




The University of Tehran Press

Regulatory Models for the Cyberspace: Providing a Comprehensive Framework of Regulation for the National Environment

Mohammad Reza Hosseini¹ 

1. Associate Professor of International Law, International Law Group, School of National Security, Supreme National Defense University, Tehran, Iran. Email: rezahsn88@gmail.com

Article Info	Abstract
<p>Article Type: Research Article</p> <p>Pages: 1213-1239</p> <p>Received: 2022/06/16</p> <p>Received in revised form: 2023/01/25</p> <p>Accepted: 2023/05/22</p> <p>Published online: 2023/09/23</p> <p>Keywords: <i>cyberspace,</i> <i>cyber-libertarianism,</i> <i>cyber-paternalism,</i> <i>law-making frameworks,</i> <i>regulatory models.</i></p>	<p>The cyberspace is a human ecosystem that is extremely complex. In such a space different paradigms, approaches and methods of regulation are possible. The regulatory paradigms of the cyberspace are based on two basic approaches, namely: cyber paternalism and cyber libertarianism. Under these two paradigms, different models for regulating the relationships of the cyberspace actors exist. This paper seeks to answer the fundamental questions of how law-making can take place in the dynamic, complex, and networked environments of the cyberspace? And which model can be applied as a desirable framework for regulating the cyberspace? The present study, which uses a comparative and descriptive method, evaluates different models of cyberspace regulation in order to obtain the desired model for Iran. The results show that due to the uncertainty and complexity of the cyberspace, a dynamic and flexible regulatory framework should be considered as a suitable regulatory model for the cyber environment both nationally and internationally. While Iran's approach to regulating the cyberspace at the national level should be based on the paternalistic paradigm, its approach at the international level should follow libertarianism.</p>
How To Cite	Hosseini, Mohammadreza (2023). Regulatory Models for the Cyberspace: Providing a Comprehensive Framework of Regulation for the National Environment. <i>Public Law Studies Quarterly</i> , 53 (3), 1213-1239. DOI: https://doi.com/10.22059/JPLSQ.2023.344418.3102
DOI	10.22059/JPLSQ.2023.344418.3102
Publisher	The University of Tehran Press. 



انتشارات دانشگاه تهران

فصلنامه مطالعات حقوق عمومی

شاپا الکترونیکی: ۱۱۳۹-۲۴۲۳

دوره: ۵۳، شماره: ۳

پاییز ۱۴۰۲

Homepage: <http://jpls.ut.ac.ir>

الگوهای مقررات گذاری در فضای سایبر:

ارائه چارچوب جامع تنظیم‌گری برای محیط ملی

محمد رضا حسینی ✉

۱. دانشیار حقوق بین‌الملل، گروه حقوق بین‌الملل، دانشکده امنیت ملی، دانشگاه عالی دفاع ملی، تهران، ایران. رایانامه: rezahsn88@gmail.com

اطلاعات مقاله	چکیده
<p>نوع مقاله: پژوهشی</p> <p>صفحات: ۱۲۱۳-۱۲۳۹</p> <p>تاریخ دریافت: ۱۴۰۱/۰۳/۲۶</p> <p>تاریخ بازنگری: ۱۴۰۱/۱۲/۰۵</p> <p>تاریخ پذیرش: ۱۴۰۲/۰۳/۰۱</p> <p>تاریخ انتشار برخط: ۱۴۰۲/۰۷/۰۱</p> <p>کلیدواژه‌ها: چارچوب‌های مقررات گذاری، سایبرلیبرالیسم، سایبرپاترنالیسم، فضای سایبر، مدل‌های تنظیم‌گری.</p>	<p>فضای سایبر یک زیست‌بوم جدید برای بشر و به‌عنوان یک فضای پیچیده شناخته شده است؛ فضایی که در آن پارادایم‌ها، رویکردها و الگوهای مختلفی برای مقررات‌گذاری و تنظیم‌گری پیشنهاد شده است. پارادایم‌های حاکم بر فضای سایبر بر دو رویکرد اساسی پاترنالیست سایبری و لیبرتارینیسم (لیبرالیسم) سایبری استوار است که ذیل هر کدام از این دو پارادایم، الگوها و مدل‌های مختلفی برای تنظیم روابط کنشگران فضای سایبر ارائه شده است. این مقاله به‌دنبال پاسخ به این پرسش‌های اساسی است که در محیط‌های پویا، پیچیده و شبکه‌ای چگونه می‌توان اقدام به تنظیم مقررات کرد؟ و از میان این الگوهای پیشنهادی، کدام مدل می‌تواند به‌عنوان چارچوب مطلوب برای مقررات‌گذاری و تنظیم فضای سایبر اعمال شود؟ مقاله حاضر که با استفاده از روش تحلیلی و توصیفی انجام گرفته، مدل‌های مختلف مقررات‌گذاری فضای سایبر را ارزیابی کرده تا به الگوی مطلوب برای کشورمان دست پیدا کند. نتایج نشان می‌دهد که با توجه به عدم قطعیت و پیچیدگی فضای سایبر، چارچوب مقررات‌گذاری پویا و دینامیک می‌تواند به‌عنوان الگوی تنظیم‌گر مناسب برای محیط سایبری هم در سطح ملی و هم بین‌المللی به‌شمار رود. رویکرد ایران برای تنظیم مقررات فضای سایبر در سطح ملی باید مبتنی بر پارادایم پاترنالیستی باشد و در سطح بین‌المللی از لیبرتارینیسم تبعیت کند.</p>
<p>استناد</p> <p>حسینی، محمد رضا (۱۴۰۲). الگوهای مقررات گذاری در فضای سایبر: ارائه چارچوب جامع تنظیم‌گری برای محیط ملی. <i>مطالعات حقوق عمومی</i>، ۵۳ (۳)، ۱۲۱۳-۱۲۳۹. DOI: https://doi.com/10.22059/JPLSQ.2023.344418.3102</p>	
DOI	10.22059/JPLSQ.2023.344418.3102
ناشر	مؤسسه انتشارات دانشگاه تهران.



۱. مقدمه

مقررات‌گذاری ابزاری است که برای کنترل رفتارهای اجتماعی بشر استفاده می‌شود. هدف اصلی مقررات‌گذاری تنظیم رفتار افراد یک جامعه و ضرورتی انکارناپذیر برای زیست اجتماعی است. اگرچه ایجاد چارچوب‌های قانونی توسط دولت‌ها در نگاه اول مانع آزادی است، ولی در واقع محدودیت ناشی از مقررات‌گذاری به آزادی بیشتر منجر می‌شود و هنگامی که فردی متعرض حقوق دیگران می‌شود، مقررات‌گذاری جنبه حمایت از آزادی پیدا می‌کند (هداوند، ۱۳۸۵: ۵۰).

اکنون فضای مجازی به‌عنوان یک زیست‌بوم جدید، تمام ابعاد زندگی بشری را در خود جای داده است و مقررات‌گذاری در این فضا نیز برای تنظیم روابط اجتماعی امری اجتناب‌ناپذیر است. از زمانی که فضای سایبر آشکارا در روابط اجتماعی تأثیر گذاشته و ارتباطات را متحول ساخته، مقوله مقررات‌گذاری به مهم‌ترین چالش حکمرانی دولت‌ها تبدیل شده است. بدون وجود مقررات، حقوق ذی‌نفعان و کاربران و بازیگران فضای مجازی پامال خواهد شد و روابط اجتماعی تضعیف می‌شود. از این‌رو مقررات‌گذاری فضای سایبر پیش‌نیاز ضروری توسعه در محیط ملی و بین‌المللی است (Klarić & Perešin, 2016: 43).

«مقررات‌گذاری فضای سایبر» مفهومی پیچیده و در عین حال بسیط است. این عبارت شامل مجموعه‌ای از فرایندهای تقنینی، کنترلی و اجرایی است که تلاش می‌کند تا دو مقوله متفاوت را که می‌توانند از یکدیگر مجزا و متضاد به‌نظر برسند، باهم آشتی دهد و آنها را به تعادل بکشد. این مفهوم درصدد تأمین حقوق و آزادی‌های مشروع بازیگران و ذی‌نفعان فضای سایبر از یک سو، و برقراری و ارتقای امنیت ملی و حاکمیت دولت‌ها از سوی دیگر است.

با ورود فضای مجازی به زیست‌بوم بشری و ظهور و توسعه شبکه‌های اجتماعی، نظام تنظیم‌گری و مقررات‌گذاری سنتی دیگر پاسخگوی نیز دچار چالش جدی شد. مدل‌های مقررات‌گذاری و تنظیم‌گری در فضای مجازی، مبتنی بر دو نوع نگرش (پارادایم) متفاوت به فضای سایبر است. نگرش نخست، مبتنی بر «رویکرد پدرسالارانه و سلسله‌مراتبی دولت‌ها» (سایبرپاترنالیسم) و رویکرد دوم مبتنی بر «آزادی و چندذی‌نفعی» (سایبرلیبرالیسم یا لیبرتارینیسم) است. ذیل هر یک از این دو پارادایم (مکتب)، الگوهای مقررات‌گذاری و تنظیم‌گری مختلفی ارائه شد. با توجه به ویژگی‌ها و نقاط ضعف و قوت این دو رویکرد، برخی حقوقدانان و اندیشمندان این فضا، رویکرد سومی بینابینی و مختلط مبتنی بر چهار مؤلفه اجتماعی - حقوقی - فنی - اقتصادی^۱ را مطرح کردند تا ضمن رفع نواقص این الگوها، زمینه را برای همراهی و مشارکت بیشتر کنشگران فضای سایبر هموار سازند (موری، ۱۳۹۸: ۱۲).

در واقع می‌توان گفت در فضای سایبر دو پارادایم حقوقی در مقابل هم قرار گرفته‌اند: پارادایم سایبر لیبرتارینیسم^۱ و پارادایم سایبر پاترنالیسم^۲. هریک از این پارادایم‌ها (مکاتب) طرفداران خود را دارند. طرفداران پارادایم سایبر لیبرالیسم یا آزادی سایبری تصور می‌کنند که فقدان اثربخشی سیستم‌های کنترلی و ناکارایی قوانین سنتی در فضای سایبر به معنای آزادی محیط آنلاین (برخط) است؛ اما طرفداران سایبرپاترنالیسم (کسانی که اصرار دارند فضای سایبر را باید به صورت سلسله مراتبی از بالا به پایین کنترل کرد) معتقدند که می‌توان این فضا را با ابزارهای قانونی در کنار ابزارهای فنی مدیریت کرد. طرفداران این پارادایم اجرای سیستم‌های تنظیم مقررات حقوقی سنتی را در فضای سایبر بسیار پیچیده و پرهزینه می‌دانند و علت آن را ناشی از عوامل مختلفی همچون ناشناخته بودن، فیزیکی نبودن، دیجیتالی بودن محتوا، محیط انعطاف‌پذیر و ماهیت بین‌المللی یا فرامرزی بودن آن می‌دانند. ساختار و ویژگی‌های فضای سایبر تأثیر شگرفی در نظام تنظیم‌گری و مقررات‌گذاری دارد. از این رو از یک سو، ابزارها و عوامل کنترل‌کننده و نظارتی فضای سایبر به ماهیت و ویژگی‌های این فضا برمی‌گردد، و از سوی دیگر به نگرش و پارادایم حاکم بر فضای سایبر وابسته است (موری، ۱۳۹۸: ۱۳).

به‌طور کلی، حامیان مکتب سایبرلیبرالیسم (سایبرلیبرتارینیسم) معتقد به استقلال فضای سایبر از فضای واقعی‌اند و هرگونه مقررات‌گذاری آن را از سوی دولت‌ها بی‌فایده می‌دانند؛ اما پیروان سایبر پاترنالیسم اعتقاد دارند فضای سایبر باید توسط سلسله‌مراتب از سوی سازمان‌ها و نهادهای بین‌المللی و سپس دولت‌ها و سایر ذی‌نفعان به صورت دقیق و مانند فضای حقیقی تنظیم شود.

با توجه به چالش‌های دو پارادایم پیش‌گفته، رویکرد بینابینی و تلفیقی از دو پارادایم قبلی شکل گرفت که تأکید دارد: «الگوی کنترل و تنظیم فضای سایبر باید ترکیبی از چهار مؤلفه (اجتماعی-حقوقی-فنی و اقتصادی) باشد. این چهار مؤلفه در کنار هم می‌توانند تا حد زیادی پاسخگوی پیچیدگی و آشوبناکی فضای مجازی باشند». این پارادایم برخلاف مکاتب سایبرلیبرالیسم که استدلال می‌کردند فضای مجازی غیرقابل تنظیم است، و یا سایبرپاترنالیسم که معتقدند باید نوعی کنترل نظارتی سلسله مراتبی حاکم باشد، تصریح می‌کند: «ابزار حقوق در کنار هنجارهای اجتماعی، معماری فناوری و اقتصاد دیجیتال که در مجموع به‌عنوان «کد» شناخته می‌شود، می‌تواند به چالش‌های تنظیم‌گری در فضای سایبر پاسخ دهد. «کد» به‌عنوان بستر نرم‌افزاری فضای مجازی، هم به‌مثابه پروتکل‌های تشکیل‌دهنده شبکه، و هم به‌عنوان مجموعه قوانین و مقررات، توانایی حفظ منافع و امنیت ملی، صیانت از حقوق

1. Cyber-libertarianism

2. Cyber-paternalism

ذی‌نفعان و کنشگران این فضا کنترل و نظارت بر رفتارهای اجتماعی در این محیط را دارد» (Reed, 2012: 11). از این رو طراحی نظام مقررات‌گذاری متناسب با ویژگی‌های فضای سایبر از اهمیت زیادی برخوردار است. کشورهای توسعه‌یافته از الگوهای تنظیم‌گری متفاوتی بهره گرفته‌اند. در کشورمان نیز تلاش‌هایی برای مقررات‌گذاری این فضا انجام گرفته، اما عدم تعیین رویکرد مطلوب و گزینش پارادایم مناسب با توجه به مقتضیات بومی موجب شده است الگوی مشخصی در این حوزه را نتوان انتخاب و بومی‌سازی کرد. وجود الگوی مقررات‌گذاری مناسب می‌تواند علاوه بر ایجاد انسجام، یکپارچگی و هماهنگی در تنظیم قوانین، جهت حرکت نهادهای تنظیم‌گر و رگولاتور را مشخص و از وضع قوانین موازی، متداخل و متضاد جلوگیری کند. از این رو در این تحقیق سعی بر آن است که به این پرسش‌ها پاسخ داده شود که چه پارادایم‌ها و الگوهای تنظیم‌گری و مقررات‌گذاری در فضای سایبری وجود دارد؟ و با توجه به مقتضیات جمهوری اسلامی ایران چه الگویی می‌تواند کاربرد بیشتری داشته باشد؟ برای پاسخ به پرسش‌ها، ابتدا به بررسی مطالعات، یافته‌ها و تحقیقات اندیشمندان و متفکران در این حوزه می‌پردازیم. سپس ویژگی‌ها، مشخصات، ابعاد و قابلیت‌های فضای سایبر را تعریف و مدل‌های مقررات‌گذاری و تنظیم‌گری این فضا را تشریح می‌کنیم.

۲. مبانی نظری تحقیق

اصطلاح تنظیم‌گری اولین بار در فرانسه در ۱۴۶۰م به کار گرفته شد، اما در مفهوم خاص حقوقی آن در اواخر قرن نوزدهم در این کشور برای تبیین صلاحیت و کارکردهای نهادهای خاص، معادل مراجع اداری مستقل در حقوق کنونی، به عنوان تنظیم‌کننده فعالیت و روابط آزاد و خصوصی در برخی حوزه‌ها از آن استفاده شده است (یاوری، ۱۳۹۳: ۶۲۹-۶۴۷).

در کنار سازوکارها، شیوه‌ها و ابزارها و نهادهای کلاسیک مداخله دولت در اداره امور عمومی از طریق قانونگذاری، اجرایی و قضایی، اشکال و ابزار دیگری نیز پیش‌بینی شده است. در این زمینه، بازیگران خاص و مستقل از دولت (نهادهای تنظیم‌گر یا رگلاتورها) در تنظیم‌گری وارد عمل می‌شوند. بر این اساس، دولت دیگر فعال مایه انحصاری در عرصه اداره امور اجتماعی نبوده؛ و قوانین نیز تنها ابزار تنظیم‌کننده روابط جمعی در محیط‌های پیچیده نیست.

گسترش فناوری‌های اطلاعات و ارتباطات و ظهور فضای سایبر و پیدایش شبکه جهانی اینترنت، موجب تحول وسیع اجتماعی و تغییر در حاکمیت و شیوه‌های حکمرانی دولت‌ها شده است. توسعه شبکه ارتباطی با قابلیت‌های پیچیده ذخیره‌سازی، پردازش و توزیع اطلاعات به وابستگی همه شئون زیست

بشری به این فضا منجر شده است. این تحولات ضرورت وضع قواعد جدید برای تنظیم روابط اجتماعی به‌خصوص در حوزه‌های حاکمیتی را نمایان کرده است. (Gisela & Natarajan, 2020: 68) شناخت و تبیین ویژگی‌های فضای مجازی می‌تواند به مقررات‌گذاری و تنظیم‌گری بهتر در این فضا کمک کند. در جدول ۱ به برخی از مهم‌ترین ویژگی‌های آن اشاره شده است. البته و ویژگی‌های فضای سایبر محدود به موارد زیر نیست و بر اساس دیدگاه‌های کارشناسان این حوزه توسعه یافته است.

جدول ۱. ویژگی‌های فضای سایبر

ویژگی‌ها	توضیحات
نامحدود و فرامرزی	فضای سایبر محدوده مشخصی ندارد و محیط سایبر محیطی بدون مرز است. حاکمیت در فضای سایبر وجود ندارد. اطلاعات در فضای سایبر به‌صورت غیرمتمرکز قابلیت ذخیره‌سازی و بهره‌برداری است (کیان‌خواه، ۱۳۹۶: ۷۵).
توسعه و تغییرپذیری	ماهیت فضای سایبر و پیشرفت روزافزون علوم مرتبط موجب شده، روزانه شاهد ظهور برنامه‌ها، نرم‌افزارها و خدمات اینترنتی متنوعی باشیم که وجود برنامه‌ریزی‌های مناسب برای استفاده صحیح این ابزارها را ضرورت می‌بخشد (فیروزآبادی، ۱۳۹۹: ۲۴-۲۸).
جذابیت و تنوع	در فضای سایبر حجم اطلاعات در قالب متن، صدا، فیلم، بازی‌های رایانه‌ای، موسیقی، کتاب‌ها، مجلات و چت‌های آنلاین منبع جاذبه، سرگرمی برای میلیون‌ها کاربر در سراسر جهان انباشته شده و این وضعیت سبب جذابیت و تنوع کرده است (کیان‌خواه، ۱۳۹۶: ۷۵).
پنهان ماندن هویت	از ویژگی‌های این فضا امکان پنهان ماندن هویت کاربر است. این امکان موجب حاکمیت‌گریزی کاربران می‌شود (حافظ‌نیا، ۱۳۹۰: ۲۴).
تعاملی بودن	امکان پیوند تمامی گروه‌ها، اجتماعات، سازمان‌ها، دولت‌ها در سطح جهان و شکل‌گیری ائتلاف‌ها و همکاری‌ها (حافظ‌نیا، ۱۳۹۰: ۴).
پیچیدگی	ماهیت سیال فضای سایبری به دلیل معماری فنی و درهم‌تنیدگی ابعاد مختلف آن از حیث مدیریتی، فنی، محتوایی و امنیتی این فضا، نیازمند الگوهای متناسب با پیچیدگی این فضا است.

۳. نظریات مقررات‌گذاری در فضای سایبر

نظریه‌ها ارکان اساسی علوم را تشکیل می‌دهند، زیرا تمام تفسیرها و تحلیل‌های ما از پدیده‌های طبیعی و اجتماعی در قالب نظریه‌ها صورت می‌گیرد. انسان بدون ذهن مسلح به نظریه، قادر به درک علمی از جهان پیرامون خود نخواهد بود. نظریه به داده‌ها و مشاهدات هر فرد نظم، ترتیب و میدان دید می‌دهد (مهدی‌زاده، ۱۳۹۳: ۱۱).

پرداختن به نظریه‌های مرتبط با موضوع و مسئله تحقیق ابعاد و عناصر مهم را برای محقق ترسیم می‌کند. هدف نظریه، تشریح و کمک به درک و تفسیر پدیده‌هاست تا نشان دهد که چرا چنین پدیده‌هایی به شیوه‌هایی خاص اتفاق می‌افتد. بنابراین بررسی نظریه‌های فضای سایبر برای درک و فهم این پدیده پیچیده مهم و ضروری است. هدف نهایی تحلیل و ارزیابی نظریات تنظیم‌گری در فضای سایبر این است که بفهمیم شیوه مقررات‌گذاری صحیح در این فضا باید چگونه باشد و آبشخور هر نظریه و الگو در کدام پارادایم حاکم بر فضای سایبر نهفته است.

فارغ از نظریاتی که در مورد رسانه‌ها مطرح است، جان پری بارلو اولین نظریه‌پرداز در فضای سایبر، نظریه خود را در حمایت از آزادی سایبری (لیبرالیسم سایبری) ارائه کرد. بارلو در سال ۱۹۹۶ «بیانیه استقلال فضای سایبر» را منتشر و بیان کرد، مقررات‌گذاری ابزار حکمرانی دولت‌هاست، اما این فرایند بر اساس مرزهای فیزیکی تعریف شده است و با توجه به ویژگی‌های ذاتی فضای سایبر مقررات دولتی در فضای سایبر مؤثر نیست (Barlow, 1996: 11).

نظریه بارلو چند سال بعد مورد توجه دو استاد حقوق، دیوید جانسون^۱ و دیوید پست^۲ قرار گرفت. آنها نیز همانند بارلو معتقد به استقلال فضای سایبر از سیطره دولت‌ها هستند و از طرفداران لیبرالیسم سایبری به‌شمار می‌روند. البته مواضع آنها کمی فراتر از نظرات جان پری بارلو مطرح شد (Johnson & Post, 1996: 9). پورتر^۳ و وندر کلاس^۴ نیز معتقدند که اساساً فناوری‌ها ایستایی ندارند و از پویایی و پیچیدگی منحصر به فردی برخوردارند. این ویژگی فناوری‌ها به‌ویژه فناوری‌های ارتباطات و اطلاعات موجب شده آنها مقررات‌گذاری و تنظیم‌گری فضای سایبر را بی‌معنی و بدون فایده تصور کنند و مداخلات نظارتی را بلاوجه بدانند (Porter & Linde, 1995: 97-115).

اما این نظریه با مخالفت جدی جامعه حقوقی روبه‌رو شد. عده زیادی از حقوقدانان معتقدند فضای سایبر هم مانند جهان واقعی نیازمند مقررات‌گذاری است. البته اختلافی بین آنها وجود دارد که آیا فضای سایبر این پتانسیل را دارد که به‌عنوان یک حوزه حقوقی مستقل بررسی شود یا خیر. این دیدگاه از سوی فرانک ایستربورک^۵ تحت عنوان "فضای سایبر و حقوق اسب" در سمپوزیومی درباره حقوق سایبر در دانشگاه شیکاگو مطرح شد. او معتقد بود حقوقدان‌ها صلاحیت ندارند به حوزه‌هایی که در آن تخصص

-
1. David Johnson
 2. David Post
 3. Porter
 4. Van der Claas
 5. Frank H. Easterbrook

ندارند، ورود پیدا کنند.^۱ به‌طور مثال آیا لازم است حقوقدانان درباره مسائل مرتبط با اسب، قانون بنویسند؟ (Easterbrook, 1996: 207). در دهه ۱۹۹۰ میلادی، «حقوق سایبر» هنوز در مرحله ابتدایی شکل‌گیری خود بود. در این زمان مسائل حقوقی متعددی مطرح شد که دادگاه‌ها و محاکم دادگستری برای آنها پاسخ قانع‌کننده‌ای نداشتند. برای مثال در مورد مسئولیت در قبال محتوای آنلاین افتراآمیز و یا در مورد مسائل مربوط به تعارض قوانین و صلاحیت دادگاه‌ها. نظر ایستبروک بر این بود که برای معتقدان به سایبرلیبرالیسم حل این دست مسائل باید «اصول کلی حقوقی» مراجعه کرد. مفروض وی این بود که قوانین و مقررات حاکم بر فضای سایبر از نوع «قانون ۱،۰» خواهد بود، اما به‌سرعت مشخص شد که این نوع قوانین صرفاً در «زیست‌بوم طبیعی» کاربرد دارد و قوانین مربوطه حوزه سایبر باید از نوع «قانون ۲،۰» و یا «قانون ۳،۰» باشند و کاربست «قانون ۱،۰» در عصر فناوری‌های پیچیده و محیط سایبر اصلاً مناسب نیست (Easterbrook, 1996: 210).

در واکنش به نظریه ایستبروک، در سال ۱۹۹۶ پروفیسور لونس لسیگ^۲ نشان داد که «حقوق سایبر» می‌تواند به‌عنوان یکی از ابزارها در کنار معماری فناوری و اقتصاد دیجیتال، به چالش‌های تنظیم‌گری فضای سایبر پاسخ دهد (Lessig, 1999: 15). در سال‌های اخیر نظریه این حقوقدان، مورد پذیرش بیشتر اندیشمندان، جوامع حقوقی و نهادهای بین‌المللی و واقع شده است.

در سال ۲۰۰۰ یوچای بنکلر^۳ «نظریه معماری لایه‌ای فضای سایبر» را مطرح کرد و در سال ۲۰۰۲، میل وود هارگریو^۴ هشت عامل را برای مدیریت و کنترل فضای سایبر معرفی کرد. اندرو موری^۵ نیز در سال ۲۰۰۷ نظریه «کنترل شبکه‌ای» را معرفی کرد. پس از او، وینگ فیلد و انیکین تیک^۶ در سال ۲۰۰۹ با رویکرد امنیتی به مقررات‌گذاری فضای سایبر توجه کردند. سپس جک دی لیپتون^۷ در سال ۲۰۱۰ نظریه تنظیم‌گری لورنس لسیگ را تکمیل و در نظریه خود به نقش آموزش و کمک دولت به بخش خصوصی تأکید ورزیده است. همان‌گونه که ملاحظه شد، هریک از این نظریه‌ها به ارائه مدل‌ها و الگوهایی منجر شده که کشورها برای مدیریت و کنترل محیط پیچیده فضای سایبر ملی و تعاملات بین‌المللی از آن استفاده کرده‌اند (Tan & Ang, 2023: 149).

۱. تمثیل «حقوق اسب» ناظر بر این است که هر حوزه جدید، لزوماً نیاز به مقررگذاری جدید و ایجاد حوزه مطالعاتی مستقل ندارد.

2. Lawrence Lessig

3. Yochai Benkler

4. Millwood-hargrave

5. Andrew Marray

6. Eneken Tikk

7. Jacqueline D. Lipton

۴. تنظیم مقررات در محیط‌های پیچیده

الگوی تنظیم‌گری در محیط‌های پیچیده، روش‌های نظارتی و کنترلی مدرن را مطالبه می‌کند. در این محیط‌ها دیگر عنصر قانون به تنهایی نمی‌تواند محیط پیچیده را کنترل و نظارت و تنظیم کند. به عبارتی نظارت و تنظیم‌گری از یک ابزار به یک جریان و فرایند عملیاتی تبدیل شده است و عوامل تغییردهنده محیط مانند فناوری، اقتصاد، سیاست، محیط زیست، هنجارها و غیره در نظارت و تنظیم‌گری تأثیرگذارند (Murray, 2010: 38).

در بررسی عوامل محیطی نمی‌توان دقیقاً مشخص کرد هر کدام از عوامل و شرایط چقدر در تنظیم محیط تأثیر دارند. آیا این تأثیر در زمان‌های مختلف یکسان است یا با گذشت زمان کم یا زیاد می‌شود؟ و در شرایط مختلف این عوامل چگونه شکل می‌گیرند؟ آنچه مسلم است این عوامل ورودی‌های نظام تنظیم‌گری و مقررات‌گذاری است، پس باید این عوامل متنوع را که کل رفتارهای سیستم را در برمی‌گیرد، به‌نوعی مدیریت و کنترل کرد که هر رفتار با تعداد کمتری از عوامل درگیر باشد. در نتیجه نیاز به تنظیم فضای سایبر موجب شد که نظریه‌پردازان الگوها و مدل‌های مختلف تنظیم‌گری فضای سایبر را تهیه و ارائه کنند. کارآمدی این الگوها به نوع و سطح نیازمندی‌ها و دیدگاه‌های ارائه‌کنندگان آنها وابسته است.

۵. مدل‌های تنظیم‌گری فضای سایبر

۵.۱. قانون و هنجارها به مثابه سیستمی برای تنظیم‌گری

نگرش به قانون به‌عنوان یک نظام اجباری برای نظارت بر رفتارها بازتابی از فلسفه آستین است (Austin, 1869: 11). این نگرش دال بر آن است که اگر ما آزادی انتخاب داشتیم، رفتارمان از قانون متفاوت بود و این ترس از مجازات‌های قانونی است که ما را به پیروی از قانون ترغیب می‌کند. قانون به‌عنوان یک سیستم تنظیم‌گر باید عمده‌تاً مانند یک بازدارنده و جلوگیری‌کننده به‌کار رود. ولی تصور قانون به‌عنوان یک عامل بازدارنده ممکن است کارایی اندکی داشته باشد یا کلاً فاقد آن باشد. در عوض انسان‌ها زندگی خود را وفق هنجارهای اجتماعی تنظیم می‌کنند. از این‌رو هنجارها باید بخشی از قانون باشد و محتوای قانون نیز باید با این هنجارها هماهنگ باشد (Darley, 2000: 28 & Tyler).

«هارت» در مفهوم قانون، معتقد است که درک ما از قانون باید همانند گروهی کوچک از مقررات اجتماعی باشد که به‌وسیله آنها اعضای یک جامعه زندگی خود را با شناسایی این مقررات به‌وسیله قواعد ثانویه درباره منشأ و سرچشمه این مقررات و همچنین صلاحیت وضع آنها توسط وضع‌کنندگان تنظیم می‌کنند (Hart, 1994: 96). بیشترین قواعد حقوقی تسهیل‌کننده‌اند، تا دستوردهنده. شمار اندکی از این

قواعد حقوقی دستوری هنجارهای اجتماعی را شامل می‌شوند. برای مثال قوانین رانندگی عمدتاً در مورد پرداخت غرامت به قربانیان تصادف ناشی از تخلف رانندگان است، تا یک نوع هنجارهای اجتماعی. بیشتر این نوع قوانین شکل دستوری و اجباری که توسط مجازات پشتیبانی شوند، به خود نمی‌گیرد (Raz, 2009: 169-172). وقتی چنین نگرشی به قانون که قصد کنترل، نظارت و تنظیم رفتار را دارد داشته باشیم، این ایده پدید می‌آید که علاوه بر عنصر قانونگذاری، بر هنجارهای اجتماعی که بازتابی از چگونگی رفتار مردم است تمرکز داشت. این هنجارها می‌توانند قالب قانون را به خود گیرند و به همان اندازه وزن قانون، محیط را کنترل کنند.

پویایی و پیچیدگی محیط فضای مجازی ایجاب می‌کند نظام مقررات‌گذاری آن ضمن برخورداری از انعطاف لازم، مقررات آن به حوزه‌های مختلف تفکیک و اولویت‌بندی شود، چراکه تغییرات سریع و استثنایی محیط سایبری موجب می‌شود معیارهای این نظام نیز تغییر یابد. بر اساس مدل «کالیج و پرشین»^۱ می‌توان چارچوب مقررات فضای سایبری را به چهار حوزه تقسیم کرد:

۱. مقررات مربوط به تفکیک اطلاعات حساس و حقوق نام دامنه،

۲. مقررات مربوط به حوزه امنیتی،

۳. مقررات مربوط به حوزه حریم خصوصی،

۴. مقررات مربوط به مسئولیت‌پذیری و پاسخگویی کنشگران.

تفکیک اطلاعات حساس و شخصی محوری‌ترین لایه در اولویت‌بندی نظام مقررات‌گذاری است. مقررات امنیتی ارتباط وثیقی با معیارهای اطلاعات حساس و شخصی افراد دارد. حریم خصوصی نیز شامل مقرراتی است که با معیارهای امانتداری و کیفیت و مسئولیت‌پذیری سروکار دارد. مقررات مربوط به پاسخگویی کنشگران نیز مستقیماً به نظام مسئولیت در فضای مجازی مرتبط است. کالیج و پرشین در تقسیم‌بندی مقررات به حوزه‌های خاص، انواع اطلاعات را به چهار گروه تقسیم می‌کنند (اطلاعات طبقه‌بندی‌شده، اطلاعات طبقه‌بندی‌نشده، داده‌های شخصی و مالکیت معنوی). آنها جرائم سایبری و زیرساخت‌های حیاتی اطلاعاتی و شنود را در حوزه مقررات امنیتی قرار می‌دهند. آنها در لایه سوم حریم خصوصی را مشمول مقرراتی می‌دانند که مربوط به ارائه‌کنندگان خدمات اینترنتی و اطلاعات کاربران نهایی می‌شود و در لایه چهارم پاسخگویی کنشگران فضای مجازی را که با معیارهای «مراقبت مقتضی»، «ایجاد مراکز هشدار اولیه» و «حمایت مناسب» طبقه‌بندی کرده‌اند (Klaić & Perešin, 2016: 37-55).



شکل ۱. حوزه های مقررات‌گذاری فضای سایبر

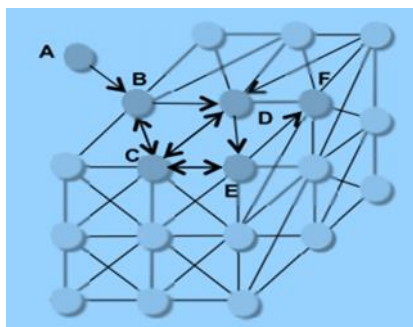
پاسخگویی به این همه تغییرات در محیط سایبری، چارچوب قانونی و هنجاری نمی‌تواند به‌تنهایی حمایت کافی از صاحبان داده‌ها و امنیت زیرساخت اطلاعاتی فضای مجازی را تأمین کند. برای رفع این نقیصه باید از فناوری‌های سایبری برای تنظیم‌گری و ارائه خدمات بهتر و صیانت از زیرساخت‌های حیاتی فضای مجازی استفاده کرد.

۲.۵. فناوری به‌عنوان سیستمی برای تنظیم‌گری

مقررات‌گذاری و تنظیم‌گری فرایندی از ارتباط میان شخص و جامعه است. گاهی تنظیم‌گرها با به‌کار بستن استانداردهای فنی و معماری شبکه به‌طور غیرمستقیم سعی در تغییر بافتار جامعه از طریق تغییر هنجارها یا عرف‌ها دارند که این مکانیزم خود را در قامت قانون ((کد)) نشان می‌دهد (Ashwin, 2022: 9)، اما با توسعه جوامع بشری و شبکه‌ای شدن آنها، دیگر جامعه از این مقررات سنتی و رسمی پشتیبانی نمی‌کند و آن را کافی نمی‌داند. در نظریه جامعه‌گرایی شبکه، اختیار تصمیم‌گیری درباره محیط قابل تنظیم تنها به یک تنظیم‌گر (رگلاتور) واگذار نمی‌شود، بلکه عواملی متعدد دیگری در آن دخیل‌اند.

رویکردی که امروزه به کار می‌رود، شناسایی و ارزیابی «روش‌های تنظیم‌گری ماکرو» است که ممکن است توسط تنظیم‌گران برای کنترل الگوهای رفتاری در سیستم‌های پیچیده استفاده شود. سیستم‌های پیچیده مدام با محیط در حال تعامل هستند و چنین تعاملی، به تکامل مداوم منجر می‌شود. در حال حاضر با فضای سایبر به‌عنوان یک محیط پیچیده روبه‌رو هستیم. در این محیط پیچیده، دیگر روش‌های سنتی تنظیم‌گری کارآمد نیستند.

«اندرو موری» با به‌کارگیری «نظریه شبکه‌ای و سیستم‌ها» در تنظیم فضای سایبری که آن را «اجتماع‌گرایی شبکه‌ای»^۱ می‌خواند، مشخص می‌کند که کاربر محیط‌های پیچیده و شبکه‌ای (مانند فضای مجازی) تنها یک دریافت‌کننده منفعل دستورهای تنظیم‌گر (رگلاتور) نیست. بلکه در عوض نقاط ارتباطی به‌صورت شبکه‌ای بین رگلاتورها، کاربران و سایر کنشگران فضای مجازی وجود دارد که به‌عنوان الگوی مقررات‌گذاری در محیط پیچیده معروف شده است. شکل زیر ماتریس تنظیم‌گران فضای سایبر را نشان می‌دهد (Murray, 2010: 68-70).



شکل ۲.

- A یک تنظیم‌گر خارجی است (برای مثال دولت ایالات متحده).
- B سازمان ملل است که از طریق ارکان خود عمل می‌کند.
- C به صاحبان نام دامنه اشاره دارد (سهامداران ICANN).
- D اتحادیه اروپا (EU) و
- E اجلاس جهانی در مورد جامعه اطلاعاتی (WSIS) نیز به‌عنوان دارند
- F انجمن حاکمیت اینترنت (IGF) که یکی دیگر از نهادهای مهم تنظیم‌گری است.

این ماتریس نشان می‌دهد که پیچیدگی فضای سایبر در حال افزایش است و در نتیجه، مقررات‌گذاران و تنظیم‌گرها باید مداخله‌گران و بازیگران بیشتری را مدنظر قرار دهند و نظرها و دیدگاه‌های آنها را اعمال کنند. بر اساس این الگو در محیط‌های پیچیده مانند فضای سایبر که تغییرات خطی نیستند، باید از «قانون اشبی» یا همان «قانون پیچیدگی» استفاده کرد؛ به این معنا که هرچه محیط پیچیده‌تر باشد، واکنش‌ها هم باید به همان اندازه از پیچیدگی برخوردار باشد. مطابق با نظر روس اشبی^۱ در کتاب *مقدمه‌ای بر سایبرتیک* که به «قانون اشبی» معروف است در تنظیم مقررات فعال «تنها تنوع می‌تواند تنوع را از بین ببرد» (Ashby, 1966: 68-70)؛ بدین معنی که هنگامی که در ایجاد یک پدیده عوامل تأثیرگذار متعدد باشند، عوامل خنثی‌کننده نیز باید به اندازه عوامل تأثیرگذار از نظر تعداد و میزان تأثیر متنوع باشند. پس اگر بخواهیم فضای سایبر تنظیم شود، باید تنوع را به حداکثر رساند تا برای مواجهه با هر شرایطی آماده شد. ارائه‌دهندگان الگوهای تنظیم‌گری باید تلاش کنند اشتراکات اجزای مختلف را شناسایی کرده و با استفاده از نظریه سیستم‌ها، الگوهای تنظیم‌گری ارائه کنند (Murray, 2006: 247).

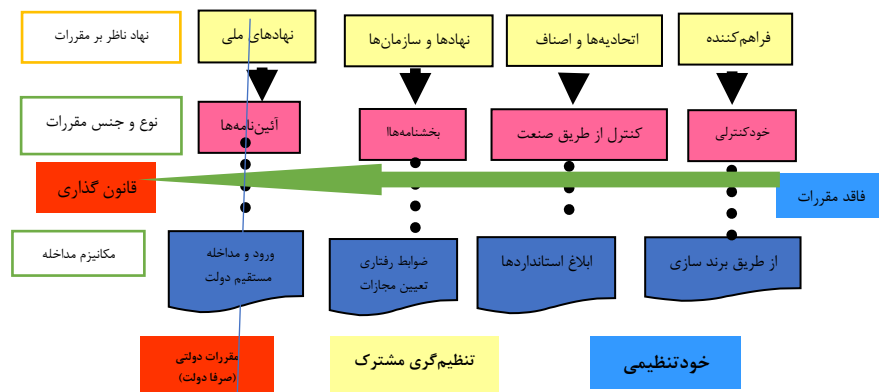
روبرت بادوین و مارتین کیو^۲ در سال ۱۹۹۹ نظریه هشت‌عاملی تنظیم فضای سایبر را ارائه کردند. این عوامل عبارت‌اند از: ۱. دستور و کنترل، ۲. مقررات خودتنظیمی، ۳. اعطای مشوق‌ها، ۴. به کنترل در آوردن بازار، ۵. آشکارسازی، ۶. اقدام مستقیم، ۷. حقوق و قوانین مسئولیت‌ها، ۸. جبران سازی عمومی. آن‌ها این هشت عامل را جهت استفاده از ظرفیت‌های دولت برای تأثیرگذاری بر فعالیت‌های فضای سایبر تعریف می‌کنند. بنابراین دولت می‌تواند (الف) از حق قانونی و احکام قانونی برای پیگیری اهداف سیاسی خود استفاده کند، (ب) توانمندی مالی را از طریق قراردادهای وام‌ها، کمک‌های مالی، یارانه‌ها یا سایر مشوق‌ها برای تأثیرگذاری بر رفتارها توسعه دهد، (ج) بازار را از طریق هدایت نیروهای رقابتی به اهداف خاص کنترل کند، (د) استقرار اطلاعات را به‌طور راهبردی انجام دهد، یا (ه) به‌طور مستقیم با اقدام فیزیکی عمل کند، (خ) از ایجاد مشوق‌ها حفاظت کند. بدین ترتیب بالدوین و کیو بررسی می‌کنند که چگونه دولت می‌تواند با استفاده از ترکیبی از مشوق‌ها و کنترل‌ها برای دستیابی به نتایج موردنظر، بر نتایج هر وضعیت تأثیر بگذارد (Baldwin & Cave, 1999: 11).

میل وود هارگریو در مدل خود از یک طیف استفاده می‌کند که یک سوی آن «خودتنظیمی» و سوی دیگر آن «تنظیم دولتی» است. وی نحوه مقررات‌گذاری در طول این طیف را به چند بخش تقسیم می‌کند. وی از یک سو به کدهای تنظیم‌کننده (کدهای یکجانبه، کدهای صنعتی، کدهای تصویب‌شده و کدهای مورد تأیید قوانین) و از سوی دیگر به تنظیم‌گرها و رگلاتورها (شامل ارائه‌دهندگان خدمات

1. Ross Ashby

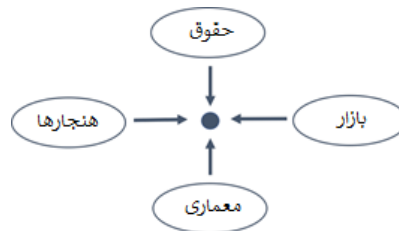
2. Robert Baldwin and Martin Cave

اینترنتی، مؤسسات صنعتی، اپراتورها، نهادهای مستقل دولتی) توجه دارد. او همچنین سطوح مقررات‌گذاری را به سه سطح (خودتنظیمی، تنظیم‌گری مشترک و تنظیم‌گری دولتی) تقسیم و واکنش حقوقی به نقض مقررات را در هر سطح پیش‌بینی می‌کند (Hargrave, 2007: 60-61).



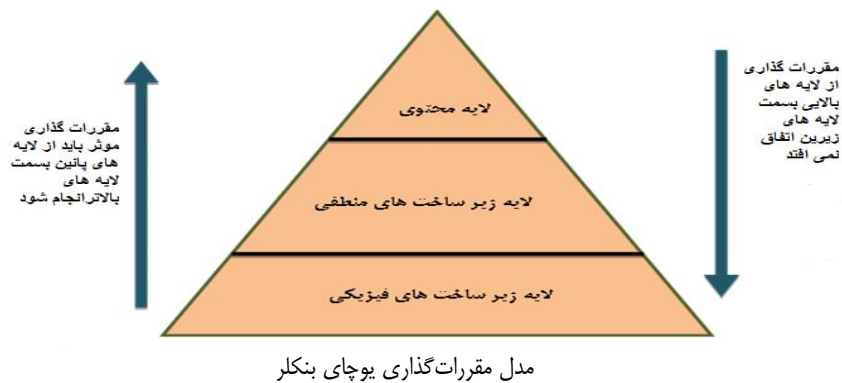
شکل ۳. مدل تنظیم‌گری چندسطحی هوشمند (هارگریو)

لورنس لسیگ در کتاب *کد و قوانین* دیگر در فضای سایبر چهار روش جهت تنظیم‌گری فضای مجازی معرفی می‌کند، که عبارت‌اند از: حقوق، بازار، معماری و هنجارها. اگرچه این عوامل به صورت منفرد یا جمعی می‌توانند در تنظیم‌گری و کنترل فضای سایبر مؤثر باشد، اما او پیشنهاد می‌کند هر چهار عامل در تعامل باهم یک تنظیم‌گری واقعی‌تری را ارائه می‌کنند که نتیجهٔ بهتری در پی خواهد داشت و قابلیت تنظیم‌گری شبکه‌ای افزایش پیدا خواهد کرد. اما لزوماً این به معنی تنظیم‌گری کامل نیست. لسیگ به خوبی «کد و معماری شبکه» را به عنوان تنظیم‌کننده مطرح کرده است. معماری و کد این پتانسیل را دارند که سایر عناصر تنظیم‌کننده را تحت کنترل بگیرند (Lessig, 2000: 98).



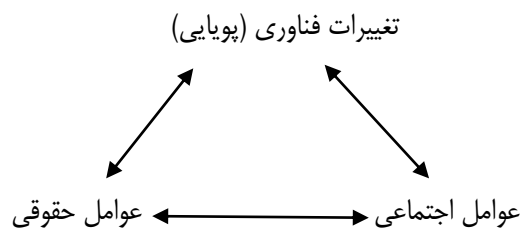
لسیگ استدلال کرد که فضای مجازی اساساً توسط «کد» (معماری و برنامه‌نویسی رایانه‌ای سیستم) تنظیم می‌شود و معتقد است که اینترنت بر اساس پروتکل‌ها ساخته شده است و فضای سایبر صرفاً محصول معماری است. او استدلال می‌کند که اینترنت قابل تنظیم‌ترین فضایی است که ما می‌شناسیم، زیرا از طریق معماری آن می‌توان مشخص کرد، چه کسی، در کجا، چه کار می‌کند. وقتی فرد به اینترنت متصل است، می‌توان همه تعاملاتش را کنترل و شناسایی کرد (Loader, 2010: 18). لسیگ معتقد است معماری می‌تواند حتی تنظیم‌کننده رفتار انسان در محیط باشد، مانند طراحی یک زندان که در آن نگهبانان می‌توانند همه زندانیان را تحت نظر بگیرند (Murray & Scott, 2002: 491-516)

پس از لسیگ، **یوچای بنکлер**^۱ با الهام از الگوی استاندارد لایه‌بندی شبکه‌ها و با استفاده از مدل چهار لایه «تیم برنرلی»^۲، فضای سایبر را به سه لایه (زیرساخت فیزیکی، زیرساخت منطقی و محتوا) تقسیم کرد. او معتقد است تنظیم‌گری و مقررات‌گذاری در فضای سایبری باید به صورت عمودی و از لایه‌های پایین (زیرساخت) به سمت لایه‌های بالایی صورت پذیرد و در صورتی که این فرایند از لایه‌های بالایی به سمت لایه زیرین انجام شود، مقررات مؤثر واقع نخواهند شد چراکه لایه‌های پایینی همواره از لایه‌های بالایی تأثیر می‌پذیرند (Benkler, 2000: 561-579). بنکлер در مدل خود تنظیم‌گری را وظیفه لایه زیرساخت می‌داند. این به معنای این است که تولیدکنندگان محتوی تحت تنظیم‌گری لایه منطقی هستند و هیچ کنترلی روی محصولاتشان ندارند و این موضوع موجب تعارض منافع می‌شود، حتی در زمینه مالکیت فکری و معنوی نمی‌توانند تنظیم‌گری کنند. با توجه به اینکه توافقات در حقوق اجتماعی و ارتباطات انسانی، به‌طور مؤثر شکل می‌گیرد، نمی‌توان آن را محدود به یک لایه کرد و در مدل بنکлер این موضوع نادیده گرفته شده است.



1. Benkler.
2. Tim Berners-Lee

کالین اسکات و اندرو موری در سال ۲۰۰۲ با توسعه «مدل لورنس لسیگ»، روش تنظیم‌گری جدیدی را پیشنهاد می‌کنند که عبارت‌اند از کنترل سلسله‌مراتبی، کنترل مبتنی بر جامعه، کنترل مبتنی بر رقابت، و کنترل مبتنی بر طراحی. آنها این روش‌ها را در ترکیب با سه حالت تنظیم استاندارد، جمع‌آوری و پایش اطلاعات، و اصلاح رفتار، برای کنترل حوزه رسانه فضای مجازی پیشنهاد کردند و معتقدند که مدل پیشنهادی آنها پایگاه غنی‌تری برای درک مکانیسم کنترل تنوع، ایجاد می‌کند. مدل سه شاخگی (SLT) که اندرو موری در کتاب *مقررات‌گذاری فضای سایبر* در ۲۰۰۶ معرفی کرده است، بر اساس سه اصل ((جامعه، حقوق و فناوری)) استوار است. او در این کتاب تصریح می‌کند ماهیت مدل‌های تنظیم‌گری محیطی منبع‌گرا هستند و بخش‌های زیادی از این منابع صرف تنظیم‌گری و مقررات‌گذاری می‌شود. اگرچه فضای حقیقی یکی اینرسی در برابر تغییر و تنظیم دارد و در برابر تنظیم‌گری مقاومت می‌کند، اما فضای مجازی چیزی جز سیم و شبکه‌های کابل و روترها نیست که همگی در لایه فیزیکی قرار دارند و وقتی به لایه محتوا می‌رسیم دیگر مقاومتی در برابر تغییر نیست و راحت‌تر می‌توان با هنجارهای اجتماعی و حقوقی، این لایه را تنظیم کرد. با توجه به توضیحات لسیگ فناوری نیز می‌تواند به‌عنوان تنظیم‌گر وارد شود. در این مورد موری با لسیگ اتفاق نظر دارد؛ لیکن موری تأکید بر نقش عوامل دیگری در تنظیم‌گری دارد و همچنین او اعتقاد به تأثیر دوطرفه عوامل تنظیم‌کننده بر هم دارد، درحالی‌که مدلی که لسیگ ارائه کرده است، تأثیر یکطرفه معماری و کد است (Murray, 2006: 247). موری معتقد است تنظیم‌گری پلتفرم‌های مبتنی بر فناوری را از طریق نظریه (اجتماع-فناوری-حقوق) (STL) اثربخش خواهد بود که در این نظریه عوامل فنی، اجتماعی و حقوقی تأثیرات متقابل دارند:

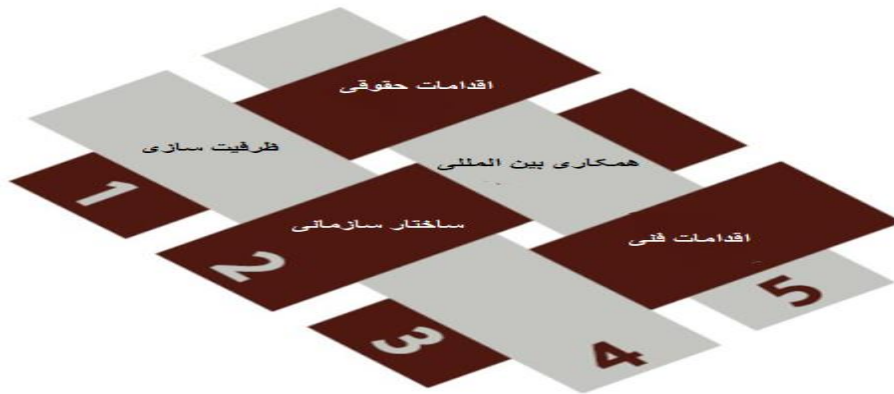


۵.۳. امنیت و دفاع به‌عنوان هدفی برای مقررات‌گذاری

فضای مجازی همه ارکان یک جامعه و دولت را در برمی‌گیرد و همه مطالبات جامعه مدرن به‌طور مستقیم یا غیرمستقیم به فضای مجازی و محیط اطلاعاتی متکی است. این وابستگی به کاهش ضریب امنیتی و

بروز برخی محدودیت‌ها در امر تنظیم‌گری و مقررات‌گذاری منجر می‌شود و زمینه بروز تهدیدها و مخاطرات امنیتی را برای کاربران و دولت‌ها ایجاد می‌کند. برای پیشگیری و مقابله با این تهدیدات، الگوها و مدل‌هایی برای برقراری امنیت سایبری و تدوین چارچوب همکاری چندجانبه بین‌المللی ارائه شد.

اولین چارچوب برای تأمین امنیت سایبری جامعه اطلاعاتی جهانی، الگویی است که توسط «اتحادیه بین‌المللی ارتباطات راه دور» (ITU) تحت عنوان «دستور کار جهانی امنیت سایبری^۱» در سال ۲۰۱۰ ارائه شد. این الگو امنیت فضای سایبر را بر پایه پنج رکن مهم (قانونی، فناوری، ساختار سازمانی، ظرفیت‌سازی و همکاری‌های بین‌المللی) قرار داده است. البته هر کدام از این ارکان پنج‌گانه دارای مؤلفه‌ها و شاخص‌هایی است که در مجموع برای ارزیابی و تحلیل وضعیت امنیت محیط سایبر کشورها استفاده می‌شود. ارکان پنج‌گانه چارچوب معماری فضای سایبری (ITU) را می‌توان در شکل زیر ارائه کرد:



رکن ۱- اقدامات قانونی

این رکن به دنبال توسعه راهبردهایی برای توسعه قوانین مقابله با جرائم سایبری و روش‌های قابل اجرا در سطح جهانی است.

رکن ۲- اقدامات فنی و رویه‌ای

این رکن بر اقداماتی برای کاهش آسیب‌پذیری در محصولات نرم‌افزاری و سخت‌افزاری تمرکز دارد. در هدف ستون ایجاد طرح‌های معماری، پروتکل‌های فنی و استانداردهای معتبر جهانی است.

رکن ۳- ساختارهای سازمانی

هدف این رکن ایجاد ساختارها و راهبردهای سازمانی برای کمک به پیشگیری و شناسایی و مقابله با حملات علیه زیرساخت‌های اطلاعاتی حیاتی و طراحی مکانیزم پاسخگویی به تهدیدات سایبری است.

رکن ۴- ظرفیت‌سازی

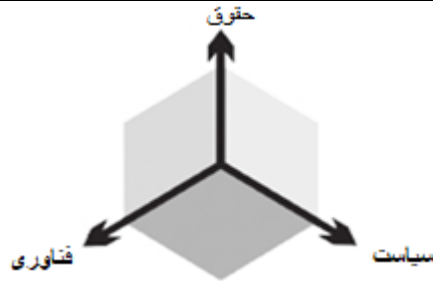
این رکن به دنبال توسعه راهبردهایی برای ارتقای دانش تخصصی و تقویت امنیت سایبری از طریق افزایش سواد رسانه‌ای و تدوین سیاست ملی است.

رکن ۵- همکاری بین‌المللی

هدف کلی این رکن توسعه مشارکت و همکاری بین‌المللی در تدوین فرایندهای همسو و سازگار برای توسعه فناوری‌های اطلاعات و ارتباطات و ممانعت از آسیب به زیرساخت‌های حیاتی دولت‌ها است (Wamala, 2011: 19).

روبرت بادوین و مارتین کیو در سال ۱۹۹۹ در کتاب *درک مقررات، الگویی مرکب از هشت عامل برای تنظیم فضای سایبر معرفی کرده‌اند*. این عوامل عبارت‌اند از: «هرماندهی و کنترل، سیاست خودتنظیمی، مشوق‌ها، نیروی بازار، افشای فعالیت‌ها، اقدام مستقیم، بهره‌گیری از قوانین حقوقی و ایجاد تعهدات قانونی، جبران خسارت و بیمه تأمین اجتماعی» (Baldwin & Cave, 1999: 1-63). آنها معتقدند که این راهبردهایی است که دولت‌ها می‌توانند برای کنترل و مدیریت فعالیت‌های مختلف در فضای مجازی به کار گیرند.

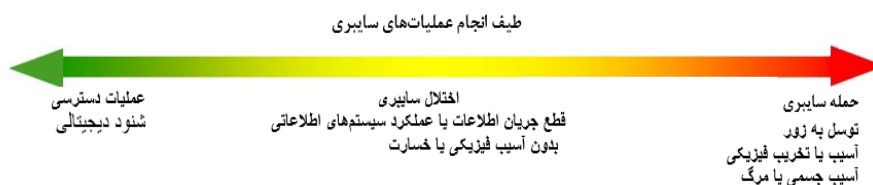
وینگ فیلد و انیکین تیک در سال ۲۰۰۹ با معرفی مکعبی که بر سه محور (سیاست، فناوری، قانون) قرار می‌گیرد، معتقدند که می‌توان محیط تنظیم‌گری را تقسیم‌بندی کرد. آنان می‌گویند هر محور می‌تواند تقسیم‌بندی جداگانه‌ای داشته باشد. این محیط به شش مؤلفه (دیپلماسی، اطلاعات، نظامی، سیاسی، حقوقی و اقتصادی) تقسیم می‌شود و بر روی هر مؤلفه می‌توان تنظیم‌گری خاصی را وضع و راهبرد ملی خود را تعیین کرد. ویژگی دیدگاه وینگ فیلد این است که عنصر سیاست را در نظام تنظیم‌گری مؤثر دانسته است. وینگ فیلد معتقد است فضای سایبر را می‌توان با یک مدل منشوری شکل که شامل سه محور (**مکعب، هرم و صفحه نمایش**) می‌شود، کنترل و مدیریت کرد تا امنیت آن تأمین شود. محور **مکعب**: مشتمل بر سه بخش قانون، فناوری و سیاست است. **هرم**: پاسخ حقوقی به مسائل مخرب امنیت سایبری است؛ و **صفحه نمایش**: محیط دیجیتالی که مکانی برای ثبت وضعیت‌ها، تهدیدها و گزینه‌ها، احتمالات و شکاف اطلاعات است (Wingfield & Tikk, 2010: 16-22).



جک دی لیپتون نیز معتقد است، مقررات سنتی نمی‌تواند به‌طور مؤثر فضای مجازی را تنظیم کند و باید عوامل و عناصر جدیدی به قوانین و مقررات اضافه شود. او عوامل آموزش و تربیت عمومی، هنجارها، نیروی بازار و رقابت، معماری سیستم، کمک مؤسسات غیردولتی را بر تنظیم‌گری فضای مجازی مؤثر می‌داند (Lipton, 2014: 47).

انکین تیک در تز دکتری تحت عنوان «**رویکرد جامع به امنیت سایبری**» سال ۲۰۱۱، عوامل مؤثر در عملیات سایبری را معرفی کرده که عبارت‌اند از: دیپلماسی، جاسوسی، نظامی، سیاست، قانون، اقتصاد. وی در تحقیقات خود امنیت سایبری را متأثر از چهار حوزه شامل جنگ سایبری، تهدید سایبری، جرم سایبری و جامعه سایبری می‌داند. او نقش ابزارهای حقوقی و فرایندهای قانونی را برای تحقق رویکرد جامع امنیت سایبری و مقابله با حملات و جرائم سایبری ترسیم می‌کند. همچنین او چهار وزارتخانه دفاع، دادگستری، فرهنگ و کشور را در مقررات‌گذاری فضای سایبری دخیل می‌داند. تیک معتقد است تحقق رویکرد جامع به امنیت سایبری می‌تواند این نتایج را رقم بزند: (الف) تقویت امنیت ملی؛ (ب) مقابله مؤثر با جرائم سایبری؛ (ج) جلوگیری از استفاده تروریستی از فضای سایبر جلوگیری؛ (د) پاسخگویی به طیف وسیعی از خطرها و تهدیدات، از جمله نظامی، سیاسی؛ (د) مقامات ذی‌صلاح را قادر می‌سازد تا از طیف وسیعی از اهداف کاربران گرفته تا زیرساخت‌های حیاتی محافظت کنند؛ و (ه) حفاظت از فضای سایبر به‌عنوان محیطی برای آزادی بیان و آزادی تجمعات (Tikk, 2011: 561-579). البته تحقق رویکرد جامع، در گام اول مستلزم رصد و شناسایی تمامی فعالیت‌ها، تهدیدات، مخاطرات و حملات در فضای سایبر است؛ و در گام بعدی باید تمامی قابلیت‌ها و ابزارهای قانونی و حقوقی موجود مورد توجه قرار گیرد و به تناسب هر عملیات سایبری واکنش حقوقی متناظر آن در نظر گرفته شود. برای مثال قبل از اینکه یک عملیات سایبری به مرحله نقض امنیت ملی و یا «آستانه حمله مسلحانه» برسد، می‌توان آن را با مقررات کیفری و مدنی کنترل و نظارت کرد. از نظر تیک، عملیات سایبری بسته به

انگیزه مهاجم، آثار و عوامل، و میزان نقض استانداردهای فنی، نقض قوانین ارتباطات، نقض تعهدات حقوقی، نقض مقررات امنیت ملی یا نقض قواعد حقوق جنگ طبقه‌بندی می‌شود. در واکنش به این طیف از نقض‌ها، شاخه‌های مختلف رشته حقوق (حقوق جامعه اطلاعاتی/ ارتباطات، حقوق جزا، حقوق امنیت ملی و حقوق حاکم بر مواضع مسلحانه) پاسخ متناظر با نوع و سطح عملیات سایبری مخرب را خواهد داد (Tikk, 2011: 561–579). بنابراین عملیات سایبری می‌توانند طیفی از اقدامات را در برگیرند که از سطح دسترسی تا یک حمله سایبری تمام‌عیار را شامل می‌شود:



۶. تجزیه و تحلیل

لیبرالیسم و پاترنالیسم سایبری دو پارادایم مهم در تعیین الگوهای مقررات‌گذاری فضای سایبر هستند. لیبرالیسم سایبری کاملاً مدافع آزادی و بدون قانون بودن فضای سایبری است. سایبرلیبرالیسم‌ها معتقدند فضای سایبر را نباید قانونگذاری کرد. دولت‌ها حق کنترل، نظارت و سیاست‌گذاری بر فضای سایبر را ندارند و مدیریت این فضا در سطح جهان در یک «سپهر افقی چندذی‌نفعی» و بر عهده ذی‌نفعان - یعنی دولت آمریکا به‌عنوان اهداکننده این سرویس به جهانیان - و غول‌های فناوری که خدمات دهندگان این فضا هستند است. در سپهر افقی مفاهیمی چون آزادی، اقتصاد و تجارت بسیار بااهمیت است و نظام حکمرانی در این پارادایم به تحلیل حاکمیت دولت‌ها منجر می‌شود. نتیجه این پارادایم جهانی‌سازی، بروز بحران هویت، تغییر ارزش‌ها، رقابت ناعادلانه، تغییر سبک زندگی و از بین رفتن سنت‌های اجتماعی در سطح جهان است. اما در طرف مقابل، سایبر پاترنالیسم‌ها معتقدند فضای سایبر به‌صورت «سلسله مراتبی» قابل مدیریت است. دولت‌ها حق کنترل، نظارت و سیاست‌گذاری بر فضای سایبر را دارند و مدیریت این فضا در سطح جهان در یک «سپهر عمودی چندجانبه» دولت‌محوری نظیر وضعیت موجود در سازمان ملل متحد و اعمال قدرت تابعان حقوق بین‌الملل در قلمروهای زمینی، دریایی، هوایی و فضایی است. در سپهر عمودی ارزش‌های ملی و مقررات‌گذاری دولتی از اهمیت بسیار

زیادی برخوردار است. نظام حکمرانی در این پارادایم منجر به حفظ ارزش‌های فرهنگی، دینی، قومی و ملی می‌شود. نتیجه تداوم حمایت از سپهر عمودی ضمن استمرار حاکمیت و امنیت ملی می‌شود، لیکن به محدودساز آزادی‌ها و از دست دادن سرمایه‌های اجتماعی منجر می‌شود. پیروان این پارادایم دارای دیدگاهی پدرسالارانه هستند و با قانونگذاری و کنترل فضای سایبری، درصدد حفظ ارزش‌ها و فرهنگ جامعه، امنیت و حکمرانی نظام ملی خود هستند. با توجه به چالش‌های دو پارادایم پیش‌گفته، پارادایم بینابینی و مختلطی به نام (SLTE) شکل گرفت و الگوی کنترل و تنظیم فضای سایبر را مرکب از چهار مؤلفه (اجتماعی - حقوقی - فنی و اقتصادی) می‌داند. این چهار مؤلفه در کنار هم می‌توانند تا حد زیادی پاسخگوی پیچیدگی و آشوبناکی فضای مجازی باشند.

هم طرفداران لیبرالیسم و هم پشتیبانان پاترنالیسم در این موضوع متفق‌القول هستند که «قانون» و «کد» در کنار هم باید برای کنترل و معماری فضای سایبری بکار گرفته شوند. هدف «قانون» این است که چگونه رفتار کردن را به مردم تحمیل کند و کسانی که از آن تخطی کنند با مجازات روبه‌رو شوند. لسیگ معتقد است «کد» نیز همانند «قانون»، یک رگلاتور و تنظیم‌گر فنی است که وظیفه نظارت بر رفتار کاربران را به عهده دارد. در واقع دست نامرئی فضای سایبری در حال ایجاد نوعی معماری است که به فرایند مقررات‌گذاری در این فضا تکامل می‌بخشد (Lessig, 1999: 16-22). فرض بر این است که تنها قوانینی که قانونگذار اعمال آنها را امکان‌پذیر بداند، مردم را وادار به رفتاری خواهد کرد. اگر این فرض درست باشد، قانونگذار (یا سازنده قانون) باید رفتارهای آنلاین مجاز و ممنوع را تعیین کند و باید قانون را طوری وضع کند (یا ساختن قانون را اجباری کرد) تا بتواند رفتار را بر طبق آن الزامی یا اجباری کند (Reed, 2012: 5-7)، اما مقررات‌گذاری باید از لایه‌های زیرساختی شروع شود تا مؤثر باشد و اگر در یک محیط چندین روش تنظیم‌گری را باهم ترکیب کنیم، به رقابت تنظیم‌گری منجر می‌شود و محیط را برای مقررات‌گذاری پیچیده‌تر می‌کند:

توجه به سه عامل «قانون و هنجارهای اجتماعی و معماری فنی» در کنار هم و در ارتباط دوسویه می‌تواند الگوی تنظیم‌گری مناسبی باشد. البته باید به عواملی همچون اقتصاد، آموزش، فرهنگ و سیاست نیز توجه کرد. برای مثال در بعضی از مدل‌ها سیاست را نیز جزء عوامل تأثیرگذار در تنظیم‌گری فضای سایبر دانسته و آن را هم‌وزن دیگر عوامل فرض کرده‌اند. اما این سؤال کماکان بی‌پاسخ مانده که میزان تأثیر عوامل بر محیط سایبر چقدر است؟

بررسی مدل‌های مختلف بیانگر آن است که حقوقدانان بر اساس نگرش خود به فضای مجازی و شناخت عوامل تأثیرگذار در آن، مدل‌های مقررات‌گذاری خود را طراحی کرده‌اند. این مدل‌ها نگرش

لیبرالیستی، پاترنالیستی یا بینابینی به فضای سایبر را نشان می‌دهد. هر کدام از این پارادایم‌ها سعی کرده‌اند مدل جامع‌تری ارائه کنند و کمبودهای مدل‌های قبلی را برطرف کنند. با وجود این، این مدل‌ها برای عواملی که در آینده ممکن است محیط سایبر را متحول سازد، تجویزی نداشتند و تنها به تقسیم‌بندی عواملی که تصور می‌کردند در فضای مجازی مؤثر است پرداختند. بنابراین این مدل‌ها اغلب به صورت استاتیک و ایستا و بدون تفکیک محیط ملی و بین‌المللی طراحی شده‌اند. از این رو چنانچه تعارضی بین عوامل محیط ملی و بین‌المللی رخ دهد سازوکاری برای رفع آن وجود ندارد و اساساً به نقش تنظیم‌کنندگان بین‌المللی توجه نشده است.

۷. چارچوب جامع تنظیم‌گری مطلوب جمهوری اسلامی ایران

با توجه به اینکه کشورهای مختلف اهداف متفاوتی را در فضای سایبر دنبال می‌کنند، ارتباط میان تنظیم‌کنندگان بین‌المللی با رگلاتورهای ملی حائز اهمیت است، چراکه راهبردها و انتظارات و مقتضیات بومی کشورها می‌توانند عوامل تأثیرگذار محیطی را تغییر/حذف و یا اضافه کنند. برای نیل به این مقصود، باید مدل تنظیم‌گری دینامیک با سطح انعطاف‌پذیری بسیار بالا طراحی شود. در این مدل باید تأثیر نظام تنظیم‌گری بین‌المللی بر داخلی و برعکس در نظر گرفته شود، زیرا این دو نظام هم از حیث اهمیت و هم از نظر عوامل محیطی در تعامل با یکدیگرند. برخی الگوها با تمرکز بر نظام خودتنظیمی و هم‌تنظیمی (خودانتظامی و ساماندهی مشترک) تلاش کرده‌اند نقاط ضعف مقررات‌گذاری ملی فضای سایبر را مرتفع کنند. بنابراین به منظور صیانت از حقوق همه ذی‌نفعان فضای سایبر باید علاوه بر تنظیم مقررات در سطح ملی و بین‌المللی، از الگوی خودتنظیمی در سطح فنی نیز استفاده شود. به طور کلی، در الگوی تنظیم‌گری نیز از سه روش بهره گرفته می‌شود:

الف) روش تنظیم‌گری داوطلبانه یا کامل: در این روش خودتنظیمی بدون دخالت دولت انجام می‌شود؛

ب) روش تنظیم‌گری اجباری: در این روش دولت‌ها به طور کاملاً مستقیم حضور دارند؛

ج) روش تنظیم‌گری جزئی اجباری: این روش با حضور محدود دولت‌ها ایجاد می‌شود.

با توجه به ادبیات موجود و با استفاده از مدل‌های ارائه شده، می‌توان «الگوی جامع مقررات‌گذاری فضای سایبری ایران» را مبتنی بر مقتضیات بومی و ارزش‌های ملی طراحی کرد که در این الگو هم لایه‌های فضای سایبر (کاربر، محتوا، خدمات و زیرساخت) و نظامات تنظیم‌گری (اجباری جزئی و اجباری داوطلبانه) و سطوح مقررات‌گذاری (ملی، بین‌المللی و خودانتظامی) و هم نوع

مقررات‌گذاری (دولتی، هم‌تنظیمی و خودتنظیمی) در آن لحاظ شده باشد.

		شیوه‌های تنظیم‌گری				
		داوطلبانه	اجباری جزئی	اجباری		
ساخت‌های فضای مجازی	کاربر	---	---	•	همکاری و تعاون	بین‌المللی
	محتوا	---	•	---		
	خدمات	---	---	---		
	زیرساخت	---	---	•		
	کاربر	---	---	•	قانون‌گذاری	ملی
	محتوا	---	---	•		
	خدمات	---	•	---		
	زیرساخت	---	---	---		
	کاربر	---	---	---	استانداردسازی	خودانتظامی
	محتوا	---	---	---		
	خدمات	---	•	---		
	زیرساخت	•	---	---		
		خودتنظیمی	تنظیم مشترک	دولتی		
		نوع مقررات‌گذاری				

۸. نتیجه

فضای سایبری یک زیست‌بوم و محیط ایستا نیست، بلکه حوزه پویا و در حال تحول است که شاخص‌های آن با هر نوآوری جدید تغییر می‌کند. از این نظر، فضای سایبری شامل سخت‌افزار، کدها و داده‌هاست. علاوه بر این، فضای سایبری همچنین شامل یک «فضای اجتماعی» است، یعنی فضایی که از تعاملات اجتماعی بر اساس ارتباطات و تعاملات بین کاربران ناشی می‌شود. این ابعاد به‌طور مشترک فضای سایبری را به‌عنوان یک فضای واحد تشکیل می‌دهند.

مقررات‌گذاری در فضای سایبر، مفهومی پیچیده و در عین حال امری بسیط است. این عبارت

مجموعه‌ای از فرایندهای تقنینی، کنترلی و اجرایی است که تلاش می‌کند تا دو ساحت متعارض را با هم آشتی دهد و آنها را به تعادل بکشد. این دو ساحت عبارت‌اند از: از یک سو، حقوق و آزادی‌های مشروع بازیگران و ذی‌نفعان فضای سایبر؛ و از سوی دیگر، ارتقای امنیت ملی، حاکمیت و استقلال.

در واقع در فضای سایبر دو پارادایم حقوقی در مقابل هم قرار گرفته‌اند: پارادایم فکری سایبرلیبرالیستی و پارادایم فکری سایبرپاترنالیست. طرفداران پارادایم فکری سایبرلیبرالیسم یا آزادی سایبری تصور می‌کنند که فقدان اثربخشی سیستم‌های کنترلی و ناکارایی قوانین سنتی در فضای سایبر به معنای آزادی محیط آنلاین (برخط) است؛ اما معتقدان به سایبر پاترنالیسم (کسانی که اصرار دارند فضای سایبر را باید به صورت سلسله مراتبی از بالا به پایین کنترل کرد) نشان دادند که می‌توان این فضا را با ابزارهای قانونی در کنار ابزارهای فنی مدیریت کرد؛ هرچند طرفداران این پارادایم اجرای سیستم‌های تنظیم مقررات سنتی را در فضای سایبر بسیار پیچیده و پرهزینه می‌دانند و علت آن را ناشی از عوامل مختلفی همچون میزان نسبی ناشناخته بودن آن، فیزیکی نبودن آن، دیجیتالی بودن محتوا، محیط انعطاف‌پذیر و ماهیت بین‌المللی یا فرامرزی بودن شبکه می‌شمارند.

چالش تنظیم مقررات و شیوه‌های کنترل و پایش فضای سایبر، پیچیدگی و چندوجهی بودن آن را تأیید می‌کند. با توجه به ابعاد فلسفی، اجتماعی، فنی و حقوقی فضای سایبر ذاتاً مقررات‌گذاری و تنظیم‌گری این فضا با مشکلات جدی مواجه است. روند مقررات‌گذاری و تنظیم‌گری فضای سایبر هم‌اکنون به طور جدی از طرف دولت‌ها، حقوقدانان و اندیشمندان و نهادهای بین‌المللی دنبال می‌شود. در این جهت، الگوهای برای تعریف و دسته‌بندی عوامل تأثیرگذار در نظام مقررات‌گذاری و روشن کردن میزان ارتباط عوامل با محیط سایبر ارائه شده است تا از پیچیدگی مسائل بکاهد و ارتباط عوامل را به شکل ساده تبیین کند.

در این مقاله مدل‌های ارائه‌شده برای تنظیم فضای سایبر بررسی شد. نتایج بررسی‌ها نشان می‌دهد که هر کدام از این الگوها مبتنی بر پارادایم حاکم، عوامل تأثیرگذار در فضای سایبر را شناسایی، دسته‌بندی و نظام مقررات‌گذاری خود را برای فضای سایبر جامع معرفی کنند. اما صرف‌نظر از نقاط مثبت هر یک از مدل‌ها، اغلب الگوهای مقررات‌گذاری ارائه شده ایستا هستند و به ساحات فضای سایبر، نوع و سطح تنظیم‌گری توجه نشده است.

در مدل تنظیم‌گری و مقررات‌گذاری پیشنهاد شده برای کشورمان، عوامل تأثیرگذار بر فضای سایبر با یکدیگر تعامل چندسویه دارند. در این مدل با توجه به رویکردهای بین‌المللی تنظیم‌گری ارتباط آن را با تنظیم‌گری فضای سایبری داخلی نشان داده است. به نظر می‌رسد هرچه دولت‌ها به سمت پارادایم

سایبرپاترنالیستی سوق پیدا کنند، امنیت و حاکمیتشان حفظ و صیانت می‌شود، اما هزینه‌ها آنها بالا می‌رود و سرمایه اجتماعی آنها کم می‌شود؛ و برعکس هرچه به سمت رویکرد سایبرلیبرالیستی تمایل پیدا کنند، سرمایه اجتماعی افزایش و هزینه‌ها کاهش پیدا خواهد کرد. از این رو **پیشنهاد می‌شود** رویکرد جمهوری اسلامی ایران در فضای سایبر، اساساً باید در سطح ملی از پارادایم پاترنالیستی و در سطح بین‌المللی از رویکرد لیبرالیستی تبعیت کند تا ضمن ارتقای سرمایه اجتماعی در محیط ملی، بتواند از حاکمیت و استقلال خود در محیط بین‌الملل صیانت کند.

منابع

۱. فارسی

الف) کتاب‌ها

۱. آندرو، موری (۱۳۹۸). *تنظیم مقررات فضای سایبر: کنترل در محیط آنلاین*. ترجمه محمد رضا حسینی و نصیب اله دوستی مطلق، تهران: انتشارات حقوقی.
۲. غلامی، رضا (۱۳۹۸). *الگوی شش ضلعی حکمرانی ج.ا.ا. در فضای مجازی*. تهران: مرکز ملی فضای مجازی.
۳. مهدی‌زاده، سید مهدی (۱۳۹۵). *نظریه‌های رسانه‌اندیشه‌های رایج و دیدگاه‌های انتقادی*. تهران: همشهری.
۴. میرزاپور، حسین (۱۳۹۸). *چالش‌های حکمرانی و تنظیم‌گری فضای مجازی در کشور*. تهران: اندیشکده حکمرانی شریف.

ب) مقالات

۵. الوانی، سید مهدی؛ خنیفر حسین و حاجی ملامیرزایی، حامد (۱۳۹۳). *تدوین الگوی خط‌مشی‌گذاری فضای مجازی کشور*. فصلنامه راهبرد اجتماعی فرهنگی، ۴(۱۳)، ۷۵-۱۰۰.
۶. حافظ‌نیا، محمد رضا (۱۳۹۰). *مفهوم‌سازی ژئوپلیتیک اینترنت و فضای مجازی*. فصلنامه بین‌المللی علمی-پژوهشی ژئوپلیتیک، ۷(۲۱)، تهران: انجمن ژئوپلیتیک ایران، ۲۴، ۱-۱۳.
۷. ضیایی، سید یاسر و شکیب‌نژاد، احسان (۱۳۹۶). *قانون‌گذاری در فضای سایبر: رویکرد حقوق بین‌الملل و حقوق ایران*. مجله حقوقی بین‌المللی، ۳۴(۵۷)، ۲۲۷-۲۴۷.
۸. کیان خواه، احسان (۱۳۹۷). *چالش‌های راهبردی حکمرانی با گسترش فضای سایبر*. فصلنامه علمی امنیت ملی، ۹(۳۴)، ص ۴۴، ۱۵۳-۱۷۴.
۹. کیان خواه، احسان (۱۳۹۶). *تبیین ماهیت و مؤلفه‌های فضای سایبر بر اساس تفکر اسلامی*. رساله دکتری،

تهران: دانشگاه عالی دفاع ملی، دانشکده امنیت ملی، ۶۱-۸۷.

۱۰. محمودی میمند، محمد؛ شایان، علی و کلانتری، نادیا (۱۳۹۱). چارچوب خط‌مشی‌گذاری توسعه فناوری اطلاعات و ارتباطات در ایران. *فصلنامه علمی پژوهشی پژوهشگاه علوم و فناوری اطلاعات ایران*، ۳(۲۷)، ۶۱۷-۶۳۹.

۱۱. هداوند، مهدی (۱۳۸۵). درآمدی بر مقررات‌گذاری اجتماعی. *فصلنامه حقوق عمومی*، ۲، ۴۸-۶۳.

۱۲. یآوری، اسدالله (۱۳۹۳). درآمدی بر مفهوم تنظیم‌گری حقوقی. *فصلنامه مطالعات حقوق تطبیقی*، ۵(۲)، ۶۲۹-۶۴۷.

۲. انگلیسی

A) Books

1. Ashby, W. Ross, Ashby, W. Ross (1957). *Introduction to Cybernetics*. Science Editions, John Wiley Sons Inc, (London: Chapman & Hall).
2. Austin, John (1986). *Lectures on Jurisprudence*, 3rd edn (London: John Murray), Vol. I, Lecture I.
3. Baldwin, R., & Cave, M. (1999). *Understanding Regulation Theory, Strategy, and Practice*. Oxford University Press (Oxford).
4. Barlow, John P., A. (1996) *Declaration of the Independence of Cyberspace*, Davos: Electronic Frontier Foundation.
5. Easterbrook, F. (1996). *Cyberspace and the Law of the Horse*. University of Chicago Legal Forum.
6. Lessig, L. (2000). *The Code in Law, and the Law in Code* (New York: Basic Books).
7. Lessig, L. (1999). *Code and Other Laws of Cyberspace*, (New York: Basic Books).
8. Loader, B. D. (2010). *The Governance of Cyberspace, The Governance of Cyberspace*.
9. Lipton, J. D. (2014). *Cyberlaw 2.0*, Akron Law Publications.
10. Murray, Andrew (2006). *The Regulation of Cyberspace: Control in the Online Environment*, London: Routledge-Cavandish.
11. Murray, A. (2010). *Information Technology Law: The Law and Society*. (Oxford: Oxford University Press).
12. Hart, H. (1994). *The Concept of Law*. 2nd edn (Oxford: Oxford University Press).
13. Raz, J. (2009). *The Authority of Law*. 2nd edn (Oxford: Oxford University Press).
14. Reed, C. (2012). *Making Laws for Cyberspace*. British Library Cataloguing in publication Data.
15. Tikk, E. (2011). *Comprehensive Legal Approach to Cyber Security*. (University of Tartu)
16. Wamala, F. (2011). *ITU National Cybersecurity Strategy Guide*. PHD theses, CISSP.
17. Elsner G., & Natarajan, A. (2020). *Regulating the Cyberspace: Perspectives from Asia*. Konrad-Adenauer-Stiftung.

B) Articles

18. Benkler, Y. (2000). From Consumers to Users: Shifting the Deeper Structures of Regulation toward Sustainable Commons and User Access. *Federal Communications*

-
- Law Journal*, 52(3), 561–579.
19. Johnson, D.R., & David G. Post (1996). Law And Borders-The Rise of Law in Cyberspace. *Stanford Law Review*.
 20. Klaić, A., & Perešin, A.(2016). The Impact of the National Information Security Regulation Framework on Cyber Security in Global Environment. *An International Journal*, 34(1), 37-55.
 21. Lessig, L. (1999). The Law of the Horse: What Cyberlaw Might Teach. *Harvard Law Review*, 113.
 22. Millwood-hargrave, M. (2007). report for Working group 3 of the Conference of Experts for European Media policy, More Trust in Content – The potential of Co- and Self-regulation in Digital Media. 60-61.
 23. Murray, A.(2002). and Colin Scott, "Controlling the New Media: Hybrid Responses to New Forms of Power. *The Modern Law Review*, 65(4,) 491–516.
 24. Porter, M. E., & Claas van der Linde (1995). The relationship between environmental goals and industrial competitive. *The journal of Economic Perspective*, 9(4), 97-115.
 25. Tyler, T. R. ,& Darley, J.M. (2000). Building a Law-abiding Society: Taking Public Views about Morality and the Legitimacy of Legal Authorities into Account when Formulating Substantive Law.28 *Hofstra Law Review*, 707, 713:
 26. Wingfield, T. C., & Tikk, E. (2010). Frameworks for International Cyber Security: The Cube, the Pyramid, and the Screen. *2nd International Conference on Cyber Conflict*, June, 16–22.
 27. Tan, Eugene EG and Benjamin Ang(2023). ASEAN Ambiguity on International Law and Norms for Cyberspace. *Balfic Yearbook of Internafional*, 133-162.
 28. Ashwin, s. (2022). Cyberspace Regulatory Models and their Feasibility. *Enhelions blogs*, 3-18.