطه با اینترنت که مرزهای ملی را به چالش کشیده است، اهمیت دارد.^۶

در رابطه با محدودیت آزادی بیان در اینترنت با وجود تأکید بر آزادی اینترنت؛ اما دادگاه اروپایی حقوق بشر اهمیت کنترل دولت را در دعوی مگادات علیه کشور مولداوی تصدیق نمود.^۷ بند ۳، ماده ۱۹ میثاق حقوق مدنی و سیاسی و بند ۲، ماده ۱۰ کنوانسیون اروپایی حقوق بشر این ساختار را انعکاس داده است. هر دو سند حاوی فهرستی از اهداف مشروعی است که می‌تواند دخالت دولت در آزادی بیان را توجیه نمایند. این اهداف شامل اصولی و علائقی؛ مانند آزادی سایر افراد، امنیت ملی، نظم عمومی و اخلاق حسنه است.

1-Eur. Court H.R. Perrin v. United Kingdom, Judgment of 18 October 2005.

2-Eur. Court H.R., Times Newspapers Ltd v. United Kingdom (nos. 1 and 2), Judgment of 10 March 2009

3-Ibid .

4-Eur. Court H.R., Fatullayev v. Azerbaijan, Judgment of 22 April 2010

5-Wenzel, Nicola, Opinion and Expression, Freedom of, International Protection, MPEPIL, Rüdiger Wolfrum, 2009

6-Eur. Court H.R., Megadat.com SRL v. Moldova, Judgment of 8 April 2008

در صورت تعارض، برقراری یک تعادل منصفانه بین منافع رقیب ضرورت دارد.^۱ این تعادل باید به لحاظ معیارهایی که در بند ۳، ماده ۱۹ میثاق حقوق مدنی و سیاسی و بند ۲، ماده ۱۰ کنوانسیون اروپایی حقوق بشر مقرر شده است، ایجاد گردد و مداخله‌ی دولت در محدودیت آزادی ارتباطات اینترنتی باید متناسب با اهداف مشروعی باشد که محدودیت آزادی بیان در راستای آن اهداف انجام می‌گیرد.^۲

اصل بیست و چهارم قانون اساسی ایران، به آزادی مطبوعات و نشریات اشاره دارد و به‌نظر می‌رسد منظور از تدوین این اصل، اصل آزادی بیان و عقیده است؛ چرا که این امر بدیهی است که یک عقیده و اندیشه تا زمانی که ظاهر و ابراز نشود نمی‌تواند مورد مؤاخذه و تعرض قرار گیرد؛ بنابراین می‌توان حق آزادی بیان و اندیشه را از این اصل استنباط نمود.^۳ بر مبنای اصل ۲۴ قانون اساسی، باید پذیرفت که اصل آزادی ارتباطات اینترنتی در نظام حقوقی ایران پذیرفته شده است؛ با این حال این آزادی با محدودیت‌هایی مواجه است. در ایران طبق ماده ی ۲۲ قانون جرائم رایانه‌ای، وظیفه‌ی پالایش فضای مجازی برعهده‌ی کمیته تعیین مصادیق مجرمانه (ماده ۲۲ قانون جرائم رایانه‌ای) قرار دارد. کارگروه مصادیق مجرمانه^۴ به استناد تبصره ۲ ماده ۲۲ قانون جرائم رایانه‌ای^۵ کارگروه کمیته، موظف است به شکایات راجع به مصادیق پالایش (فیلتر) شده رسیدگی و نسبت به آن‌ها تصمیم‌گیری کند. مسئول اجرای محدودیت آزادی ارتباطات اینترنتی در فضای مجازی است.

در مصوباتی که در ارتباط با فضای مجازی تصویب شده است محدودیت آزادی بیان در فضای مجازی تعیین شده است. شورای عالی انقلاب فرهنگی پیرو تصویب و ابلاغ سیاست‌های کلی شبکه‌های اطلاع رسانی رایانه‌ای از سوی مقام رهبری، ضوابط شبکه اطلاع‌رسانی رایانه‌ای را در سال ۱۳۸۰ تصویب نمود. مقرر شد شورای عالی انقلاب فرهنگی شامل چندین آیین‌نامه است.

در ماده ی ۶، آیین‌نامه واحدهای ارائه کننده ی خدمات اطلاع‌رسانی و اینترنت رسا، به ممنوعیت تولید و عرضه توهین و افتراء به مقدّسات اسلامی و رهبری و مقامات حکومتی و اشخاص حقیقی و حقوقی اشاره کرده است. ضمانت اجرای تخطی از موارد مندرج در

1-Eur. Court H.R., Von Hannover v. Germany, Judgment of 24 June 2004, Reports of Judgments and Decisions 2004-VI

2-Ehlers,Dirk, General Principles, in European Fundamental Rights And Freedoms, Dirk Ehlers ed.,2007.

۳. انصاری، باقر، **حقوق رسانه**، چاپ دهم، تهران: انتشارات سمت، ۱۳۹۰.

۴. ماده ۲۲ قانون جرائم رایانه‌ای

۵. «کارگروه (کمیته) موظف است به شکایات راجع به مصادیق پالایش (فیلتر) شده رسیدگی و نسبت به آن‌ها تصمیم‌گیری کند»

آیین‌نامه طبق ماده ۹؛ شامل تذکر، قطع موقت مجوز، لغو پروانه و طرح در دادگاه و محاکم قانونی است. هم‌چنین در ماده ۷، آیین‌نامه‌ی دفاتر خدمات اینترنت مصوب شورای عالی انقلاب فرهنگی، تولید و عرضه توهین و افتراء به مقدّسات اسلامی، مقامات حکومتی توسط شبکه‌های انتقال اطلاعات رایانه‌ای ممنوع اعلام شده است.

بررسی عملکرد در ارتباط با آزادی بیان در فضای مجازی در سال‌های اخیر نشان دهنده‌ی اتخاذ رویکرد حداکثری در فیلترینگ است؛ به‌طوری که در حوزه‌ی اخلاقی، سیاسی و اعتقادی، به دو روش استفاده از لیست سیاه و فیلترینگ بر اساس کلید واژه‌ها، سایت‌های مورد نظر را غیر قابل دسترس می‌کند و گسترده‌ی فیلترینگ سایت‌های اینترنتی بسیار وسیع است.^۱

در ارتباط با آسیب‌شناسی آزادی ارتباطات اینترنتی در ایران می‌توان استدلال نمود که محدودیتی که به موجب مصوبات قانونی فوق مقرر شده بسیار کلی و مبهم است و در نتیجه موجب حاکمیت رویکرد حداکثر محدودیت فضای مجازی در ایران شده است و از سوی دیگر اختیارات وسیع کمیته تعیین مصادیق مجرمانه در محدودیت‌سازی اینترنت نیز قابل انتقاد است.

گفتار دوم: اصل احترام به حریم خصوصی

اصل احترام به حریم خصوصی، هم‌چنین در قوانین بین‌المللی حقوق بشر گنجانده شده است. ماده ۱۷، میثاق حقوق مدنی و سیاسی از زندگی خصوصی و خانوادگی و اقامتگاه یا مکاتبات اشخاص حمایت می‌کند. ماده ۸ کنوانسیون اروپایی حقوق بشر، حق احترام به زندگی خصوصی و خانوادگی افراد را مطرح کرده است. هر دو ماده حوزه‌ی شمول گسترده‌ایی دارند که به‌طور خاص توسط دادگاه اروپایی حقوق بشر توسعه داده شده است؛ بنابراین نامه‌های الکترونیکی نیز تحت حمایت‌های مقررات این دو ماده قرار می‌گیرند. سایر داده‌هایی که از طریق اینترنت منتقل می‌گردند یا از طریق اینترنت قابل دسترس می‌باشند به زندگی خصوصی اشخاص تعلق دارد مگر این‌که امکان دسترسی برای عموم از سوی خود شخص اجازه داده شود. در دعوای کوپلند علیه دولت بریتانیا، دادگاه اروپایی حقوق بشر تردیدی در شناسایی استفاده اشخاص از اینترنت به‌عنوان بخشی از زندگی خصوصی و مکاتبات خود نداشت.^۲

در نتیجه، کنترل دولت بر استفاده‌ی خصوصی از محتویات اینترنت از جمله نامه‌های الکترونیکی، معادل مداخله‌ی خودسرانه تلقی می‌گردد. همین استدلال در خصوص تعهدات

۱. سعد، علی، درآمدی بر سیاست‌های فیلترینگ سایت‌های اینترنتی، فصلنامه مطالعات رسانه‌های نوین، سال اول شماره ۲، ۱۳۹۴، ص ۲۱.

2-Eur. Court H.R., Copland v. United Kingdom, Judgment of 3 April 2007.

ارائه دهندگان خدمات اینترنتی به نگهداری داده‌ها به شکلی که در ماده ۳ دستورالعمل اتحادیه ی اروپا، در خصوص نگهداری داده‌هایی که در ارتباط با مقررات مربوط به ارائه‌ی خدمات الکترونیکی در دسترس عموم قرار دارد، تولید یا پردازش می‌شود نیز صادق است. در صورتی که کارکنان دولتی چنین اطلاعاتی را منتشر نمایند یا در صورتی که قانون‌گذار تکلیفی را در خصوص انتشار اطلاعات خصوصی افراد در اینترنت تحمیل نماید همان‌طور که دادگاه اروپایی حقوق بشر مقرر داشته، نوعی دخالت دولت در زندگی خصوصی افراد محسوب می‌گردد؛^۱ بنابراین مشروعیت دخالت دولت در حریم خصوصی در اینترنت نیازمند توجیهات ویژه‌ای است.

تهدید حریم خصوصی در اینترنت تنها از سوی مقامات دولتی نیست؛ بلکه هم‌چنین اشخاص و شرکت‌های خصوصی نیز ممکن است تهدیدی علیه حریم خصوصی باشند. برخی شرکت‌ها یا انجمن‌ها مقادیر زیادی از داده‌های شخصی را نگهداری می‌کنند که در صورت سرقت و یا هر نوع سوءاستفاده می‌تواند تهدیدی علیه شخص باشد یا به او آسیب برساند. به‌علاوه، هر شخص ممکن است از انتشار اطلاعاتی در رابطه با خود اینترنت متأثر گردد در چنین شرایطی دولت‌ها تعهدات مثبتی جهت حمایت از حریم خصوصی دارند.

این الزام دولت‌ها به‌طور خاص در بند ۲، ماده ۱۷ اعلامیه جهانی حقوق بشر به‌صراحت بیان شده است که مطابق با آن هر کسی حق دارد در مقابل این‌گونه مداخلات یا تعرضات نسبت به زندگی خصوصی خود، از حمایت‌های قانونی برخوردار گردد. با این‌حال، تمرکز صرف بر رعایت حریم خصوصی در مواردی اشکالاتی ایجاد می‌کند.

در برخی موارد، حمایت از حریم خصوصی با آزادی اینترنت در تعارض قرار می‌گیرد. در این حالت، این دو اصل راهنما در زمینه‌ی استفاده از اینترنت در تعارض قرار می‌گیرند؛ باوجود این که آزادی بیان را می‌توان در راستای حقوق دیگران به‌طور خاص حق بر حریم خصوصی محدود نمود؛ اما هر نوع محدودیتی باید متناسب با اهدافی باشد که دنبال می‌گردد. دولت‌ها باید تعادلی منصفانه بین حریم خصوصی از یک سو و آزادی اینترنت از سوی دیگر، ایجاد نمایند.^۲

در دعوایی علیه دولت فنلاند، شخص ناشناسی اعلامیه‌ایی را به نام پسری ۱۲ ساله در یک سایت اینترنتی قرار داد. در آن زمان ارائه دهندگان خدماتی اینترنتی به‌موجب قوانین فنلاند ملزم نبودند هویت شخصی که اعلامیه را قرار داده است، افشاء نمایند؛ بنابراین تعقیب آن شخص ناممکن گردید. از دید دادگاه اروپایی حقوق بشر دولت فنلاند نتوانسته به تعهدات مثبت خود جهت حمایت از حریم خصوصی آن شخص عمل نماید.

1-Eur. Court H.R., Wypych v. Poland, Judgment of 25 October 2005.

۲. در رابطه با تعارض حریم خصوصی با آزادی مطبوعات نگاه کنید به رای دیوان اروپایی حقوق بشر mutatis mutandis, Eur. Court H.R., von Hannover, paras. 57-58.

3-K. U. v. Finland, Judgment of 2 December 2008.

اگر حریم خصوصی به حوزه‌های حریم خلوت و تنهایی یا حریم مکانی،^۱ حریم اطلاعاتیو حریم ارتباطی^۲ و حریم جسمانی^۳ طبقه‌بندی شوند، قانون‌گذار اساسی در اصل بیست و پنجم به صراحت به ممنوعیت تجاوز به حریم خصوصی افراد اشاره کرده است. در این اصل، بدون آن‌که به آزادی ارتباطات تصریح شده باشد به استثنای این آزادی اشاره شده و حریم خصوصی ارتباطات در مورد شایع‌ترین وسایل ارتباطی مورد حمایت قرار گرفته است.^۴

در حال حاضر، دو «قانون تجارت الکترونیک مصوب ۱۳۸۳» و «قانون جرائم رایانه‌ای مصوب ۱۳۸۸» به‌طور خاص از داده‌های شخصی در فضای مجازی حمایت کرده است. قانون تجارت الکترونیک در ماده ۵۸، به اصل رضایت در جمع‌آوری و پردازش اطلاعات وضعیت جسمانی، روانی و یا جنسیتی اشخاص اشاره شده است. در ماده ۵۹ این قانون شرایط ذخیره، پردازش و توزیع داده پیام شخصی در بستر مبادلات الکترونیکی تعیین شده است. در ماده ۷۱ و ۷۲ این قانون، برای نقض حریم خصوصی جسمانی برخلاف ماده ۵۹ مذکور ضمانت اجرای کیفری تعیین کرده است.

ایراد اساسی قانون تجارت الکترونیک این است که تنها تعرض به حریم خصوصی جسمانی اشخاص در فضای مجازی را منع کرده است؛ درحالی‌که در فضای مجازی، حریم خصوصی اطلاعات و ارتباطات که اهمیت بالایی دارد نیز باید تحت شمول حمایت‌های قانون قرار گیرد؛ بنابراین نقض حریم خصوصی افراد در فضای مجازی از طریق تلاش برای دسترسی به اطلاعات و داده‌هایی که شخص از طریق ابزارهای الکترونیکی (نامه‌های الکترونیکی) انتقال می‌دهد فاقد حمایت است. این امر باعث عدم ترغیب کاربران ایرانی به استفاده از پیام‌رسان‌های داخلی شده است.

ماده ۱ و ماده ۲ قانون جرائم رایانه‌ای به‌طور خاص، در ارتباط با حمایت از حریم خصوصی در فضای مجازی است. حمایت‌های این قانون جنبه‌ی کیفری دارد. ماده ۱ این قانون، نقض اصل تحصیل مجاز و مشروع اطلاعات شخصی افراد را جرم‌انگاری کرده است.

۱. حریم خصوصی ارضی در برگزیده یکی از ابتدایی‌ترین و سنتی‌ترین اشکال حق افراد دایر بر لزوم محترم و مصون از تعرض بودن منازل مسکونی است. (امام‌وردی، محمدحسن، ماهیت‌شناسی حق بر حریم خصوصی در نظام حقوقی ایران، مجله حقوق خصوصی، دوره ۱۴، شماره ۲، ۱۳۹۶، ص ۳۴۹)

۲. حریم ارتباطی شامل مصون ماندن ارتباطات اشخاص از هر گونه تعرض است. در فضای مجازی این بحث به شکل امنیت داده‌های که در حال پردازش است مطرح است.

۳. حریم خصوصی جسمانی در باب حمایت از تمامیت جسمانی و اطلاعات مربوط به سلامتی انسان است. (انصاری، باقر، حق بر حریم خصوصی، تهران: انتشارات سمت، ۱۳۹۱، ص ۱۲۳).

۴. انصاری، باقر، حریم خصوصی و حمایت از آن در حقوق اسلام-تطبیقی و ایران، مجله دانشکده حقوق و علوم سیاسی، شماره ۶۶، ۱۳۸۳، ص ۳۵.

ماده ۲ این قانون، به بحث حمایت از حریم خصوصی اطلاعات و ارتباطات مرتبط است. در این ماده ششود غیرقانونی در فضای مجازی که به معنای دریافت داده‌های در حال انتقال یا به هر نحوی دسترسی به آن‌ها است.^۱ در ماده ۱۷ این قانون نیز از حریم خصوصی جسمانی شامل صوت، تصویر و یا فیلم خصوصی زندگی در فضای مجازی حمایت کرده است؛ اما این حمایت را مقید به اضرار به هتک حیثیت آن شخص نموده است. یکی از نوآوری‌های قانون جرائم رایانه‌ای نسبت به قانون تجارت الکترونیک، حمایت از حریم خصوصی اطلاعات و مکاتبات افراد در فضای مجازی است و از این جهت این اقدام قانون‌گذار قابل تقدیر است؛ بنابراین در حال حاضر ششود غیرقانونی مکاتبات اشخاص در فضای مجازی نیز ممنوع و جرم است؛ اما در خصوص حمایت از حریم خصوصی جسمانی این ایراد اساسی باقی است که این حمایت در ماده ۱۷، مقید به ضرر و یا هتک حیثیت شخص قربانی نموده که از این جهت قابل انتقاد است.

گفتار سوم: اصل صلاحیت سرزمینی

اصل صلاحیت سرزمینی در حوزه ی مقررات گذاری اینترنت، از دو جهت قابل بحث است. نخست از جهت اعمال تنظیم‌گری اینترنت و دوم اعمال صلاحیت نسبت به جرائم اینترنتی.

بند اول: صلاحیت سرزمینی در ارتباط با مقررات گذاری اینترنت

بر مبنای اصل صلاحیت سرزمینی، دولت‌ها می‌توانند در ارتباط با کلیه‌ی موضوعات در قلمرو سرزمینی خود قانون‌گذاری و یا عمل تنظیم‌گری را انجام دهند؛ بنابراین هر دولت صلاحیت دارد که در رابطه با اینترنت در قلمرو سرزمینی خود مقررات‌گذاری نماید. این مقررات‌گذاری شامل تنظیم جنبه‌های فنی اینترنت، تعریف جرائم اینترنتی، آیین رسیدگی به این جرائم و ... می‌باشد.

تنظیم‌گری اینترنت با توجه به ویژگی‌های آن، وضعیت خاصی دارد. صرف نظر از واقعیت روشن تسلط چند کشور محدود بر بخش قابل توجهی از زیرساخت‌های مهم اینترنت هیچ فرد، دولت یا مؤسسه‌ی تجاری مالک آن نیست. اینترنت توسط یک مدیریت واحد اداره نمی‌شود؛ اما برای حفظ جنبه‌های فنی و سیاست‌های زیرساختی، نهادی به نام «انجمن اینترنت برای اسامی و اعداد تعیین شده»^۲ وجود دارد.^۳ با وجود این که هر دولتی بر مبنای

۱. فتحی، یونس، شاهمرادی، خیراله (۱۳۹۶) گسترده و قلمرو حریم خصوصی در فضای مجازی، مجله حقوقی دادگستری، شال هشتاد و یکم، شماره نود و نهم، ۱۳۹۶، ص ۳.

2-Internet Corporation for Assigned Names and Numbers – ICANN.

۳. رضایی، مهدی؛ بابازاده مقدم، حامد، اصول تدوین قوانین و مقررات برای اینترنت با تأکید بر مصوبات یونسکو و شورای اروپا، فصلنامه پژوهش حقوق عمومی، سال پانزدهم، شماره ۴۲، بهار ۱۳۹۳، ص ۵۴.

قاعده صلاحیت سرزمینی، می‌تواند آزادانه نسبت به تنظیم‌گری فضای سایبری اقدام نماید؛ اما در این خصوص الزامات بین‌المللی مقرر شده است. طبق اصل ۴۸ اعلامیه اصول، مصوب سازمان ملل متحد، مقررات‌گذاری اینترنت باید چندجانبه، شفاف، دموکراتیک و با مشارکت کامل دولت‌ها و بخش خصوصی و نهادهای جامعه مدنی و سازمان‌های بین‌المللی باشد.^۱ در نتیجه کشورها در اعمال صلاحیت سرزمینی خود در رابطه با مقررات‌گذاری اینترنت، با محدودیت‌هایی مواجه هستند. مقررات‌گذاری اینترنت باید شفاف و دموکراتیک باشد و دولت باید در مشارکت با سایر ذی‌نفعان اقدام نماید؛ حتی این الزام مقرر شده که دولت در مقررات‌گذاری اینترنت باید سازمان‌های بین‌المللی را مشارکت دهند که این موضوع نوعی تحدید صلاحیت سرزمینی دولت‌ها است.

نتیجه این‌که صلاحیت دولت در خصوص مقررات‌گذاری اینترنت در قلمرو سرزمینی خود؛ مانند سایر موارد مقررات‌گذاری دولت، انحصاری نیست و باید به‌شکل مشارکتی انجام گیرد. از سوی دیگر، اینترنت در حال تبدیل شدن به حقّ مستقل بشری است؛ بنابراین مقررات‌گذاری اینترنت باید با احترام به اصول بنیادین حقوق بشر و همچنین اصول حقوق بشر در حال ظهور مرتبط با اینترنت انجام گیرد.^۲

بند دوم: اصل صلاحیت سرزمینی در جرائم فضای سایبری

صلاحیت سرزمینی دولت‌ها بر جرائم فضای سایبری بر دو مبنا اعمال می‌گردد: نخست، دکترین^۳ آثار^۴ که صلاحیت را به دولتی اعطاء می‌کند که عمل مجرمانه در قلمرو آن آثاری دارد و دوم، کد دامنه سطح بالای^۵ که قلمرو سایبری کشورها محسوب می‌گردد. بر مبنای دکترین آثار جرم نیز در قلمرویی روی می‌دهد که آثار جرم در آن‌جا نمایان گردیده است؛^۶ بنابراین دولت‌ها بر مبنای این نظریه، توانایی و اختیار اعمال صلاحیت نسبت به بیگانگان در خارج از کشور که رفتار آن‌ها آثاری را در قلمرو دولت ایجاد کرده است را دارند. کمیته‌ی وزیران شورای اروپا، دکترین اثر را در نظریه تفسیری خود درباره‌ی

۱. قاجار قیونلو، سیامک، مقدمه حقوق سایبری، تهران، انتشارات میزان، ۱۳۸۶، ص ۱۶۲.

۲. در رابطه با ارتباط حقوق بشر و اینترنت ر.ک: اکرمی خدیجه؛ غفاری، هدی و رستمی ولی، «دسترسی به اینترنت حق مستقل بشری: رویکرد نظام حقوق بین‌الملل و نظام حقوقی ایران»، فصلنامه تحقیقات حقوق خصوصی و کیفری، ۱۴۰۰.

۳. محبی، محسن؛ صفایی‌عبدالحسین، صلاحیت فراسرزمینی بر اساس دکترین آثار در حقوق بین‌الملل، نشریه مطالعات حقوق تطبیقی، دوره ۹، شماره ۲، ص ۸۵.

4-The Effects Doctrine.

5-Code Top Level Domain.

6-Vaughan Lowe & Christopher Staker Jurisdiction in International Law, Malcom D. Evans ed, 2010.

ماده ۲۲ کنوانسیون اروپایی حقوق بشر در رابطه با جرائم سایبری مورد تأیید قرار داد. بر طبق دیدگاه این کمیته، دولت‌ها نه تنها باید اصل صلاحیت سرزمینی را در وضعیتی که هم شخص حمله‌کننده به سیستم رایانه‌ای و هم سیستم رایانه‌ای مورد حمله در درون یک قلمرو قرار دارند اعمال نمایند؛ بلکه هم‌چنین در جایی نیز این صلاحیت باید اعمال گردد که سیستم رایانه‌ای مورد حمله، در دورن قلمرو یک کشور قرار داشته باشد؛ حتی اگر حمله‌کننده در خارج از قلمرو آن کشور باشد.^۱

به‌موجب دکترین تأثیرگذاری وسیع،^۲ صلاحیت صرفاً بر مبنای این حقیقت به‌وجود می‌آید که مقام تعقیب‌کننده وب‌سایتی که حاوی محتوای مضر است را از محل کار یا میز خود مشاهده می‌کند. در قضیه پرین، دادگاه بریتانیا یک تبعه فرانسه را به دلیل انتشار محتوای مستهجن بر روی یک وب‌سایت آمریکایی محکوم کرد؛ زیرا افسر پلیس آن محتویات را در ایستگاه پلیس لندن مشاهده کرده بود.^۳

دکترین تأثیرگذاری به شکل مشروط، در رابطه با صلاحیت کشورها برای رسیدگی به جرائم رایانه‌ای به‌طور گسترده از سوی دادگاه‌ها و نویسندگان حقوقی پذیرفته شده است؛^۴ بنابراین تلاش‌های متعددی صورت گرفته تا این که دکترین تأثیر را به شیوه‌ای محدود نمایند که ماهیت فراسرزمینی فضای سایبری در آن لحاظ گردد. دادگاه‌های ایالات متحده آمریکا در اعمال صلاحیت بر جرائم رایانه‌ای، بر «دکترین تأثیرگذاری معقول»^۵ متکی هستند. با این توضیح که اعمال صلاحیت بر مبنای آثار ناشی از رفتار بیگانگان در خارج از کشور مشروط به «مستقیم»، «ماهوی»، و «قابل پیش‌بینی بودن» و «اثر» دانسته است؛ بنابراین اعمال صلاحیت بر مبنای دکترین آثار مشروط به این است که جرمی که در خارج از ایالات متحده آمریکا ارتکاب یافته است آثار آن به اندازه کافی گسترده بوده و زیان قابل توجهی نیز وارد نموده باشد.^۶

اعمال صلاحیت کشورها بر مبنای دکترین تأثیرگذاری در شکل نامحدود، نه تنها نقض حاکمیت سایر کشورها می‌باشد؛ بلکه هم‌چنین منجر به تقابل با اصل آزادی اینترنت

1-Available at: <http://conventions.coe.int/treaty/en/reports/html/185.htm>.

2-Wide Effects Doctrine.

3-Eur. Court H.R. Perrin v. United Kingdom, Judgment of 18 October 2005

4-Kohl, op cit, p 49.

5-Reasonable Effects Doctrine.

6-Zippo Manufacturing Co. v. Zippo Dot Com Inc., US District Court for the Western District of Pennsylvania, 952 F.Supp. 1119, at 1124, W.D.Pa. 2009, p 306-307

۷. محبی، محسن؛ صفایی، عبدالحسین، صلاحیت فراسرزمینی بر اساس دکترین آثار در حقوق بین‌الملل، نشریه مطالعات حقوق تطبیقی، دوره ۹، شماره ۲، ۱۳۹۷.

می‌گردد. در صورتی که تولیدکنندگان محتوا در فضای سایبری مجبور شوند که دسترسی کاربران خارجی را به دلیل ترس از این که در خارج از کشور خود مورد تعقیب و یا محاکمه قرار گیرند مسدود نمایند، آزادی بیان صرف‌نظر از مرزهای آن؛ همان‌طور که در بند ۲ میثاق بین‌المللی مدنی و سیاسی مقرر شده، نقض می‌گردد.

به نظر می‌رسد دکتترین تأثیر به‌شکل محدود، معیاری معقول برای اعمال صلاحیت در فضای مجازی است. دامنه سطح بالای کد کشورها در اینترنت برای نمونه UK برای کشور پادشاهی متحد^۱ یا PL برای لهستان^۲ را نیز می‌توان به‌عنوان قلمرو سایبری خاص کشورها تلقی کرد و معیاری برای اعمال صلاحیت سرزمینی باشد. این دامنه‌ها به فهرستی از کدهای کشورها اشاره دارد که به‌وسیله‌ی سازمان بین‌المللی استانداردسازی (ایزو)^۳ ایجاد شده است. در سال ۱۹۸۰ میلادی، دامنه‌های سطح بالای عمومی با هفت پسوند (.com, .org, .net, .mil, .gov, .edu) ایجاد شدند.

در نظام حقوقی ایران، دکتترین تأثیرگذاری به‌شکل مشروط و دامنه‌های سطح بالای اینترنتی به‌عنوان مبنایی برای صلاحیت رسیدگی به جرائم فضای سایبری از سوی ایران پذیرفته شده است. مطابق بند (ج) ماده ۲۸ قانون جرائم رایانه‌ای ایران، دادگاه‌های ایران در موارد زیر صالح به رسیدگی خواهند بود. جرم توسط هر ایرانی یا غیر ایرانی در خارج از ایران علیه سامانه‌های رایانه‌ای و مخابراتی و تارنماهای مورد استفاده یا تحت کنترل قوای سه‌گانه یا نهاد رهبری یا نمایندگی‌های رسمی دولت یا هر نهاد و مؤسسه‌ای که خدمات عمومی ارائه می‌دهند یا علیه تارنماهای دارای دامنه‌ی مرتبه‌ی بالای کد کشوری ایران در سطح گسترده ارتکاب یافته باشد.^۴

مطابق بند (ب) ماده ۲۸، (آئین‌نامه مرکز خدمات داده اینترنتی مصوب ۱۳۸۳ کمیسیون تنظیم مقررات و ارتباطات رادیویی)، وب سایت‌های دارای نام دامنه مرتبه بالای کد کشوری در حکم قلمرو ایران است.^۵

1-United Kingdom.

2-Poland.

3-International Organization for Standardization.

۴. جلالی‌فراهانی، امیرحسین، صلاحیت کیفری سایبری در پرتوی قوانین داخلی، حقوق فن‌آوری اطلاعات و ارتباطات (مجموعه مقالات). تهران: انتشارات روزنامه رسمی جمهوری اسلامی ایران، ۱۳۸۵، ص ۵۳.

۵. افتخارچهرمی، گودرز؛ اسلامی، ابراهیم، نحوه اعمال صلاحیت دادگاه‌ها در رسیدگی به جرائم فضای مجازی، مجله حقوقی دادگستری، شماره هشتاد و هشتم، ۱۳۹۳، ص ۵۲.

گفتار چهارم: همکاری بین دولت‌ها

در رابطه با حکمرانی از طریق اینترنت،^۱ بیش از هر چیزی نیاز به همکاری بین‌المللی احساس می‌شود. از آن جایی که اینترنت مرزهای ملی را به چالش می‌کشد، مسائل عمده در این حوزه را تنها نمی‌توان به‌وسیله‌ی یک دولت به‌تنهایی حل نمود؛ به‌عنوان مثال کلاهبرداری اینترنتی و سایر جرائم مرتباً توسط مجرمان و از طریق سرورهای اینترنتی واقع در خارج از کشور قربانی، ارتکاب می‌یابد.

پیگرد قانونی چنین جرائمی نیازمند تحقیقات در کشورهای مختلف است که این امر نیز همکاری مؤثر کشورها را می‌طلبد. کنوانسیون جرائم سایبری مصوب ۲۰۰۱^۲ نتیجه‌ی این پدیده است؛ زیرا بر این باور استوار است که یک مبارزه‌ی مؤثر در برابر جرائم سایبری به همکاری‌های بین‌المللی گسترده و کارآمد نیاز دارد.

صرف نیاز به همکاری، لزوماً به‌معنای الزام حقوقی دولت‌ها به همکاری در این زمینه نیست. برخی ضرورت‌ها برای همکاری بین دولت‌ها می‌تواند از حقوق بین‌الملل عمومی ناشی گردد؛ برای مثال، یکی از اهدافی که در ماده ۱ منشور سازمان ملل متحد ذکر شده حصول همکاری بین‌المللی در حل مسائل بین‌المللی که دارای جنبه‌های اقتصادی و اجتماعی و فرهنگی یا بشر دوستانه است و در پیشبرد و تشویق احترام به حقوق بشر و آزادی‌های اساسی برای همگان بدون تمایز از حیث نژاد، جنس، زبان و یا مذهب است. اعلامیه اصول حقوق بین‌الملل در زمینه‌ی روابط و همکاری بین‌المللی بین دولت‌ها مطابق با منشور سازمان ملل متحد^۳ (اعلامیه روابط دوستانه) که به‌عنوان تفسیری معتبر از منشور می‌تواند تلقی گردد، الزام دولت‌ها به همکاری را مورد تأیید قرار می‌دهد؛^۴ با این حال این الزام کلی بسیار انتزاعی است و به سختی می‌توان آن را به‌عنوان یک تکلیف حقوقی خاص تفسیر کرد.^۵

الزامات دولت‌ها به طور خاص به همکاری در رابطه با حل و فصل برخی مشکلات بین‌المللی را می‌توان در معاهدات بین‌المللی؛ مانند «کنوانسیون حقوق کودک»^۶ یافت.^۷

1-Internet governance.

2-The Convention on Cybercrime of 2001.

3-The Declaration on Principles of International Law concerning Friendly Relations and Co-operation among.

4-Schreuer, Christoph, State Sovereignty and the Duty of States to Cooperate – Two Incompatible Notions?, in International Law Of Cooperation And State Sovereignty, Jošt Delbrück ed, 2012, p30

5-Ibid

6-The Convention on the Rights of the Child 1989.

7-GA Res. 44/25 of 20 November 1989.

بند (ج) ماده ۳۳ کنوانسیون حقوق کودک، کشورهای طرف کنوانسیون را ملزم می‌کند که کلیه اقدامات ملی دو و چندجانبه را در جهت جلوگیری از استفاده‌ی استثماری از کودکان در اعمال و مطالب پرونوگرافیک به‌عمل آورند.

به‌دلیل این‌که مطالب پرونوگرافی غالباً از طریق اینترنت از یک دولت به دولت دیگر تبادل می‌یابد، هر گونه واکنش مؤثر باید با همکاری بین دو یا چند دولت صورت گیرد؛ از این‌رو، بند (ج) کنوانسیون حقوق کودک دولت‌ها را ملزم می‌کند که در مبارزه با پرونوگرافی کودکان با هم همکاری نمایند. در نتیجه کنوانسیون جرائم سایبری که جرائم مربوط به پرونوگرافی را در ماده ۹ بیان می‌کند، صریحاً به کنوانسیون حقوق کودک ارجاع می‌دهد.

تعهدات مشابهی را برای دولت‌ها می‌توان از اسناد بین‌المللی حقوق بشر از جمله کنوانسیون اروپایی حقوق بشر استنباط نمود. در دعوی رانتسوف علیه قبرس و روسیه دادگاه اروپایی حقوق بشر بر ماهیت فراملی قاچاق انسان تأکید نمود؛ بنابراین، تعهد مثبت به تحقیقات در زمینه‌ی موارد قاچاق انسان که از ماده ۴ کنوانسیون اروپایی حقوق بشر ناشی می‌گردد، به این عنوان تفسیر می‌گردد که الزام به همکاری مؤثر فراملی را شامل می‌گردد.^۱ این وضعیت هم‌چنین در رابطه با ارتکاب جرم از طریق اینترنت که عموماً بیش از یک دولت را درگیر می‌سازد، صدق می‌کند.

برای نمونه، در دعوی کی.یو علیه فنلاند تاریخ سایت از طریق شخصی خارج از فنلاند که خدمات اینترنتی را ارائه می‌داد کنترل می‌گردید. تکلیف به حمایت از پسر ۱۲ ساله به‌موجب ماده ۸ کنوانسیون اروپایی حقوق بشر، به‌طور ضمنی مستلزم همکاری با دولتی بود که ارائه دهنده‌ی خدمات اینترنتی در آن ساکن بود؛^۲ با این‌حال، الگوی یکسانی در رابطه با تکلیف به همکاری وجود ندارد.

در حقیقت باوجود این‌که دیپلماسی، اساس همکاری بین‌المللی محسوب می‌گردد؛ اما دولت‌ها حتی ملزم به حفظ روابط دیپلماتیک نیستند. اسناد نهایی اجلاس جهانی جامعه اطلاعاتی^۳ نیز در این خصوص ضد و نقیض است.

اعلامیه ژنو^۴ مصوب ۱۲ دسامبر ۲۰۰۳ به این تعهد عمومی برای دولت‌ها منتج گردید که همکاری خود را جهت واکنش مشترک به چالش‌ها و برای اجرای نقشه اقدام که

1-Eur. Court H.R., Rantsev v. Cyprus and Russia, Judgment of 7 January 2010, para 289.

2-K. U. v. Finland, Judgment of 2 December 2008, para 389.

3-World Summit on the Information Society.

این اجلاس به پشتیبانی سازمان ملل متحد در خصوص فناوری اطلاعات و ارتباطات جامعه اطلاعاتی در سال‌های ۲۰۰۳ در ژنو و ۲۰۰۵ در تونس برگزار شد.

3-The Geneva Declaration

چشم‌انداز یک جامعه‌ی اطلاعاتی فراگیر را براساس اصول کلیدی موجود در این اعلامیه را تحقق می‌بخشد، تقویت نمایند؛^۱ با این حال پاراگراف ۴۰ دستورالعمل تونس،^۲ صرفاً تأکید بر ضرورت برای ارتقاء همکاری‌های بین‌المللی است.

اگرچه نیاز به همکاری از سوی دولت‌ها به‌طور کلی پذیرفته می‌شود؛ اما دولت‌ها تمایلی به پذیرش چنین الزامی را ندارند. از جنبه‌ی حقوقی، اصل الزام دولت‌ها به همکاری جایگاه بسیار ضعیفی در حقوق بین‌الملل دارد.

گفتار پنجم: اصل مشارکت چند جانبه

نظام تنظیم‌گری مشارکتی در بردارنده‌ی دولت و مؤلفه‌های غیردولتی است و از این جهت متمایز از نظام خود تنظیمی است که در این شکل اخیر مقررات‌گذاری اینترنت، نهاد مقررات‌گذار بدون دخالت دولت و به‌طور مستقل عمل می‌کند.^۳ مشارکت جامعه مدنی و بخش خصوصی به‌طور سنتی نقش مهمی را در حکمرانی از طریق اینترنت بازی می‌کند. اگرچه توسعه‌ی اینترنت از طریق سرمایه‌گذاری دولت ایالات متحده آمریکا صورت گرفته؛ اما ساختار آن به‌وسیله‌ی جامعه علمی تعیین می‌گردد.

هنگامی که نیاز به ایجاد ساختارهای پایدار برای اداره‌ی سیستم دامنه مرتبه بالای کد کشوری احساس گردید، این وظیفه نه به مقامات دولتی و نه به سازمان‌های بین‌المللی؛ مانند اتحادیه بین‌المللی مخابرات بلکه به یک سازمان غیرانتفاعی با نام «آیکان»^۴ محول گردید. با این حالت ایده حکمرانی اینترنت فراتر از کنترل دولت‌ها، تاکنون نتوانسته واقعیت یابد.

آیکان از ابتدا تحت قراردادی با وزارت بازرگانی ایالات متحده آمریکا قرار داشت.^۵ از آن هنگام، نفوذ دولت افزایش یافته و کمیته‌ی مشورتی دولتی در حال حاضر نهاد مهم کنترل دولتی است؛ بنابراین برنامه دولت ایالات متحده آمریکا برای اعطای استقلال کامل به آیکان هنوز تحقق نیافته است. از اوایل سال ۲۰۰۲ رئیس آیکان خواستار مشارکت بخش عمومی و خصوصی به شکل مؤثری گردید.

1-Doc. WSIS-03/GENEVA/DOC/4-E, para. 65, available at: http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-E.pdf

2-Doc. WSIS-05/TUNIS/DOC/6(Rev.1)E, available at: <http://www.itu.int/wsis/docs2/tunis/off/6rev1.pdf>.

۳. ابدی، سعیدرضا، تنظیم مشارکتی مالیاتی، الگوی جدید در نظام مالیاتی ایالات متحده آمریکا، فصلنامه تحقیقات حقوقی، شماره ۷۱، ۱۳۹۴، ص ۲۱۳.

4-ICANN

۵. به یادداشت تفاهم ۲۵ نوامبر ۱۹۹۸ بین وزارت بازرگانی ایالات متحده و آیکان، مراجعه کنید:

<http://www.icann.org/en/general/icann-mou-25nov98.htm>

در این مدل پیشنهادی نقش اصلی را بخش خصوصی، بازی می‌کند و دولت نقش مشارکت و پشتیبانی را برعهده داشت.^۱ این پیشنهاد به تدریج در حال تحقق یافتن است. نشانه‌های روشنی وجود دارد که رویکرد مشارکت چند جانبه نه تنها در واقعیت در حال تحقق است؛ بلکه هم‌چنین به‌عنوان یک اصل راهنما نیز برای حقوق بین‌الملل اینترنت تلقی می‌گردد.

در راستای تأکید بیشتر بر تعهد به مشارکت، وزارت بازرگانی ایالات متحده آمریکا تعهد خود را به مشارکت چند جانبه با محوریت بخش خصوصی، مدل توسعه سیاست‌گذاری از پایین به بالا برای همکاری فنی در زمینه‌ی دامنه‌های اینترنتی که در راستای منافع کاربران جهانی اینترنت عمل می‌کند را مورد تأیید قرار داد. این موضوع در چارچوبی گسترده‌تر در طی اجلاس جهانی جامعه اطلاعاتی مطرح گردید.

به‌موجب اصول اعلامیه ژنو ۲۰۰۳،^۲ مدیریت اینترنت که شامل هم موضوعات فنی و هم سیاست‌گذاری عمومی می‌گردد باید کلیه‌ی نمایندگان ذی‌نفعان، سازمان‌های دولتی و بین‌الدولی را شامل گردد.^۳ در این رابطه، این اعلامیه به بازیگران متفاوت نقش‌های خاص را واگذار می‌کند. اختیار خط مشی‌گذاری برای موضوعات مربوط به سیاست‌گذاری عمومی در رابطه با اینترنت به دولت‌ها محوّل می‌گردد؛^۴ در حالی که بخش خصوصی باید نقش مهمی در توسعه اقتصادی و فنی اینترنت داشته باشد^۵ در این رابطه نقش ویژه‌ای برای جامعه مدنی پیش بینی شده است.

جامعه مدنی باید نقش مهمی در رابطه با موضوعات مرتبط با اینترنت، در سطح اجتماع بازی نماید.^۶ دو سال بعد، دستور اجلاس‌یه تونس برای جامعه

1-ICANN, President's Report: ICANN – The Case for Reform of 24 February 2002, available at: <http://www.icann.org/general/lynn-reform-proposal-24feb02.htm>

2-Doc. WSIS-03/GENEVA/DOC/4-E, available at: http://www.itu.int/dms_pub/itu/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-E.pdf

۳. اجلاس‌یه جهانی جامعه اطلاعاتی (WSIS)، که با حمایت سازمان‌ملل متحد در طی دو اجلاس‌یه در رابطه با اطلاعات، ارتباطات و در معنای گسترده، جامعه اطلاعاتی در سال ۲۰۰۳ در ژنو برگزار گردید. دور بعدی آن در سال ۲۰۰۵ در تونس تشکیل شد. نخستین مصوبه این اجلاس‌یه اصول اعلامیه ژنو و نقشه اقدام ژنو بود.

۴. اعلامیه ژنو ۲۰۰۳ پارگراف (الف) ماده ۴۹

۵. بند(ب) پارگراف ۴۹ اعلامیه ژنو ۲۰۰۳.

۶. بند (ج) پارگراف ۴۹ همان.

اطلاعاتی^۱ رویکرد چند جانبه‌گرایی که در اعلامیه ژنو مقرر شده بود را بار دیگر در قالب عبارت مشابهی مورد تأیید قرار داد.^۲ این اعلامیه رویکرد مشارکت چند جانبه در کلیه سطوح را پیشنهاد نمود^۳ و نهادی برای حکمرانی اینترنت تحت عنوان «انجمن جدید برای گفتگو در زمینه‌ی سیاست‌گذاری چند جانبه» ایجاد کرد.^۴

رویکرد مشارکت چند جانبه تنها محدود به موضوعاتی مانند سیستم نام دامنه یا آیکان نیست، بلکه برعکس در اجلاس جهانی جامعه اطلاعاتی از مفهومی گسترده‌تر در رابطه با حکمرانی اینترنت حمایت شد که موضوعات سیاست‌گذاری عمومی؛ مانند تعقیب جرائم اینترنتی را شامل می‌گردید.^۵ در حقیقت، همکاری بین ذی‌نفعان متعدد نکته کلیدی اعلامیه ژنو^۶ و دستور جلسه تونس^۷ است. رویکرد چند جانبه‌گرایی تنها محدود به مقررات‌گذاری بین‌المللی در رابطه با اینترنت نیست.

سایر کنفرانس‌های جهانی هم‌چنین بر اهمیت رو به رشد بازیگران غیردولتی تأکید داشته‌اند. با این حال در مقررات‌گذاری بین‌المللی اینترنت، مفهوم مشارکت چندجانبه چنان استحکام یافته که در حال حاضر به شکل یک اصل بنیادین تبدیل شده است. در ایران، در ارتباط با تنظیم‌گری فضای مجازی از مدل کاملاً دولتی استفاده می‌گردد. در سال ۱۳۹۰ با دستور مقام رهبری، شورای عالی فضای مجازی تشکیل گردید. این شورا از ترکیب

1-The Tunis Agenda for the Information Society 2005.

«دستور جلسه تونس برای جامعه اطلاعاتی» در دومین اجلاس سران جهان درباره جامعه اطلاعاتی در تونس در حالی در روزهای شانزدهم تا هجدهم نوامبر ۲۰۰۵ برگزار شد، مصوب گردید که ۱۹۴۰۱ شرکت‌کننده با این ترکیب داشت:

شرکت‌کنندگانی از بخش دولتی و جامعه اروپایی

شرکت‌کنندگانی از سازمان‌های دولتی

شرکت‌کنندگانی از سازمان‌های غیردولتی و جامعه مدنی

شرکت‌کنندگانی از بخش تجاری

و شرکت‌کنندگانی از بخش رسانه‌ای

۲. پاراگراف ۳۵ دستور جلسه تونس.

۳. پاراگراف ۳۷ همان.

۴. پاراگراف ۷۲ همان.

۵. نگاه کنید به پاراگراف های ۴۰ و ۵۶-۶۲ همان

۶. اعلامیه ژنو ۲۰۰۳ پاراگراف های ۱۷، ۲۰، ۳۵، ۶۰، ۶۱.

۷. پاراگراف ۲۷، ۳۹، ۴۱، ۷۱، ۸۳، ۸۸-۸۹ دستور جلسه تونس

اشخاص حقوقی و حقیقی به ریاست رئیس جمهور تشکیل می‌گردد. هر دو دسته اعضای شورا را مقام رهبری منصوب می‌کند. مصوبات آن در حکم قانون است و هیچ نهادی حق ابطال آن را ندارد. هم‌چنین مجلس، حق قانون‌گذاری مغایر با مصوبات شورا را ندارد. این شورا در ارتباط با فضای مجازی نهاد سیاست‌گذار و نهاد مجری محسوب می‌گردد. دستگاه‌های اجرایی به ویژه وزارت ارتباطات و فناوری اطلاعات مجری مصوبات شورای عالی فضای مجازی است. این مدل تنظیم‌گری کاملاً یک مدل تنظیم‌گری دولتی بدون مشارکت ذی‌نفعان غیردولتی است.

نتیجه گیری

در این مقاله تلاش شده است که مدل و چارچوب تنظیمی برای مقررات گذاری و مدیریت اینترنت ارائه گردد. بر مبنای اصل صلاحیت سرزمینی مقررات گذاری و مدیریت اینترنت در انحصار دولت ملی قرار دارد؛ با این حال به لحاظ اهمیت اینترنت در دنیای کنونی و ارتباط نزدیکی که با حقوق بشر دارد در سطح بین‌المللی، اصولی در ارتباط با مقررات گذاری اینترنت شکل گرفته و در حال تکامل است که الزامات و چارچوب الگو و مدل تنظیم‌گری اینترنت در سطح ملی را نیز تشکیل می‌دهد.

یافته‌های تحقیق نشان می‌دهد که اینترنت در وضعیت کنونی مهم‌ترین ابزار حق آزادی بیان است و در عین حال حریم خصوصی افراد را متأثر ساخته است. هم‌چنین ظهور اینترنت بحث‌های جدیدی را در ارتباط با نحوه‌ی اعمال صلاحیت سرزمینی در مقررات گذاری اینترنت و رسیدگی به جرائم ارتكابی در فضای مجازی موجب گردیده است.

در شیوه‌ی مقررات گذاری اینترنت بحث همکاری دولت‌ها و نیز مشارکت سایر ذی‌نفعان راهکار اساسی است. حتی می‌توان از مدل خودتنظیمی فضای مجازی بدون مداخله دولت دفاع نمود؛ بنابراین پنج اصل اساسی در زمینه مقررات گذاری اینترنت در این تحقیق بحث گردید. در نتیجه‌ی این فرضیه این تحقیق اثبات می‌گردد که اصول بنیادینی در سطح بین‌المللی در ارتباط با مقررات گذاری اینترنت شکل گرفته و در حال تکامل است.

نتیجه‌ی تحقیق نشان می‌دهد که تنظیم‌گری فضای مجازی در ایران در مقایسه با اصول بنیادین مقررات گذاری اینترنت با کمبودهایی مواجه است. درباره‌ی تنظیم‌گری حریم خصوصی در فضای مجازی در ایران، قانون تجارت الکترونیک و قانون جرائم رایانه‌ای به‌عنوان تنها اسناد قانونی در باب حمایت از داده‌های اشخاص در فضای مجازی جامعیت ندارند. حریم خصوصی همان‌طور که بحث گردید، ابعاد متعددی دارد؛ در حالی که در قوانین مذکور تنها یک جنبه‌ی خاص مورد حمایت قرار گرفته است.

قانون تجارت الکترونیک تنها به حمایت از حریم خصوصی جسمانی پرداخته و ذکری از سایر اقسام حریم خصوصی نشده است. در قانون جرائم رایانه‌ای از حریم خصوصی اطلاعات و ارتباطات حمایت شده؛ اما این حمایت مقید به اضرار یا هتک حیثیت شخص شده که از این جهت قابل ایراد است و از این‌رو این حمایت باید مطلق باشد. ترس از نقض حریم خصوصی کاربران در فضای مجازی موجب عدم گرایش به استفاده از نرم افزارهای پیام‌رسان داخلی است.

اصلی‌ترین خلاء مقررات گذاری فضای مجازی در ایران، تضمین آزادی ارتباطات اینترنتی است. در این زمینه، سیاست حداکثرسازی محدودیت اینترنت ایران دنبال می‌گردد. مصادیق

محدودیت آزادی بیان که در قوانین مربوط به فضای مجازی ذکر شده است، بسیار کلی و مبهم است و در نتیجه صلاحدید نهاد مقررات‌گذار در تعیین مصادیق محدودیت آزادی بیان به شکل غیرقابل قبولی، توسعه یافته است.

در حال حاضر کمیته‌ی مصادیق مجرمانه نقش اصلی را در تعیین مصادیق محدودیت‌های آزادی بیان دارد که ساختاری کاملاً دولتی دارد و قاعدتاً مطابق با سایر اصول باید تعدیل گردد. مفهوم همکاری ذی-نفعان، مفهومی کاملاً جدید در زمینه مقررات‌گذاری اینترنت است و به یکی از اصول خاص مقررات‌گذاری بین‌المللی اینترنت تبدیل شده است. در ایران، الگوی مقررات‌گذاری اینترنت الگویی کاملاً دولتی از طریق شورای عالی فضای مجازی و بدون مداخله سایر ذی‌نفعان است.

در راستای نظریه‌پردازی برای ترسیم الگوی مطلوب مقررات‌گذاری اینترنت در ایران در پرتوی اصول بنیادین مقررات‌گذاری اینترنت، نکات ذیل ضروری به نظر می‌رسد:

۱. ضرورت دارد که یک قانون عام در ارتباط با حریم خصوصی به تصویب برسد که تمام ابعاد حریم خصوصی را تحت حمایت قرار دهد که این حمایت، فضای مجازی را نیز شامل گردد. در این قانون به طور جامع می‌بایست حریم خصوصی مکانی، جسمانی و حریم خصوصی اطلاعات و ارتباطات تضمین گردد.

۲. تعیین محدودیت‌های آزادی ارتباطات اینترنتی، از آن جهت که تحدید حقوق و آزادی‌های عمومی باید به موجب قانون باشد می‌بایست صرفاً از طریق قانون مصوب مجلس شورای اسلامی صورت پذیرد.

۳. اصل آزادی ارتباطات اینترنتی در وضعیت کنونی مطلوب نیست و باید از اقتدار کارگروه مصادیق مجرمان کاسته شود. به این شکل که تصمیمات این هیأت تحت نظارت قضایی دیوان عدالت اداری قرار گیرد و قابل رسیدگی باشد.

۴. مدل تنظیم‌گری کنونی اینترنت در ایران دارای ایراداتی است و باید در تنظیم‌گری اینترنت، سایر ذی‌نفعان نیز مشارکت داده شوند.

فهرست منابع

۱- فارسی

الف) کتاب

۱. انصاری، باقر، **حق بر حریم خصوصی**، تهران: انتشارات سمت، ۱۳۹۱.
۲. انصاری، باقر، **حقوق رسانه**، چاپ دهم، تهران: انتشارات سمت، ۱۳۹۰.
۳. قاجار قیونولو، سیامک، **مقدمه حقوق سایبری**، تهران، انتشارات میزان، ۱۳۸۶.

ب) مقاله

۱. ابدی، سعیدرضا، **تنظیم مشارکتی مالیاتی، الگوی جدید در نظام مالیاتی ایالات متحده آمریکا**، فصلنامه تحقیقات حقوقی، شماره ۷۱، ۱۳۹۴.
۲. افتخار جهرمی، گودرز؛ اسلامی، ابراهیم، **نحوه اعمال صلاحیت دادگاه‌ها در رسیدگی به جرائم فضای مجازی**، مجله حقوقی دادگستری، شماره هشتاد و هشتم، ۱۳۹۳.
۱. اکرمی، خدیجه؛ غفاری، هدی و رستمی ولی، «**دسترسی به اینترنت حق مستقل بشری: رویکرد نظام حقوق بین‌الملل و نظام حقوقی ایران**»، فصلنامه تحقیقات حقوق خصوصی و کیفری، ۱۴۰۰.
۳. امام‌وردی، محمدحسن، **ماهیت‌شناسی حق بر حریم خصوصی در نظام حقوقی ایران**، مجله حقوق خصوصی، دوره ۱۴، شماره ۲، ۱۳۹۶.
۴. انصاری، باقر، **حریم خصوصی و حمایت از آن در حقوق اسلام-تطبیقی و ایران**، مجله دانشکده حقوق و علوم سیاسی، شماره ۶۶، ۱۳۸۳.
۵. جلالی فراهانی، امیرحسین، **صلاحیت کیفری سایبری در پرتوی قوانین داخلی، حقوق فن آوری اطلاعات و ارتباطات (مجموعه مقالات)**. تهران: انتشارات روزنامه رسمی جمهوری اسلامی ایران، ۱۳۸۵.
۲. رضایی، مهدی؛ بابازاده مقدم، حامد، **اصول تدوین قوانین و مقررات برای اینترنت با تأکید بر مصوبات یونسکو و شورای اروپا**، فصلنامه پژوهش حقوق عمومی، سال پانزدهم، شماره ۴۲، بهار ۱۳۹۳، ص ۵۴.
۶. سعد، علی، **درآمدی بر سیاست‌های فیلترینگ سایت‌های اینترنتی**، فصلنامه مطالعات رسانه‌های نوین، سال اول شماره ۲، ۱۳۹۴.
۷. فتحی، یونس؛ شاه‌مرادی، خیراله، **گسترده و قلمرو حریم خصوصی در فضای مجازی**، مجله حقوقی دادگستری، شال هشتاد و یکم، شماره نود و نهم، ۱۳۹۶.

۸. محبی، محسن؛ صفایی، عبدالحسین، صلاحیت فراسرزمینی بر اساس دکترین آثار در حقوق بین‌الملل، نشریه مطالعات حقوق تطبیقی، دوره ۹، شماره ۲، ۱۳۹۷.

2-Latin Source

- 1-Döge, Jenny, Cyber Warfare: Challenges for the Applicability of the Traditional Laws of War Regime, Mohr Siebeck GmbH & Co. KG, 2010
- 2-Ehlers, Dirk, General Principles, in European Fundamental Rights And Freedoms, Dirk Ehlers ed. 2007
- 3-Reidenberg, R, Joel (2002). "Yahoo and Democracy on the Internet", 42 Jurimetrics Journal, 261, 2002
- 4-Oxman, Bernard H, Jurisdiction of state, in MPEPIL, Rudiger Wolfrum Ed, online Ed, 2007
- 5-Schmitt, Michael N. "Wired Warfare: Computer Network Attack and jus in bello," international law studies, Vol 84, 2002
- 6-Schreuer, Christoph, State Sovereignty and the Duty of States to Cooperate – Two Incompatible Notions?, in International Law Of Cooperation And State Sovereignty, Jost Delbrück ed, 2012
- 7-Vaughan Lowe & Christopher Staker, Jurisdiction in International Law, Malcom D. Evans ed, 2010
- 8-Wenzel, Nicola (2009). Opinion and Expression, Freedom of, International Protection, MPEPIL, Rüdiger Wolfrum, 2009
- 9-Affirmation of Commitments, paragraph 4: <http://www.icann.org/en/documents/affirmation-of-commitments-30sep09-en.pdf>
- 10-Council Regulation (EC) 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, O.J. L 12/1
- 11-Doc.WSIS-05/TUNIS/DOC/6(Rev.1) E, the Tunis Agenda for the Information Society
- 12-EP and Council Directive 2006/24 of 15 March 2006, O.J. 2006 L 105/54.

- 13-Eur. Court H.R., Times Newspapers Ltd v. United Kingdom (nos. 1 and 2), Judgment of 10 March 2009
- 14-Eur. Court H.R., Von Hannover v. Germany, Judgment of 24 June 2004, Reports of Judgments and Decisions 2004-VI
- 15-Eur. Court H.R. Perrin v. United Kingdom, Judgment of 18 October 2005
- 16-Eur. Court H.R., Copland v. United Kingdom, Judgment of 3 April 2007.
- 17-Eur. Court H.R., Fatullayev v. Azerbaijan, Judgment of 22 April 2010.
- 18-Eur. Court H.R., Megadat.com SRL v. Moldova, Judgment of 8 April 2008.
- 19-Eur. Court H.R., Rantsev v. Cyprus and Russia, Judgment of 7 January 2010.
- 20-The Geneva Declaration Doc. WSIS-03/GENEVA/DOC/4-E, available at: http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC_0004!!PDF-E.pdf
- 21-Eur. Court H.R., Wypych v. Poland, Judgment of 25 October 2005.
- 22-Eur. Court H.R., X and Y v. the Netherlands, note 4627.
- 23-K. U. v. Finland, Judgment of 2 December 2008.
- 24-G. v. Finland, Judgment of 27 January 2009.
- 25-GA Res. 44/25 of 20 November 1989.
- 26-ICANN, President's Report: ICANN – The Case for Reform of 24 February 2002, available at: <http://www.icann.org/general/lynn-reform-proposal-24feb02.htm>
- 27-Joined Cases 89/85 et al., Wood Pulp, 1988 E.C.R. 5193, Council of Europe, Committee of Ministers, Convention on Cybercrime, Explanatory Report of 8 November 2001, available at: <http://conventions.coe.int/treaty/en/reports/html/185.htm>
- 28-The Declaration on Principles of International Law concerning Friendly Relations and Co-operation among the Convention on the Rights of the Child 1989
- 29-U. v. Finland, Judgment of 2 December 2008, Application 2827/02.the European Convention on Cybercrime
- 30-Zippo Manufacturing Co. v. Zippo Dot Com Inc., US District Court for the Western District of Pennsylvania, 952 F.Supp. 1119, at 1124 (W.D.Pa. 2009)

Basic Principles of internet regulation

Khadijah akrami*

Hoda Ghaffari**

Vali Roštami***

Abstract: Although Internet law is a relatively new legal phenomenon, some of its principles are evolving. The five basic principles of Internet regulation include freedom of Internet communication, respect for privacy, the principle of territorial jurisdiction, stakeholder participation, and government cooperation. Therefore, the purpose of this study is a legal analysis of the basic principles of Internet regulation within the framework of legal standards, in addition to theorizing in this field, to be a guide for the regulation of the Internet by the national legislature of our country. This research is a descriptive-analytical type and the library method has been used to collect information and the necessary information is collected using the library method. Based on the research findings, it can be claimed that the basic principles related to Internet regulation have emerged at the international level, which can be a practical guide for countries in cyberspace regulation. The Internet regulation system in Iran is not appropriate in comparison with the basic principles of Internet regulation. The result shows that in the current situation, the Internet regulatory system seeks to maximize restrictions on the freedom of Internet communication. The regulatory body in this regard is generally the governmental appointed body. Internet privacy has deficiency in regulatory despite legal protections. The Internet regulatory model is a purely governmental model without the participation of stakeholders, and in the field of international partnership and cooperation, there is no willingness to cooperate with other governments in the field of Internet regulation.

Keywords: Internet Freedom, Privacy, Territorial Jurisdiction, Government Cooperation, Stakeholder Cooperation.

*. Ph.D. Student in International Law, Department of public and International law, Faculty of Divinity, Political Science and Law, Science And Research Branch, Islamic Azad University(IAU), Tehran, Iran. kh_akrami@yahoo.com

** Assistant Professor, Department of Public Law, Faculty of Law and Political Science, Allameh Tabatabaei University, Tehran, Iran. hodaghafari@yahoo.com

*** Associate Professor, Department of Public Law, Faculty of Law and Political Science, University