

قانونگذاری در فضای سایبر: رویکرد حقوق بین‌الملل و حقوق ایران

سید یاسر ضیایی *

احسان شکیب‌نژاد **

شناسه دیجیتال اسناد (DOI): 10.22066/cilamag.2017.27971

تاریخ دریافت: ۱۳۹۴/۱۰/۱۹

تاریخ پذیرش: ۱۳۹۵/۴/۲۲

چکیده

از بدو ورود فضای سایبر به زندگی بشریت، مقوله قانونگذاری و شناخت قانونگذار صالح در این فضا، چالش جدی بوده است. شیوه قانونگذاری در فضای سایبر، مبتنی بر دو نوع نگرش متفاوت به حاکمیت در فضای سایبر است. نگرش نخست، مبتنی بر انحصار دولت‌ها در عرصه قانونگذاری فضای سایبر است و نگرش دوم که ملهم از دکتترین میراث مشترک بشریت است، مخالف ورود انحصاری دولت‌ها به این عرصه است. هر یک از این دو رویکرد، موجد روش‌های قانونگذاری مختلفی در فضای سایبر است. روش‌های قانونگذاری ملی، بین‌المللی و خودانتظامی در زمره روش‌های قانونگذاری در فضای سایبر به شمار می‌آیند. اگرچه توسل به هر یک از روش‌های قانونگذاری با اشکالاتی در عرصه اجرا روبه‌روست، در این میان می‌توان رویکردی بینابین و مختلط را برگزید تا ضمن رفع نواقص دیگر روش‌ها، زمینه را برای نیل به تفاهم میان کشورها و گروه‌های فعال در زمینه فضای سایبر هموار سازد. نگرش دولت جمهوری اسلامی ایران، اساساً مبتنی بر شیوه قانونگذاری ملی است. با این حال، عملکرد ایران در سطح بین‌المللی و به‌ویژه در اتحادیه بین‌المللی مخابرات، حاکی از پذیرش روش مختلط در قانونگذاری در فضای سایبر است.

واژگان کلیدی

فضای سایبر، قانونگذاری، صلاحیت قانونگذاری، نظریه میراث مشترک بشریت، حقوق ایران

* yaserziaee@gmail.com

* نویسنده مسئول، استادیار گروه حقوق بین‌الملل دانشگاه قم

** ehsan.shakib69@gmail.com

** کارشناسی ارشد حقوق بین‌الملل دانشگاه قم

مقدمه

ویژگی فضای سایبر این است که در عین مفیدبودن می‌تواند پناهگاه امن هنجارشکنان باشد. پیشگیری از جرایم در فضای سایبر، منوط به جرم‌انگاری مناسب در این فضا است. تفاوت قوانین داخلی کشورها و فقدان قوانین بین‌المللی کافی در این زمینه، مبنای حقوقی مناسب برای تعقیب مجرمین بالقوه را با چالشی حقوقی مواجه می‌کند. لذا از بدو ورود فضای سایبر به زندگی بشریت، موضوع قانونگذاری و شناخت قانونگذار صالح در این فضا از اهمیت بسزایی برخوردار بوده است. با جهان‌شمولی اینترنت و نگرانی دولت‌ها از تأثیرپذیری حاکمیت آن‌ها، قانونگذاری در این فضا از اهمیت زیادی در مناسبات بین‌المللی برخوردار شد.

شیوه قانونگذاری در فضای سایبر، بسته به نوع نگرش به حاکمیت دولت در این فضا متفاوت است. در مجموع، دو نگرش نسبت به حاکمیت دولت در این فضا وجود دارد: حاکمیت انحصاری دولت بر فضای سایبر و تعمیم نظریه میراث مشترک بشریت بر فضای سایبر. روش قانونگذاری ملی، منبعث از نگرش حاکمیت انحصاری دولت، و روش‌های قانونگذاری بین‌المللی، خودانتظامی و مختلط، منبعث از نگرش میراث مشترک بشریت در فضای سایبر است. کشورهای در حال توسعه، از نگرش مبتنی بر حاکمیت، و کشورهای غربی، حامیان حقوق بشر و نهادهای فنی فضای سایبر، از نگرش مبتنی بر میراث مشترک بشریت حمایت کرده‌اند. در این نوشتار، سعی بر آن است تا نظریات درباره قانونگذاری در فضای سایبر از منظر حقوق بین‌الملل و حقوق ایران، تحلیل و بررسی شود.

۱. نظریات حاکمیت در فضای سایبر

دو نگرش نسبت به حاکمیت در فضای سایبر مطرح است. طبق دیدگاه اول، فضای سایبر همچون سرزمین قابل تقسیم میان دولت‌هاست و دولت، یگانه مرجعی است که می‌تواند صلاحیت قانونگذاری خویش را بر فضای سایبر اعمال کند. طبق دیدگاه دوم، فضای سایبر به‌مثابه میراث مشترک بشریت است که حاکمیت هیچ دولتی به نحو انفرادی و انحصاری بر آن امکان‌پذیر نیست.

۱-۱. حاکمیت انحصاری بر فضای سایبر

این دیدگاه، حاصل پذیرش مفهوم وستفالیایی حاکمیت^۱ در فضای سایبر است. حامیان این نگرش بر این باورند که دولت، بهترین نهاد حاکمیتی موجود در فضای سایبر است.^۲ این نگرش، یادآور

1. Westphalian Concept of Sovereignty

2. Viktor Mayer-Schonberger, The Shape of Governance: Analyzing the World of Internet Regulation, *Virginia Journal of International Law*, No. 43, 2002-2003, p. 613.

نظریه «متعلق به هیچ کس»^۳ راجع به دریای آزاد در گذشته است^۴ که به هر دولتی اجازه می‌دهد به اندازه قدرت خود بر فضای سایبر، اعمال حاکمیت کند. از آنجاکه اینترنت، مرزگذر است، اعمال حاکمیت از سوی همه دولت‌ها می‌تواند مشکلات حقوقی متعددی برای کشورها و افراد ایجاد کند؛ ضمن آنکه فضای سایبر برخلاف دریای آزاد در گذشته، میان چند دولت تقسیم نشده است. هرچند سخت‌افزارهای رایانه‌ای از جمله سرورهای اینترنتی از نظر فیزیکی تحت حاکمیت صلاحیت‌های ملی قرار دارد و همین امر، مستمسک برخی دولت‌ها برای توجیه کنترل سختگیرانه اینترنت شده است، اطلاعات موجود در این سخت‌افزارها و سامانه‌های عامل آن‌ها در حقیقت این‌گونه نیست.^۵ از آنجاکه اینترنت، فاقد حاکمیت مرکزی است،^۶ طبق این نظریه، میان حاکمیت‌ها تعارض شکل خواهد گرفت.

۱-۲. فضای سایبر به مثابه میراث مشترک بشریت

با انقلاب مردمی فرانسه و تحولات بعدی در سایر کشورها، حاکمیت مردم به‌عنوان یکی از مفروضات بنیادین مشروعیت سیاسی دولت مطرح شد.^۷ در این دوره که در آن «حاکمیت فراوستفالیایا»^۸ مطرح می‌شود، حاکمیت دولت‌ها تحت‌الشعاع دو پدیده جهان‌شمولی و حقوق بین‌الملل قرار گرفت.^{۱۰} دو نظریه «متعلق به همه»^{۱۱} و «میراث مشترک بشریت»^{۱۲} برآمد این نگرش به حاکمیت است که طبق آن، هیچ کشوری حق اعلام حاکمیت بر مناطق خارج از

3. *Res nullis*

۴. نظریه متعلق به هیچ کس که تا ابتدای قرن هفدهم بر دریا حاکم بود، معادل نظریه دریای بسته بوده است که قابل مالکیت و حاکمیت بود. با انتشار کتاب دریای آزاد گروسیوس در سال ۱۶۰۵ میلادی، نظریه متعلق به همه (*res communis*) نضج گرفت. ن.ک: احمد متین‌دفتری؛ سیر تحول حقوق بین‌الملل دریایی (از گروسیوس تا کنفرانس‌های ژنو)، گنج دانش، ۱۳۸۷، صص ۱۳۴-۱۳۰.

5. Jack Goldsmith, Regulation of the Internet: Three Persistent Fallacies, *Chicago-Kent Law Review*, vol. 73, 1998, p. 1229.

اگرچه امکان شناسایی کاربران در سامانه‌های رایانه‌ای، طبق روش آدرس‌دهی IPV6 (نسل ششم و مدرن‌ترین نوع شناسه پروتکل - روش آدرس‌دهی - است که طبق آن شماره IP هر دستگاه معین می‌شود) آسان شده است، استفاده از وی.پی.ان با تغییر نشانی پروتکل (IP) روش‌ها، مانع شناسایی کاربران در فضای سایبر می‌شود.

6. Dina Koutouki, Human Rights: Benefits of Information Technology, *University of New Brunswick Law Journal*, No. 48, 1999, p. 268.

7. W. Michael Reisman, Sovereignty and Human Rights in Contemporary International Law, *Yale Law School Legal Scholarship Repository*, vol. 84, Issue 1, 1990, p. 867.

8. Post-Westphalian Sovereignty

9. Andrew Linklater, Citizenship and Sovereignty in the Post-Westphalian State, *European Journal of International Relations*, vol. 2, 1996, p. 77.

10. Jackson, John H., Sovereignty - Modern: A New Approach to an Outdated Concept, (2003). *Georgetown Law Faculty Publications and Other Works*. p. 782. <http://scholarship.law.georgetown.edu/facpub/110>.

11. *Res communis*

12. Common Heritage of Mankind

صلاحیت خود را نداشته و همچنین نمی‌تواند مانع استفاده کشورهای دیگر از آن شود.^{۱۳} طبق این نظر، صلاحیت قانونگذاری به مرجعی فراتر از دولت‌ها واگذار می‌شود. امروزه این نظریه در مناطقی چون دریای آزاد، بستر عمیق دریا، قطب جنوب، فضای ماورای جو و اجرام آسمانی پذیرفته شده است.^{۱۴}

باین‌حال، انگاشت فضای سایبر به‌عنوان میراث مشترک بشریت، با مشکلاتی فنی و حقوقی روبه‌روست. به‌طور مثال، عواملی چون برتری دانش و ثروت، حاکمیت برابر در فضای سایبر را تحت تأثیر قرار می‌دهد.^{۱۵} همچنین اگرچه اصل میراث مشترک بشریت در برخی مناطق، تبدیل به عرف بین‌المللی شده است، نحوه بهره‌برداری از آن، موضوعی مستقل محسوب می‌شود.^{۱۶}

۲. روش‌های قانونگذاری در فضای سایبر

قانونگذاری ملی، بین‌المللی، خودانتظامی و مختلط از اقسام روش‌های قانونگذاری در فضای سایبر به شمار می‌آیند. روش قانونگذاری ملی، حاکی از رویکرد حاکمیت انحصاری دولت‌ها بر فضای سایبر، و روش‌های بین‌المللی، خودانتظامی و مختلط، متأثر از نگرش مبتنی بر دکترین تعمیم نظریه میراث مشترک بشریت بر فضای سایبر است.

۱-۲. روش قانونگذاری ملی

در این روش، نهادهای قانونگذاری ملی نسبت به قانونگذاری و جرم‌انگاری در فضای سایبر اقدام می‌کنند.^{۱۷} باید توجه داشت که در این روش اولاً، نمی‌توان از جرم‌انگاری تمام جرایم در فضای سایبر، اطمینان خاطر داشت و ثانیاً، این روش می‌تواند موجب تعارض قوانین در فضای سایبر شده و اصل قانونی بودن جرم و مجازات و اصل منع مجازات مضاعف را تحت تأثیر قرار دهد. از آنجاکه این روش، مستعد تصویب قوانین فراسرزمینی و انحصاری‌سازی فضای سایبر است، می‌تواند منجر

۱۳. جالب توجه است که در خصوص دریاها موضع کشورهای غربی و قدرتمند بر نظریه متعلق به هیچ‌کس، و موضع کشورهای درحال‌توسعه بر نظریه متعلق به همه قرار داشت (ن.ک: متین‌دفتری؛ همان) درحالی‌که در فضای سایبر، موضع این دو گروه برعکس است.

14. Anthony Aust, *Handbook of International Law*, Cambridge University Press, New York, 2010, p. 40.

15. Anupam Chander & Madhavi Sunder, The Romance of the Public Domain, *California Law Review*, vol. 92, 2004, p. 1331.

16. Antonio Segura-Serrano, International Regulation and the Role of International Law, *Max Plank Yearbook of United Nations Law*, vol. 10, 2006, pp. 254-255.

۱۷. در کنار گزینه قانونگذاری ملی که مطلق کشورها را دربرمی‌گیرد به گزینه‌های دیگری چون حاکمیت قانون کشور فرستنده یا حاکمیت قانون کشور گیرنده اشاره شده است که این مدل از نظام حقوقی ناظر بر ماهواره گرفته شده است: Graham J. H. Smith, *Internet Law and Regulation*, Sweet and Maxwell, London, 2002, p. 533.

به تصویب قوانین انسدادی^{۱۸} توسط کشورها برای جلوگیری از اعمال صلاحیت کشورهای خارجی شود. از سوی دیگر، عملکرد برخی کشورها از جمله چین در قانونگذاری حداکثری، منجر به خودسانسوری در فضای سایبر شده است.^{۱۹}

از آنجا که قانونگذاری در فضای سایبر توسط مراجع ملی، مبتنی بر یکی از مبانی شناخته شده صلاحیت است در ادامه به نقد و بررسی قانونگذاری در فضای سایبر بر مبنای صلاحیت سرزمینی، صلاحیت شخصی، صلاحیت واقعی و صلاحیت جهانی پرداخته می شود.

الف. صلاحیت سرزمینی

لازمه توسل به صلاحیت سرزمینی در فضای سایبر، وجود مرزهای دقیق است تا مقررات دولتی در حیطه آن عینیت یابد.^{۲۰} عدم امکان اجرای قواعد سنتی بر فضای بی‌اتهای سایبر از پیچیدگی‌های این فضا است. یکی دیگر از معضلات صلاحیت سرزمینی در فضای سایبر، ناپیدابودن محل ارتکاب جرم در این فضا است. اغلب نمی‌توان محل وقوع جرم را شناسایی کرد. حتی اگر تارنماها با کد کشوری به‌عنوان محل وقوع جرم ملاک گرفته شود، این اشکال در مورد تارنماهای با کد عمومی باقی می‌ماند. هرچند برخی کشورها معیارهایی مانند محل وقوع سامانه‌های رایانه‌ای، داده‌های رایانه‌ای و ذخیره اطلاعات را به‌عنوان معیار تعیین سرزمین در نظر گرفته‌اند، قانونگذاری‌های متعارض موجب می‌شود یک عمل در آن واحد در صلاحیت سرزمینی چند کشور قرار گیرد.

18. Blocking Laws

بر اساس این قوانین، دولت واضح قانون، اتباع خود را از شناسایی و اجرای برخی قوانین خارجی منع می‌کند. برای مطالعه بیشتر، ن.ک:

Jennifer A. Zerk, Extraterritorial Jurisdiction: Lessons for the Business and Human Rights Sphere from Six Regulatory Areas *Corporate Social Responsibility Initiative*, No. 59, 2010, p. 103; A. V. Lowe, Blocking Extraterritorial Jurisdiction: The British Protection of Trading Interests Act, *The American Journal of International Law*, vol. 75, No. 2, 1981, pp. 257-282.

۱۹. اطلاق عبارت «اطلاعات مضر» در قوانین چین، بدون تصریح مصادیق آن، دست دولت چین را برای اعمال حداکثر حاکمیت خویش در فضای سایبر باز می‌گذارد. از سوی دیگر، صاحب تارنما نمی‌تواند قضاوت کند که چه محتویاتی از تارنمای وی، اطلاعات مضر محسوب می‌شود، چه این امر منجر به خودسانسوری می‌شود. ن.ک:

Hu, L., *Shaping the Virtual State: Internet Content Regulation in China (1994-2009)*, (Thesis). *University of Hong Kong, Pokfulam, Hong Kong SAR*. 2011, pp. 35-36. Retrieved from http://dx.doi.org/10.5353/th_b4642170.

۲۰. برخی معتقدند که مرزها در فضای سایبر تقریباً همان مرزهاست لیکن دچار تغییرات کارکردی شده است. ن.ک: رسول افضلی، محمدباقر قالیباف و میثم احمدی فیروزجائی؛ «تبیین تحولات مفهوم مرز در فضای سیاسی مجازی»، پژوهش‌های جغرافیایی/انسانی، دوره ۴۵، شماره ۱، ۱۳۹۲، ص ۲۳۵.

ب. صلاحیت شخصی

اعمال صلاحیت شخصی در فضای سایبر، مستلزم احراز تابعیت مجرم یا بزه‌دیده است. شناسایی مجرم در این فضا منوط به تعیین شناسه^{۲۱} اوست^{۲۲} در حالی که فرد به راحتی با استفاده از برنامه‌های رایانه‌ای، قادر به جعل شناسه خود است.^{۲۳} ثانیاً، لازمه اعمال صلاحیت شخصی منفعل در این فضا، انجام تحقیقات در رایانه‌های واقع در خارج از کشور (ولو از راه دور) است که موجب نقض حاکمیت سرزمینی کشور محل اطلاعات خواهد شد.^{۲۴} علاوه بر این، اعمال موسع صلاحیت شخصی در فضای سایبر به روند تجارت الکترونیک در فضای سایبر، لطمه خواهد زد.^{۲۵}

ج. صلاحیت واقعی

اعمال صلاحیت واقعی نیز با این اشکال روبه‌روست که ضابطه دقیقی برای توسل به آن وجود ندارد.^{۲۶} البته دست دولت‌ها برای اعمال صلاحیت واقعی کاملاً باز نیست و باید از اعمال موسع صلاحیت واقعی امتناع کرد. لذا در این زمینه لازم است میان اعمال صلاحیت واقعی و اصل آزادی اینترنت، موازنه‌ای عادلانه برقرار شود که در نتیجه آن، اعمال صلاحیت واقعی در فضای سایبر در چارچوب موازین حقوق بشری صورت پذیرد.^{۲۷} دادگاه آلمان در قضیه توین در رابطه با انکار هولوکاست توسط یک استرالیایی در تارنمایی در استرالیا، صلاحیت واقعی را اعمال کرد.^{۲۸} دادگاه فرانسه نیز در رابطه

۲۱. شناسه پروتکل (IP) شماره اختصاصی هر رایانه متصل به اینترنت است.

۲۲. این نظریه در قضایای مختلفی مطرح شده است:

Playboy Enterprises, Inc. v. Chuckleberry Publishing Inc., Award 19 June 1996; *Inset Systems Inc. v. Instruction Set Inc.*, Award 17 April 1996; *Martiz Inc. v. Cybergold Inc.*, Award 19 August 1996; *Dow Jones & Company Inc. v. Gutnick*, Award 10 December 2002, *Gator.com Corp. v. L.L. Bean Inc.*, Award 15 February 2005.

۲۳. وی.پی.ان‌ها (VPN) و برنامه‌های تغییر شناسه پروتکل در این زمره‌اند.

24. Jack Goldsmith, *The Internet and the Legitimacy of Remote Cross-Border Searches* *University of Chicago Legal Forum*, vol. 16, 2001, p. 2.

همان‌طور که در جریان دعوی ایالات متحده آمریکا علیه *ایونفگورسکف*، انجام تحقیقات سایبری توسط پلیس فدرال از سامانه‌های واقع در خاک روسیه بدون کسب اجازه این کشور به‌عنوان نقض اصل عدم مداخله و حاکمیت کشور روسیه مطرح بود. ن.ک:

United States of America v. Aleksey Vladimirovich Ivanov, Crim. No. 3:00CR00183(AWT), Award 6 December 2001.

25. James R. Pielemeier, *Why General Personal Jurisdiction over Virtual Stores Is a Bad Idea*, *Quinnipiac Law Review*, vol. 27, 2009, p. 671.

۲۶. دادگاه بریتانیا در پرونده پرین، یک تبعه فرانسه را برای انتشار محتویات قبیح در یک تارنمای امریکایی به دلیل مشاهده این سایت در اداره پلیس لندن توسط یک افسر پلیس محکوم کرد. ن.ک:

R v. Stephane Laurent Perrin EWCA Crim. 747, 2002, Award 22 March, 2002, paras. 2-4.

27. Robert Uerpmann-Witzack, *Principles of International Internet Law*, *German Law Journal*, vol. 11, 2010, pp. 1255-1256.

28. Bundesgerichtshof, Toebe (Federal Court), Award 12 December 2000.

ارائه یادبودهای نازی‌ها در یک سرور مستقر در ایالات متحده معتقد بود که حقوق کیفری فرانسه نقض شده است.^{۲۹} همچنین طبق قانون میهن‌دوستی آمریکا، اداره تحقیقات فدرال مجاز است با قرار قضایی به پیام‌های پست‌های صوتی افراد، دسترسی داشته باشد.^{۳۰} یا مقامات مجاز بدون رعایت الزامات قانون شوند، اطلاعات رایانه‌ای افراد را رهگیری کنند.^{۳۱}

د. صلاحیت جهانی

صلاحیت جهانی، یکی دیگر از مبانی قانونگذاری در فضای سایبر است. باید توجه داشت که برخی اقدامات در برخی مناطق، مورد ادعای صلاحیت هیچ دولتی نیست و لذا اعمال صلاحیت در خصوص آن‌ها نه تنها مداخله در حاکمیت دیگر دولت‌ها نیست، بلکه برای جلوگیری از تبدیل شدن آن منطقه به پناهگاه امن متخلفین و پرهیز از شکل‌گیری «سرزمین بی‌قانون»^{۳۲} لازم است. دزدی دریایی در آب‌های آزاد در گذشته و اقدامات مجرمانه در اینترنت در زمان حاضر از نمونه‌های این وضعیت است. ماده ۲۲ کنوانسیون جرایم سایبری شورای اروپا (کنوانسیون بوداپست)^{۳۳} جایگاه صلاحیت جهانی در فضای سایبر را تأیید می‌کند.^{۳۴} مبانی صلاحیت جهانی برای برخی جرایم سایبری مانند تحریک به نسل‌کشی در معاهدات بین‌المللی موجود است^{۳۵} و قوانین داخلی دولت‌ها، برخی جرایم سایبری را مانند هرزه‌نگاری کودکان، مشمول صلاحیت جهانی قرار داده‌اند.^{۳۶}

29. Ibunal de Grande Instance de Paris, UEJF et Licra c/ Yahoo! Inc., Award 20 November 2000.

30. USA Patriot Act, 2001, Title II, Sec 209.

31. *Ibid.*, Sec 217.

32. Lawless Territory

See Steve Coughlan, Robert J. Currie, Hugh M. Kindred, Teresa Scassa, Global Reach, Local Grasp: Constructing Extraterritorial Jurisdiction in the Age of Globalization, *Dalhousie Law School*, prepared for the Law Commission of Canada, Canada, 2006, p. 34.

33. Council of Europe Cybercrime Convention, Budapest, (Adopted 2001, Entered into Force 2004).

کنوانسیون جرایم سایبری شورای اروپا معروف به کنوانسیون بوداپست با هدف نیل به هماهنگ‌سازی قوانین داخلی دولت‌های اروپایی در حیطه فضای سایبر در ۲۳ نوامبر ۲۰۰۱ در بوداپست به امضا گذاشته شد و متعاقباً یک پروتکل الحاقی راجع به نژادپرستی و بیگانه‌ستیزی در ۷ نوامبر ۲۰۰۲ در استراسبورگ فرانسه نیز به آن اضافه شد.

۳۴. بند (د) ماده ۲۲: «در جایی که جرم مورد نظر، مطابق قوانین جزایی قابل مجازات شناخته شده، توسط تبعه (کشور عضو) ارتکاب یافته یا جرم ارتكابی از جمله جرایم واقع در حوزه صلاحیت جهانی حقوق جزا باشد».

See Armando A. Cottim, Cybercrime, Cyberterrorism and Jurisdiction: An Analysis of Article 22 of the COE Convention on Cybercrime, *European Journal of Legal Studies*, vol. 2, Issue 3, 2010.

35. Kelly A. Gable, Cyber-Apocalypse Now: Securing the Internet against Cyberterrorism and Using Universal Jurisdiction as a Deterrent, *Vanderbilt Journal of Transnational Law*, vol. 43, Issue 1, 2010, p. 45.

۳۶. ایالات متحده آمریکا و بلژیک در قوانین داخلی خود، هرزه‌نگاری کودکان را از زمره جرایم تحت صلاحیت جهانی تلقی کرده‌اند. ن.ک:

18 U.S. Code § 2252, 18 U.S. Code § 1466A, Act of Moniteur Belge - Belgisch Staatsblad, 10 February 1999, Article 10.

در مجموع، قانونگذاری ملی، مشکلاتی برای دولت‌ها و کاربران ایجاد خواهد کرد. این شیوه موجب اعمال فراسرزمینی قوانین خواهد شد که تعارض قوانین میان دولت‌ها را به دنبال خواهد داشت و همچنین موجب اعمال هم‌زمان چند نظام حقوقی بر کاربران فضای سایبر و متعاقباً سردرگمی کاربران خواهد شد. لذا کاربران، خودبه‌خود ملزم به رعایت قوانین متعدد و حتی متناقض خواهند بود،^{۳۷} در حالی که ممکن است از محتوای آن قوانین بی‌خبر باشند.^{۳۸} در این شیوه همچنین خطر چند کیفری وجود دارد؛ خصوصاً آنکه افراد نمی‌دانند کدام قانون را باید پاس بدارند و در نهایت مجبور خواهند بود مضیق‌ترین قانون را رعایت کنند.^{۳۹} در واقع، ماهیت جهان‌شمولی موجب می‌شود افراد بر اساس معیارهای مختلف صلاحیتی، تحت شمول قوانین چند کشور قرار گیرند.^{۴۰} با این حال، موافقت‌نامه‌های معاضدت قضایی و تعهدات حقوق بشر می‌توانند این معضل را کاهش دهند.

۲-۲. روش قانونگذاری بین‌المللی

روش قانونگذاری بین‌المللی با توجه به یکپارچگی اینترنت و مشکلات ناشی از قانونگذاری ملی مطرح شد.^{۴۱} این شیوه در بهترین شکل با انعقاد معاهدات بین‌المللی محقق می‌شود. به‌طور مثال، ماده ۳ پروتکل الحاقی به کنوانسیون حقوق کودک، مورخ ۲۰۰۰ در خصوص فروش، فحشا و هرزه‌نگاری کودکان به‌صراحت بر نقش اینترنت در توزیع هرزه‌نگاری کودکان اشاره دارد و از کشورها می‌خواهد این‌گونه افعال را جرم‌انگاری کنند. همچنین یکی از مهم‌ترین کنوانسیون‌های مربوط به فضای سایبر، کنوانسیون بوداپست در خصوص جرایم سایبری است. با این حال، این

37. Viktor Mayer-Schönberger, op cit., pp. 8-9.

38. David R. Johnson & David Post, "Law and Borders-The Rise of Law in Cyberspace", *Stanford Law Review*, Vol. 48, Issue 5, 1996, p. 1401.

مخالفین این نظر معتقدند محدودیت‌های صلاحیت فنی موجب می‌شود اغلب بارگذاران، نگران نقض قوانین خارجی نبوده و صاحبان تارنما نیز می‌توانند محدودیت‌هایی برای ورود بارگذاران ایجاد کنند. همچنین بارگذار همواره از این امر مطلع است که ممکن است اطلاعاتش وارد حوزه صلاحیت کشوری شود که در آنجا غیرقانونی است. ن.ک:

Jack L. Goldsmith, The Internet and the Abiding Significance of Territorial Sovereignty, *Indiana Journal of Global Legal Studies*, vol. 5, Issue 2, 1998, p. 484.

۳۹. زمانی که یک عمل از نظر یک کشور جرم باشد و از نظر کشوری دیگر جرم نباشد، این مشکل بیشتر است. ن.ک: جینا دی آنجلیز؛ جرایم سایبر، ترجمه: سعید حافظی و عبدالصمد خرم‌آبادی، دبیرخانه شورای عالی اطلاع‌رسانی، ۱۳۸۳، ص ۴۱؛ همین‌طور در مواردی که دعوا از نظر یک کشور، حقوقی و از نظر کشور دیگر، کیفری است؛ مثلاً سرقت اسرار تجاری در امریکا اقدام متخلفانه کیفری و در انگلستان، اقدام متخلفانه حقوقی است. ن.ک:

David S. Wall, *Cybercrime: The Transformation of Crime in the Information Age*, Polity Press, Cambridge, 2008, p. 162.

۴۰. جلالی فراهانی، امیرحسین؛ درآمدی بر آیین دادرسی کیفری جرایم سایبری، خرسندی، ۱۳۸۹، ص ۹۷.

41. Wolff Heintschel von Heinegg, Legal Implications of Territorial Sovereignty in Cyberspace, *4th International Conference on Cyber Conflict*, 2012, p. 10.

کنوانسیون نمی‌تواند به‌عنوان معاهده‌ای جامع تلقی شود، چه آنکه اولاً، تمام جرایم سایبری را دربر نمی‌گیرد و ثانیاً، این کنوانسیون صرفاً برای کشورهای اروپایی لازم‌الاجراست. در هر صورت، معاهدات منطقه‌ای و دوجانبه، پاسخگوی حل مشکلات نبوده و معاهده اینترنتی در سطح بین‌المللی مورد نیاز است.^{۴۲} برخی از قواعد آمره، نظیر ممنوعیت دزدی دریایی، برده‌داری و نسل‌زدایی نیز در فضای سایبر قابل اعمال است.^{۴۳}

سازمان‌های بین‌المللی نیز در فرایند بین‌المللی‌سازی قانونگذاری در فضای سایبر، نقش قابل توجهی داشته‌اند. پیش از همه، آنسیترال با تصویب قانون نمونه آنسیترال در خصوص تجارت الکترونیکی در سال ۱۹۹۶^{۴۴} نقش چشمگیری در هماهنگ‌سازی قوانین ملی کشورها درباره مسائل مربوط به تجارت الکترونیک داشته است. گروه هشت^{۴۵} نیز در اولین اقدام خود در سال ۱۹۹۷ کمیته فرعی جرایم رایانه‌ای^{۴۶} را برای مقابله با جرایم سایبری تأسیس و متعاقباً یک برنامه اقدام ده اصلی را در این رابطه تصویب کرد.^{۴۷} مجمع عمومی سازمان ملل متحد در سال‌های ۲۰۰۰ و ۲۰۰۳ تلاش‌هایی برای تنظیم امنیت اطلاعاتی و سایبری انجام داد.^{۴۸} پس از تلاش اتحادیه اروپا برای تصویب کنوانسیون جرایم سایبری، اتحادیه عرب به پیشنهاد ایالات متحده عربی یک مدل قانونی در خصوص همسان‌سازی قوانین ملی کشورهای عربی را در سال ۲۰۰۳ پذیرفت.^{۴۹} شورای همکاری خلیج فارس نیز در کنفرانس ۲۰۰۷ به دولت‌ها توصیه کرد که رویکردی متحدانه را در خصوص مواجهه با موضوعات سایبری اتخاذ کنند.^{۵۰} سازمان کشورهای امریکایی، سازمان همکاری و توسعه اقتصادی، سازمان همکاری و اقتصادی آسیا - اقیانوسیه و سازمان کشورهای مشترک‌المنافع نیز در یکسان‌سازی قواعد بین‌المللی تلاش‌هایی داشته‌اند.

42. Solange Ghernaoui-H. lie, We Need a Cyberspace Treaty: Regional and Bilateral Agreements Are Not Enough , *Inter Media*, vol. 38, Issue 3, 2010, p. 5.

43. Jovan Kurbalija, *An Introduction to Internet Governance*, DiploFoundation, Malta, 2014, pp. 91-92.

44. UNCITRAL Model Law on Electronic Commerce with Guide to Enactment, 1996.

۴۵. شامل کانادا، فرانسه، آلمان، ژاپن، ایتالیا، امریکا، بریتانیا و روسیه.

46. Subcommittee on High-tech Crimes

47. Ten-Point Action Plan to Fight High-Tech Crimes, The Meeting of G8 Justice and Home Affairs Ministers, 10 December 1997.

48. General Assembly Resolution 55/63 (2000), UN General Assembly Resolution 57/239 (2003).

49. Decision of the Arab Justice Ministers Council, 19th Session 2003.

۵۰. این کنفرانس از کشورها می‌خواهد به معاهده‌ای ملهم از کنوانسیون بوداپست پیوندند، قوانین داخلی خود را با مدل پیشنهادی امارات متحده عربی منطبق کنند، قوانین داخلی را یکسان‌سازی و بر تشکیل گروهی کارشناسی، تشریک مساعی کنند. ن.ک:

Recommendations of the Conference on Combating Cybercrime in the GCC Countries, (2007).

اما شاید مهم‌ترین تلاش، اجلاس جهانی جامعه اطلاعات^{۵۱} در سال ۲۰۰۳ باشد که در آن تشکیل سازمان بین‌المللی اینترنت و انعقاد معاهده‌ای اینترنتی پیشنهاد شد. اتحادیه بین‌المللی مخابرات در مه ۲۰۰۷ آژانس جهانی جرائم سایبری^{۵۲} و متعاقباً گروه کارشناسان ارشد^{۵۳} را با هدف ارائه پیشنهادهایی برای جرم‌انگاری سایبری بنیانگذاری کرد.^{۵۴} بالاخره سند اصلاحی مقررات اتحادیه بین‌المللی مخابرات^{۵۵} با اعطای وجهه حقوقی بین‌المللی به قانونگذاری در فضای اینترنت با رأی اکثریت کشورها به تصویب رسید.^{۵۶} باید توجه داشت که فناوری محوری فضای سایبر موجب می‌شود که سهم کشورهای مختلف در تنظیم نظام حقوقی حاکم بر فضای سایبر متفاوت باشد. به همین دلیل، یکی از مدل‌های پیشنهادی در قانونگذاری بین‌المللی در فضای سایبر، تقسیم وظایف و امتیازات بر مبنای مؤلفه‌هایی مانند قدرت، ثروت و تخصص است. این روش که از آن تحت عنوان «هندسه متغیر»^{۵۷} یاد می‌شود، در ساختار شورای امنیت، صندوق بین‌المللی پول و سازمان تجارت جهانی اعمال شده است.^{۵۸} این راهکار در ماده ۴۹ اعلامیه اجلاس جهانی جامعه

51. World Summit on the Information Society (WSIS)

پیرو پیشنهاد دولت تونس در شورای اتحادیه بین‌المللی مخابرات در سال ۲۰۰۱ مقرر شد این اجلاس در دو مرحله ۲۰۰۳ سوئیس و ۲۰۰۵ تونس برگزار شود. مجمع عمومی سازمان ملل در ۲۱ دسامبر ۲۰۰۱ طی قطعنامه‌ای این اجلاس را در راستای اجرای اعلامیه هزاره سازمان ملل اعلام کرد. ن.ک: A/RES/56/183

52. Global Cybercrime Agenda (GCA)

این آژانس، مرکز هماهنگی اقدامات بین‌المللی در زمینه امنیت سایبری است که تحت مدیریت دبیرکل اتحادیه بین‌المللی مخابرات است. ن.ک:

ITU Global Cybersecurity Agenda (GCA), *International Telecommunication Union*, 2007, p. 12.

53. High-Level Experts Group (HLEG)

54. Stein Schjølberg and Solange Ghernaoui-Hélie, *A Global Protocol on Cybersecurity and Cybercrime*, Cybercrimedata, Oslo, 2009, p. i.

55. Final Acts of the World Conference on International Telecommunications, Dubai, (signed 2012).

۵۶. از ۱۴۴ نماینده، ۸۹ نماینده از جمله روسیه، چین و ایران این سند را امضا کردند. ن.ک:

Final Acts of the World Conference on International Telecommunications, Article 10.1.

57. Variable Geometry Approach

هندسه متغیر از مهندسی هوانوردی اقتباس شده و به بال‌های هواپیما مربوط است که با تغییر جهت، خصیصه‌های ایرودینامیکی را تغییر می‌دهد. ن.ک:

Alex Mills, *Towards a Public International Perspective on Private International Law: Variable Geometry and Peer Governance*, *Faculty of Laws*, 2012, p. 15.

در میان طرفداران این روش می‌توان به دیدگاه قاضی *تاناکا* اشاره کرد که در قضیه آفریقای جنوب غربی، رفتار نابرابر در موضوعات متفاوت را نه تنها مجاز بلکه ضروری دانست. ن.ک:

South West Africa (Diss. Op. Tanaka), *Second Phase, Judgment*, ICJ Reports, 6, 1996, p. 306.

۵۸. این متغیرها شامل حق وتو، میزان حق رأی و پرداخت هزینه است که به منظور ایجاد هماهنگی و ایجاد موازنه بین‌المللی به کار گرفته می‌شود. ن.ک:

Alex Mills, *op. cit.*, pp. 15-16.

اطلاعاتی^{۵۹} نیز مندرج است که مسیر مشارکت همه ذی‌نفع‌ها (اعم از عمومی و خصوصی) را در مدیریت فضای سایبر هموار می‌سازد. در این روش به‌عنوان مثال می‌توان برای دولت‌ها و سازمان‌های فنی، حق رأی بیشتر و برای نمایندگان جامعه مدنی، حق رأی کمتری اختصاص داد. مشکل محتمل در استفاده از روش هندسه متغیر این است که ایجاد چنین نظامی نیازمند مذاکراتی طولانی و جزیی برای جلب منافع همه گروه‌هاست.^{۶۰}

۲-۳. روش خودانتظامی

از نظر برخی حقوق‌دانان، به جهت ماهیت یکپارچه و فرامرزی فضای سایبر، قواعد سنتی صلاحیت، مناسب بافت اینترنت نیست و باید برای اینترنت، حاکمیتی جداگانه به رسمیت شناخت.^{۶۱} نتیجه این نگرش، شیوه خودانتظامی در قانونگذاری در فضای سایبر خواهد بود.^{۶۲} در روش خودانتظامی به‌جای دولت‌ها، شرکت‌های سایبری یا مالکان تارنما ملزم به ایجاد محدودیت در فضای سایبر هستند.^{۶۳} مهم‌ترین دلیل خودانتظامی فضای سایبر این است که فضای سایبر برخلاف دولت‌ها غیرمتمرکز و جهانی است.^{۶۴} همچنین این روش، علاوه بر اینکه کارایی قانونگذاری ملی را داراست، به‌مراتب، ساده‌تر و ارزان‌تر بوده^{۶۵} و به‌دلیل نقش پیشگیرانه این روش از آمار جرایم در فضای سایبر نیز کاسته خواهد شد.

روش خودانتظامی در عمل با مشکلاتی روبه‌روست. اولاً، به دلیل حذف نهاد دولت به‌عنوان رکنی فرادستی، موجب هرج‌ومرج در فضای سایبر خواهد شد.^{۶۶} ثانیاً، از نظر حامیان «مشترکات

۵۹. ماده ۴۹ اعلامیه مذکور، وظایف ذی‌نفعان را به این شرح بیان می‌دارد: دولت‌ها به‌عنوان مقام سیاست‌گذار، بخش خصوصی در بخش توسعه اینترنت در موضوعات فنی و اقتصادی، جامعه مدنی در بخش توسعه سطوح اجتماعی اینترنت، سازمان‌های بین‌دولتی با هدف هماهنگ‌سازی و سازمان‌های بین‌المللی به‌عنوان توسعه‌دهنده استانداردهای فنی.

60. Jovan Kurbalija, *op. cit.*, p. 109.

61. Noel Cox, The Regulation of Cyberspace and the Loss of National Sovereignty, *Information and Communications Technology Law*, vol. 11, 2002, p. 8.

۶۲. در اصطلاح به طرفداران خودانتظامی در فضای سایبر (Cyberians) اطلاق می‌شود.

۶۳. مصداق این روش که تحت عنوان کد به‌عنوان قانون (code as law) مطرح است، به‌کارگیری روند ثبت‌نامی برای جلوگیری از دسترسی افراد زیر ۱۸ سال به محتویات جنسی است. باین‌حال، این روش با احتمال دوزدن سریع قوانین مواجه است. ن.ک:

Lawrence Lessig, *Code and Other Laws of Cyberspace*, Basic Books, New York, 2000, p. 247; M. Gercke, *Understanding Cybercrime: A Guide for Developing Countries*, ITU Development Sector's ICT Applications and Cybersecurity Division, Switzerland, 2011, p. 285.

64. Neil W. Netanel, Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory, *California Law Review*, vol. 88, Issue 2, 2000, pp. 400-401; Antonio Segura-Serrano, *op. cit.*, p. 194.

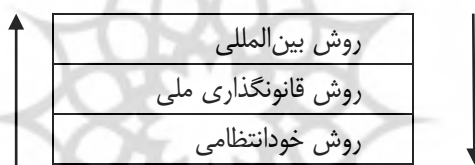
65. Molly Land, Toward an International Law of the Internet, *New York Law School Legal Studies*, vol. 5, 2013, p. 16.

66. Jack L. Goldsmith, Against Cyberanarchy, *University of Chicago Law Review*, No. 40, 1998, p. 1250.

ابتکاری»^{۶۷} الزام تأمین‌کنندگان خدمات اینترنتی به خودسانسوری، خلاقیت در محیط دیجیتال را تحت‌الشعاع قرار می‌دهد. همچنین لازمه اقدام نهادهای فنی و صاحبان تارنماها، داشتن پشتوانه قانونی توسط دولت‌هاست، درحالی‌که دولت‌ها در حال حاضر از این نظر حمایت نمی‌کنند.^{۶۸}

۲-۴. روش مختلط

برخی معتقدند که نباید مدیریت اینترنت را به قانونگذاری ملی یا قانونگذاری بین‌المللی یا شیوه خودانتظامی واگذار کرد. هر یک از سه شیوه قانونگذاری در خصوص مشروعیت یا اجراء، اشکالاتی دارد. با ملاحظه شکل پایین^{۶۹} مشخص می‌شود که برخلاف قانونگذاری بین‌المللی که از بالاترین سطح اجراء و پایین‌ترین سطح مشروعیت برخوردار است، خودانتظامی دارای بالاترین سطح مشروعیت و پایین‌ترین سطح اجراء است. همچنین قانونگذاری ملی، حالتی بینابین بوده و همواره با ضعف نسبی در اجراء و مشروعیت مواجه است.



انتخاب روشی مختلط، زمینه را برای حل معضلات ناشی از مشروعیت و اجراء و همچنین نیل به تفاهم میان همه بازیگران فعال در فضای سایبر باز خواهد کرد. خصیصه برخی جنبه‌های اینترنت مانند جرایم و تجارت اینترنتی به‌گونه‌ای است که نیازمند قانونگذاری است، درحالی‌که مناسب است جنبه‌های زیربنایی فضای سایبر با توجه به تخصصی بودن در اختیار نهادهای غیردولتی حفظ شود. همچنین همکاری بین‌المللی برای یکسان‌سازی حقوقی لازم است. کنوانسیون بوداپست به شیوه مختلط توجه داشته و در ماده ۲۳ به همکاری بین‌المللی و در ماده ۱۱ به قانونگذاری متقابل توجه کرده است.

این مسئله از سوی طیف مقابل، بی‌جواب گذاشته نشد و دیوید پست در مقاله‌ای تحت عنوان «علیه هرج‌ومرج سایبری»، دیدگاه‌های گلد/سمیت را به چالش کشید. ن.ک:

David G. Post, *Against Against Cyberanarchy*, *Berkeley Technology Law Journal*, vol. 17, 2002, p. 378.

67. Creative Commons

مشترکات ابتکاری، نهادی غیرانتفاعی با هدف گسترش و حمایت از آزادی انتشار و استفاده از محتویات سایبری است که خواهان تغییر مقررات کی‌رایت است. میان این گروه و حامیان حقوق مالکیت فکری اختلافات بسیاری وجود دارد.

68. Andrew D. Murray, *The Regulation of Cyberspace*, Routledge Cavendish, Oxon, 2007, pp. 76-77 & 124.

69. Viktor Mayer-Schonberger, *op. cit.*, p. 34.

۳. قانونگذاری در فضای سایبر از منظر حقوق ایران

۳-۱. رویکرد ایران در قانونگذاری فضای سایبر

رویکرد ایران در حیطه مدیریت داخلی اینترنت، مبتنی بر قانونگذاری ملی است. پیرو ابلاغ «سیاست‌های کلی شبکه‌های اطلاع‌رسانه‌ای رایانه‌ای» از سوی مقام رهبری،^{۷۰} شورای عالی انقلاب فرهنگی، «مقررات و ضوابط شبکه‌های اطلاع‌رسانی رایانه‌ای» را در سال ۱۳۸۰ تصویب کرد. طبق این قانون به موازات حق دسترسی آزاد به اطلاعات، بر رعایت حقوق داخلی در موضوعات اجتماعی، فرهنگی و فنی کشور تأکید شد. مقررات پراکنده دیگری مانند آیین‌نامه نحوه اخذ مجوز و ضوابط فنی نقطه تماس بین‌المللی، آیین‌نامه واحدهای ارائه‌کننده خدمات اطلاع‌رسانی و اینترنت رسا (ISP)، مصوبات کمیسیون تنظیم مقررات ارتباطات در سال ۱۳۸۴، قوانین پنج‌ساله توسعه و قانون تجارت الکترونیک نیز وجود دارد، لیکن نخستین قانون جامع و متمرکز در ایران، قانون جرایم رایانه‌ای، مصوب ۱۳۸۸ و قوانین اصلاحی آن، مندرج در قانون آیین دادرسی کیفری ۱۳۹۲ است. اگرچه رویکرد قوانین داخلی ایران بر روش قانونگذاری ملی تکیه دارد، نگرش انتقادی ایران به نحوه مدیریت زیرساخت‌های سایبری در سازمان اینترنتی، انتصاب اسامی و کدهای رقمی (آیکان)^{۷۱} مبین پذیرش روش بین‌المللی در این عرصه از سوی ایران است. آیکان یکی از مراجع مهم در شیوه خودانتظامی در فضای سایبر است که در عین حال از قوانین داخلی امریکا تبعیت می‌کند. انتقاد دولت‌ها به آیکان، مربوط به اساسنامه این سازمان است که طبق آن، وزارت بازرگانی امریکا دارای حق وتو بر تصمیمات سازمان بوده و تغییرات سازمان باید به تصویب دولت امریکا برسد.^{۷۲} بدین جهت در یادداشت ایران بر پیش‌نویس چهارم گزارش دبیرکل اتحادیه بین‌المللی مخابرات چنین آمده است: «مهم‌ترین بخش‌های اینترنت که مربوط به سیاست عمومی است تحت حاکمیت همکاری میان دولت‌ها یا سازمان‌های بین‌المللی نیست بلکه تحت حاکمیت دولت‌های انفرادی است... موضوع فاجعه‌بار آن است که برخی دولت‌ها کنترل اساسی بر بخش‌های حیاتی

۷۰. نامه شماره ۱۰۷۲/۱ مورخ ۱۳۸۰/۳/۱۳ دفتر مقام رهبری.

71. Internet Corporation for Assigned and Numbers (ICANN)

آیکان طبق قانون شرکت‌های غیرانتفاعی و منفعت عمومی برای اهداف خیریه و عمومی ایالت کالیفرنیا تشکیل شد و وظیفه مدیریت تارنماهای اینترنتی و شناسه پروتکل‌ها (IPs) را در فضای سایبر بر عهده دارد.

72. Rebecca E. Casey, ICANN or ICANN t Represent Internet Users, Faculty of the Virginia Polytechnic Institute and State University, Virginia, 2008, pp. 1-2.

کنترل منحصرانه ایالات متحده بر فضای سایبر، نه تنها موجب افزایش امنیت فضای سایبر نمی‌شود، بلکه ادامه این روند، منجر به اتخاذ مواضع تقابلی نظیر ملی‌کردن اینترنت از جانب کشورهای در حال توسعه می‌شود. ن.ک:

The Future US Role in Internet Governance: 7 Points in Response to the U.S. Commerce Dept. s Statement of Principles, Internet Governance Project, Concept Paper by the Internet Governance Project, www.internetgovernance.org, 28 July, 2005, p. 4.

اینترنت دارند».^{۷۳} حمایت ایران از نتایج اجلاس اتحادیه بین‌المللی مخابرات که منجر به ایجاد فشار بر ایالات متحده و تغییر اساسنامه آیکان شد،^{۷۴} مؤید عدم مخالفت ایران با شیوه قانونگذاری بین‌المللی عادلانه است.

رأی مثبت ایران به سند اصلاحی اتحادیه بین‌المللی مخابرات در سال ۲۰۱۲ نیز بیانگر حمایت از رویکرد بین‌المللی است. رویکرد ایران در کنار کشورهای دیگری نظیر چین و کوبا در تقابل با سیطره ایالات متحده بر این فضا، مبتنی بر مشارکت بیشتر سازمان ملل و دولت‌ها در مدیریت کلان فضای سایبر است.^{۷۵} این امر منجر به اتخاذ تصمیماتی در جریان اجلاس جهانی جامعه اطلاعاتی ۲۰۰۵ تونس شد که مسیر را بر بین‌المللی‌سازی فضای سایبر هموار ساخت؛^{۷۶} همان طور که در نامه نماینده دائم ایران در سازمان ملل به دبیرکل این سازمان به ایجاد فضای مشارکت جمعی دولت‌ها، بخش خصوصی، جامعه مدنی و نهادهای بین‌المللی اشاره شده است.^{۷۷}

امروزه طرح شبکه ملی اطلاعات^{۷۸} و مجموعه قوانین حاکم بر فضای سایبر در ایران، نشان‌دهنده رویکرد ملی ایران به قانونگذاری در فضای سایبر است. با این حال، اعمال روش قانونگذاری ملی در قوانین داخلی و پذیرش روش بین‌المللی در مدیریت آینده این فضا حاکی از تمایل ایران به اعمال روش مختلط در قانونگذاری در این فضا است.

۲-۳. صلاحیت قانونگذاری در فضای سایبر در حقوق ایران

با توجه به اینکه امروزه رویکرد اصلی ایران، قانونگذاری ملی در عرصه فضای سایبر است باید شیوه‌های قانونگذاری ایران بررسی شود. این قانونگذاری با اتکا بر اقسام صلاحیت، شامل صلاحیت سرزمینی، شخصی، واقعی و جهانی امکان‌پذیر است.

73. Comment from the Administration of the Islamic Republic of Iran on Fourthdraft of the Secretary-General s Report for the Fifth World Telecommunication/Information and Communication Technology Policy Forum, 2013, p. 2.

74. مطابق موافقت‌نامه پروژه مشترک (Joint Project Agreement) میان وزارت بازرگانی امریکا و آیکان، این سازمان، سالانه موظف به ارائه گزارش به جامعه جهانی است.

75. John W. Berry, The World Summit on the Information Society (WSIS): A Global Challenge in the New Millennium *Network of Illinois Learning Resources in Community Colleges*, vol. 56, 2006, p. 10.

76. در سند اجلاس چنین آمده است: «تمام دولت‌ها باید دارای نقش و مسئولیتی برابر برای حاکمیت اینترنت و تضمین پایداری، امنیت و تداوم اینترنت باشند». ن.ک:

Tunis Agenda for the Information Society, 2005, para. 68.

77. The Letter from Permanent Mission of the Islamic Republic of Iran to the United Nations, Consultation on Enhanced Coopery Issues Pertaining Action on International Public Policy to the Internet , 14 December 2010.

78. تبصره ۲ ماده ۴۶ قانون برنامه پنج‌ساله توسعه و مصوبه جلسه پانزدهم شورای عالی فضای مجازی در تاریخ ۱۳۹۲/۱۰/۳ شبکه ملی اطلاعات و راهکارهای ایجاد آن را تبیین کرده‌اند.

ماده ۳ قانون مجازات اسلامی، مصوب ۱۳۹۲ و قوانین مرتبط با فضای سایبر، از جمله قانون تجارت الکترونیکی، مصوب ۱۳۸۲، قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای، مصوب ۱۳۷۹، قانون جرایم رایانه‌ای، مصوب ۱۳۸۸ و مقررات اصلاحی آن، مندرج در آیین دادرسی کیفری ۱۳۹۲ اصل را بر صلاحیت سرزمینی قرار داده‌اند. تقریباً در تمام مواد قانون جرایم رایانه‌ای و مواد مرتبط در قانون آیین دادرسی کیفری، عبارت «هرکس» بدون توجه به تابعیت مرتکب به کار رفته است. هرچند معیار صلاحیت سرزمینی در جرایم گوناگون سایبری متفاوت است، معیار صلاحیت سرزمینی در ماده ۱ (دسترسی غیرمجاز)، ماده ۲ (شنود غیرمجاز) و ماده ۳ (جاسوسی رایانه‌ای) قانون جرایم رایانه‌ای، معیار وقوع «سامانه‌های رایانه‌ای» در قلمرو ایران است. معیار صلاحیت سرزمینی در مواد ۶ و ۷ قانون جرایم رایانه‌ای نیز وقوع «داده‌های رایانه‌ای» در قلمرو ایران است. بند (الف) ماده ۶۶۴ قانون آیین دادرسی کیفری، معیار دیگری اضافه می‌کند و «ذخیره اطلاعات» در قلمرو ایران را نیز مشمول صلاحیت سرزمینی ایران قرار می‌دهد.^{۷۹} به علاوه بند (ب) این ماده، تارنماهای دارای دامنه مرتبه بالای کد کشوری ایران (ir) را در حکم خاک ایران قلمداد کرده و جرایم ارتكابی در این تارنماها را به مانند جرایم ارتكابی در قلمرو ایران می‌داند.^{۸۰}

صلاحیت شخصی فعال در ماده ۷ قانون مجازات اسلامی به طور موسع آمده است و تمامی جرایم از جمله جرایم رایانه‌ای را دربرمی‌گیرد. ماده ۸ قانون مجازات اسلامی نیز به صلاحیت شخصی منفعل، اختصاص یافته است، هرچند اعمال آن، مشروط به جرم‌نگاری متقابل شده است. اغلب جرایم ارتكابی در فضای سایبر از سوی بارگذاران ارتكاب می‌یابد. لذا قانون جرایم رایانه‌ای در اغلب موارد، همانند ارتكاب هتک حیثیت و نشر اکاذیب در مواد ۱۶ و ۱۷ بارگذار را مجرم تلقی کرده است و لذا او مشمول صلاحیت قانونی ایران می‌شود. باین‌حال، ماده ۱۴ در باب انتشار، توزیع، معامله، تولید، ذخیره یا نگهداری محتویات مستهجن، علاوه بر بارگذار، پیاده‌ساز را نیز مشمول مجازات دانسته است.

صلاحیت واقعی در ماده ۵ قانون مجازات اسلامی آمده است و صراحتاً اقدام علیه امنیت داخلی یا خارجی را در حیطه صلاحیت ایران می‌داند. همچنین مطابق بند (پ) ماده ۶۶۴ قانون آیین دادرسی کیفری، ارتكاب جرم در خارج از ایران علیه سامانه‌ها یا تارنماهای مورد استفاده قوای سه‌گانه، نهاد رهبری، نمایندگی‌های رسمی دولت، نهادهای ارائه‌کننده خدمات عمومی و علاوه بر این، حمله گسترده به تارنماهای مرتبه بالای کد کشوری را در شمول صلاحیت محاکم ایران کرده است.

۷۹. داده‌های مجرمانه یا داده‌هایی که برای ارتكاب جرم به کار رفته است، به هر نحو در سامانه‌های رایانه‌ای و ارتباطاتی یا حامل‌های داده موجود در قلمرو حاکمیت زمینی، دریایی و هوایی جمهوری اسلامی ایران ذخیره شده باشد.

۸۰. جرم از طریق تارنماهای دارای دامنه مرتبه بالای کد کشوری ایران ارتكاب یافته باشد.

در خصوص صلاحیت جهانی، ماده ۹ قانون مجازات اسلامی، جرایمی را که طبق عهدنامه‌ها و مقررات بین‌المللی تحت صلاحیت جهانی قرار گرفته در صلاحیت تمامی کشورها و از جمله ایران می‌داند. در قوانین ایران در این خصوص صراحتی وجود ندارد. با این حال، جرایم موضوع بند (ت) ماده ۶۶۴ قانون آیین دادرسی کیفری^{۸۱} راجع به جرایم رایانه‌ای علیه اطفال کمتر از ۱۸ سال^{۸۲} می‌تواند تحت شمول صلاحیت جهانی ایران قرار گیرد.

بنابراین قوانین ایران در اغلب موارد، بخصوص موضوعات مرتبط با سامانه‌ها، داده‌ها و تارنماهای اینترنتی با تعیین صلاحیت بر مبنای مکان داده‌ها، صلاحیت سرزمینی را پذیرفته است. این قوانین، صلاحیت شخصی را درباره جرایم علیه اشخاص، صلاحیت واقعی را راجع به سامانه‌ها و تارنماهای حکومتی و صلاحیت جهانی را صرفاً در خصوص سوءاستفاده از اطفال شناسایی کرده است. لذا رویکرد ایران در صلاحیت قانونگذاری در فضای سایبر، در بردارنده طیف متنوعی از صلاحیت‌های قانونگذاری سرزمینی، شخصی، واقعی و جهانی است؛ هرچند در عرصه منطقه‌ای با نظر به عضویت ایران در سازمان همکاری‌های اسلامی می‌توان یکسان‌سازی قوانین ملی در سطح منطقه را پیشنهاد داد. این روش در گذشته در اتحادیه اروپا،^{۸۳} اتحادیه عرب^{۸۴} و شورای همکاری خلیج فارس^{۸۵} نیز تجربه شده است. این امر با توجه به دیدگاه مشترک کشورهای عضو سازمان کنفرانس اسلامی به برخی مقولات فضای سایبر، همچون هرزه‌نگاری و قلمرو آزادی بیان در حوزه مذهب، ممکن‌الاحصول خواهد بود.

نتیجه

دیدگاه حاکمیت انحصاری دولت بر فضای سایبر که متأثر از پذیرش مفهوم وستفالیایی حاکمیت در این فضا است، رفته‌رفته با پیدایش مفاهیم سیاسی و حقوقی نظیر جهان‌شمولی، مسئولیت بین‌المللی، اصل عدم مداخله و قواعد حقوق بشری با چالش مواجه شد. متعاقباً رویکرد تعمیم نظریه میراث مشترک بشریت با هدف خارج کردن این فضا از انحصار دولت‌ها مطرح شد. علی‌رغم امتیازات دیدگاه اخیر، اعمال آن در فضای سایبر با این اشکال همراه است که تا کنون معاهده‌ای انتظام‌بخش

۸۱. بند (د) ماده ۲۸ قانون جرایم رایانه‌ای مقرر می‌داشت: «جرایم رایانه‌ای متضمن سوءاستفاده از اشخاص کمتر از هجده سال، اعم از آنکه مرتکب یا بزه‌دیده ایرانی یا غیرایرانی باشد». (مواد ۲۸ تا ۵۱ این قانون، با ماده ۶۹۸ قانون آیین دادرسی کیفری مصوب ۱۳۹۲/۱۲/۴ از تاریخ لازم‌الاجرا شدن قانون اخیر(۱۳۹۴/۴/۱) صریحاً لغو شده و بخش دهم قانون اخیر، با عنوان آیین دادرسی جرایم رایانه‌ای، مواد ۶۶۴ تا ۶۸۷ جایگزین آن شده است). بند (ت) ماده ۶۶۴ قانون آیین دادرسی کیفری ضمن تکرار همین متن، قید «و مرتکب در ایران یافت شود» را به انتهای عبارت افزوده است.

۸۲. قید سوءاستفاده در این بند، محدود به هرزه‌نگاری نبوده و دامنه وسیع‌تری خواهد داشت.

83. Article 83 of Treaty on the Functioning of the European Union, (Entered into force 2009).

84. Decision of the Arab Justice Ministers Council, 19th session, 2003.

85. Recommendations of the Conference on Combating Cybercrime in the GCC Countries, 2007.

در این راستا در سطح بین‌المللی تنظیم نشده است. دولت‌ها در حیطه قانونگذاری سایبری، یک یا چند نوع از اقسام روش‌های قانونگذاری را به کار بسته‌اند. اتخاذ منحصراً هر یک از روش‌ها، مزایا و معایب خاص خود را دارد. در این میان، روش مختلط با رفع اشکالات ناشی از اتکای صرف بر هر یک از اقسام قانونگذاری، روشی مرکب را ارائه کرده که تلفیقی از مزایای هر سه روش قانونگذاری ملی، بین‌المللی و خودانتظامی است؛ روشی که بر مبنای آن، زیرساخت‌های سایبری در اختیار بخش خصوصی، حاکمیت ملی در قالب قانونگذاری ملی و همکاری‌های بین‌المللی در پرتو روش بین‌المللی تجلی می‌یابد. لذا روش مختلط می‌تواند زمینه را برای نیل به تفاهم میان کشورها و گروه‌های فعال در زمینه فضای سایبر باز کند.

با وجود تأکید قوانین داخلی ایران بر قانونگذاری ملی، مواضع بین‌المللی ایران در اتحادیه بین‌المللی مخابرات، مبنی بر خروج زیرساخت‌های سایبری از انحصار قوانین کشورهای غربی در کنار تأکید بر همکاری همه‌جانبه بین‌المللی میان همه ذی‌نفعان و پذیرش سند اصلاحی اتحادیه، گواه بر پذیرش روش مختلط در مدیریت فضای سایبر از سوی ایران است. در راستای جلب منافع همه ذی‌نفعان به‌ویژه کشورهای در حال توسعه در چرخه مدیریت بین‌المللی این فضا می‌توان از رویکرد هندسه متغیر که حاوی حق رأی یا حق مدیریت نابرابر باشد، بهره جست. همچنین تدوین کنوانسیون مشابه کنوانسیون بوداپست میان کشورهای اسلامی، درخور توجه است. جمهوری اسلامی ایران می‌تواند در چارچوب سازمان همکاری‌های اسلامی با تدوین مسائل مشترک اسلامی در روند بین‌المللی‌سازی فضای سایبر، نقش آفرینی کند.

منابع:

الف) فارسی

- افضل‌ی، رسول، محمدباقر قالیباف و میثم احمدی فیروزجائی؛ «تبیین تحولات مفهوم مرز در فضای سیاسی مجازی»، پژوهش‌های جغرافیایی انسانی، دوره ۴۵، شماره ۱، ۱۳۹۲.
- جلالی فراهانی، امیرحسین؛ درآمدی بر آیین دادرسی کیفری جرایم سایبری، خرسندی، ۱۳۸۹.
- دی آنجلیز، جینا؛ جرایم سایبر، ترجمه: سعید حافظی و عبدالصمد خرم‌آبادی، دبیرخانه شورای عالی اطلاع‌رسانی، ۱۳۸۳.
- متین‌دفتری، احمد؛ سیر تحول حقوق بین‌الملل دریایی (از گرو سیوس تا کنفرانس‌های ژنو)، گنج دانش، ۱۳۸۷.

ب) انگلیسی

- Books

- Andrew D. Murray, *The Regulation of Cyberspace*, Routledge Cavendish, Oxon, 2007.
- Anthony Aust, *Handbook of International Law*, Cambridge University Press, New York, 2010.
- David J. Bederman, *The Spirit of International Law*, University of Georgia Press, Athens, 2002.
- David S. Wall, *Cybercrime: The Transformation of Crime in the Information Age*, Polity Press, Cambridge, 2008.
- Graham J. H. Smith, *Internet Law and Regulation*, Sweet and Maxwell, London, 2002.
- Hu Ling, *Shaping the Virtual State: Internet Content Regulation in China (1994-2009)*, University of Hong Kong, Hong Kong, 2011.
- Jovan Kurbalija, *An Introduction to Internet Governance*, Diplo Foundation, Malta, 2014.
- Lawrence Lessig, *Code and Other Laws of Cyberspace*, Basic Books, New York, 2000.
- M. Gercke, *Understanding Cybercrime: A Guide for Developing Countries*, ITU Development Sector's ICT Applications and Cybersecurity Division, Switzerland, 2011.
- Stein Schjolberg, Solange Ghernaouti-hélie, *A Global Protocol on Cybersecurity and Cybercrime*, Cybercrimedata, Oslo, 2009.
- William A. Schabas, Nadia Bernaz, *Routledge Handbook of International Criminal Law*, Taylor & Francis Group, New York, 2011.

- Articles

- A. V. Lowe, Blocking Extraterritorial Jurisdiction: The British Protection of Trading Interests Act *The American Journal of International Law*, vol. 75, No. 2, 1981.
- Alex Mills, Towards a Public International Perspective on Private International Law: Variable Geometry and Peer Governance, *Faculty of Laws*, 2012.
- Andrew Linklater, Citizenship and Sovereignty in the Post-Westphalian State *European Journal of International Relations*, vol. 2, 1996.
- Antonio Segura-Serrano, International Regulation and the Role of International Law, *Max Plank Yearbook of United Nations Law*, vol. 10, 2006.
- Anupam Chander & Madhavi Sunder, The Romance of the Public Domain *California Law Review*, vol. 92, 2004.
- Armando A. Cottim, Cybercrime, Cyberterrorism and Jurisdiction: An Analysis of Article 22 of the COE Convention on Cybercrime, *European Journal of Legal Studies*, vol. 2, Issue 3, 2010.
- Steve Coughlan, Robert J. Currie, Hugh M. Kindred, Teresa Scassa, GlobalReach, Local Grasp: Constructing Extraterritorial Jurisdiction in the Age of Globalization, (2007) 6 *Canadian Journal of Law and Technology*, Canada, 2006.
- Rebecca E. Casey, ICANN or ICANN t Represent Internet Users, *Faculty of the Virginia Polytechnic Institute and State University*, Virginia, 2008.
- David G. Post, Against Against Cyberanarchy *Berkeley Technology Law Journal*, vol. 17, 2002.
- David R. Johnson & David Post, Law and Borders- The Rise of Law in Cyberspace *Stanford Law Review*, vol. 48, Issue 5, 1996.
- Dina Koutouki, Human Rights: Benefits of Information Technology, *University of New Brunswick Law Journal*, No. 48, 1999.
- The Future US Role in Internet Governance: 7 Points in Response to the U.S. Commerce Dept. s Statement of Principles *Concept Paper by the Internet Governance Project*, www.internetgovernance.org, 28 July, 2005.
- Jack Goldsmith, Regulation of the Internet: Three Persistent Fallacies, *Chicago-Kent Law Review*, vol. 73, 1998.
- Jack Goldsmith, The Internet and the Legitimacy of Remote Cross-Border Searches, *University of Chicago Legal Forum*, vol. 16, 2001.
- Jack L. Goldsmith, Against Cyberanarchy *University of Chicago Law Review*, No. 40, 1998.
- Jack L. Goldsmith, The Internet and the Abiding Significance of Territorial Sovereignty *Indiana Journal of Global Legal Studies*, vol. 5, Issue 2, 1998.

- James R. Pielemeier, 'Why General Personal Jurisdiction over 'Virtual Stores' Is a Bad Idea' *Quinnipiac Law Review*, vol. 27, 2009.
- Jennifer A. Zerk, 'Extraterritorial Jurisdiction: Lessons for the Business and Human Rights Sphere from Six Regulatory Areas', *Corporate Social Responsibility Initiative*, No. 59, 2010.
- John H. Jackson, 'Sovereignty - Modern: A New Approach to an Outdated Concept' *Georgetown Law Faculty Publications*, vol. 97, 2010.
- John W. Berry, 'The World Summit on the Information Society (WSIS): A Global Challenge in the New Millennium' *Network of Illinois Learning Resources in Community Colleges*, vol. 56, 2006.
- Kelly A. Gable, 'Cyber-Apocalypse Now: Securing the Internet against Cyberterrorism and Using Universal Jurisdiction as a Deterrent', *Vanderbilt Journal of Transnational Law*, vol. 43, Issue 1, 2010.
- Mohammad Hadi Sohrabi-Haghighat, 'NewMedia and Social-political Change in Iran', *CyberOrient*, vol. 5, 2011.
- Molly Land, 'Toward an International Law of the Internet' *New York Law School Legal Studies*, vol. 5, 2013.
- Neil W. Netanel, 'Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory', *California Law Review*, vol. 88, Issue 2, 2000.
- Noel Cox, 'The Regulation of Cyberspace and the Loss of National Sovereignty' *Information and Communications Technology Law*, vol. 11, 2002.
- Robert Uerpmann-Wittzack, 'Principles of International Internet Law', *German Law Journal*, vol. 11, 2010.
- Solange Ghernaouti-Helie, 'We Need a Cyberspace Treaty' *Inter Media*, vol. 38, Issue 3, 2010.
- Viktor Mayer-Schonberger, 'The Shape of Governance: Analyzing the World of Internet Regulation' *Virginia Journal of International Law*, No. 43, 2002-2003.
- W. Michael Reisman, 'Sovereignty and Human Rights in Contemporary International Law' *Yale Law School Legal Scholarship Repository*, vol. 84, Issue 1, 1990.
- Wolff Heintschel von Heinegg, 'Legal Implications of Territorial Sovereignty in Cyberspace', *4th International Conference on Cyber Conflict*, 2012.

- Awards

- Bundesgerichtshof, Toeben (Federal Court), Award 12 December 2000.
- *Dow Jones & Company Inc. v. Gutnick*, Award 10 December 2002.
- Tribunal de Grande Instance de Paris, UEJF et Licra c/ Yahoo! Inc., Award 20 November 2000

- *Gator.com Corp. v. L.L. Bean Inc.*, Award 15 February 2005.
- *Inset Systems Inc. v. Instruction Set Inc.*, Award 17 April 1996.
- *Martiz Inc. v. Cybergold Inc.*, Award 19 August 1996.
- *Playboy Enterprises, Inc. v. Chuckleberry Publishing Inc.*, Award 19 June 1996.
- *R. v. Stephane Laurent Perrin EWCA Crim 747*, 2002, Award 22 March, 2002.
- South West Africa (Diss. Op. Tanaka), Second Phase, Judgment, ICJ Reports, 6, 1996.
- *United States of America v. Aleksey Vladimirovich Ivanov*, Crim. No. 3:00CR00183 (AWT), Award 6 December 2001.

- Treaties

- Council of Europe Cybercrime Convention, Budapest, (Adopted 2001, Entered into Force 2004).
- Final Acts of the World Conference on International Telecommunications, Dubai, (Signed 2012, Will enter into force 2015).
- Treaty on the Functioning of the European Union, (Entered into force 2009).

- Acts

- Act of Moniteur Belge - Belgisch Staatsblad, 10 February 1999.
- Decision of the Arab Justice Ministers Council, 19th session, 2003.
- UNCITRAL Model Law on Electronic Commerce with Guide to Enactment, 1996.
- ITU Global Cybersecurity Agenda (GCA), *International Telecommunication Union*, 2007.
- USA PATRIOT Act, 2001.
- Tunis Agenda for the Information Society, 2005.
- 18 U.S. Code § 2252.
- 18 U.S. Code § 1466A.

- Reports

- Comment from the Administration of the Islamic Republic of Iran on Fourth Draft of the Secretary-General's Report for the Fifth World Telecommunication/Information and Communication Technology Policy Forum, 2013.
- Recommendations of the Conference on Combating Cybercrime in the GCC Countries, 2007.
- The Letter from Permanent Mission of the Islamic Republic of Iran to the United Nations, Consultation on Enhanced Cooperative Issues Pertaining Action on International Public Policy to the Internet 14 December 2010.