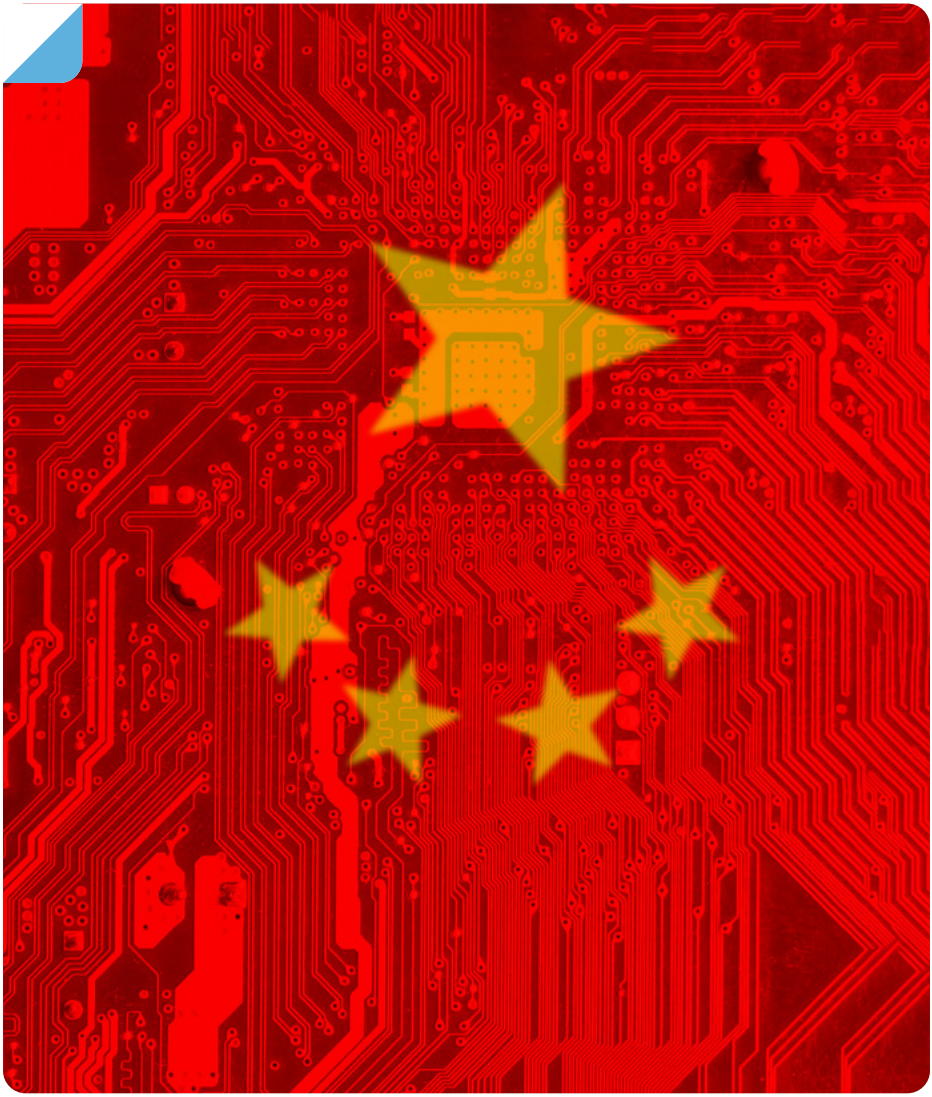
زاویه

نگاهی نو؛
به حکمرانی فضای مجازی



حکمرانی فضای مجازی در چین

سیر تحولات، ویژگی‌ها و روندهای آینده

حکمرانی فضای مجازی در چین

سیر تحولات، ویژگی‌ها و روندهای آینده

مترجم	احسان امینی
ناظر	علی زرودی
مدیر مطالعه	امین زاده‌حسین

تاریخ تنظیم	زمستان ۱۴۰۲
تعداد کلمات	۱۰,۲۷۵
کلیدواژه‌ها	مطالعه تطبیقی، چین، حکمرانی فضای مجازی، روندپژوهی

زاویه

نگاهی نو،
به حکمرانی فضای مجازی

www.zaviehmag.ir

فهرست مطالب

۱) خلاصه مدیریتی

فراگیرشدن روزافزون فضای مجازی، باعث افزایش اهمیت حکمرانی این حوزه در تجارت و سیاست بین‌المللی شده است. علی‌رغم تیره‌ترشدن روابط چین با اکثر کشورهای پیشرو در حوزه فناوری، پکن توانسته است، جامع‌ترین سیستم تنظیم‌گری و تصدی‌گری جهان را برای حکمرانیِ فضای سایبری ایجاد کند. بااین‌حال، چالش فزاینده تطبیق‌پذیری برای بازیگرانی که از فضای سایبری چین استفاده می‌کنند و همچنین نحوه‌ی مواجهه اخیر چین با شرکت‌های فناوری اینترنتی، توجهات بین‌المللی را به اهداف دولت-حزب[۱] چین در این قلمروی حساس جلب کرده است.

برای درک این اهداف، بررسی رویدادهای اخیر کافی نیست. چارچوب حکمرانی فضای سایبری چین محصولِ دهه‌ها پیگیریِ فرایند توسعه است که طی آن دولت-حزبِ این کشور با تحولات جهانی فضای سایبری مواجه شده و در این عرصه دگرگون‌شونده، منافع خود را مشخص کرده است. ماهیت نوظهور فضای سایبری چالش‌های مهمی را در عرصه حکمرانی، حتی برای پیشروترین کشورها در حوزه فناوری، ایجاد کرده است. چین به‌هنگامِ ورود به این عرصه، در فناوری موقعیت مساعدی نداشت و مسیر خود در این قلمرو را بر مبنای توسعه سریع و ایجاد آزادی‌های سیاسی نسبی طراحی کرد. به‌همین‌خاطر، دولت-حزب چین نسبتاً به‌موقع توانست حکمرانی فضای سایبری را به عنوان یک مسئله اساسی به رسمیت بشناسد. همان‌طور که نشریه حزب کمونیست چین بیان می‌کند: «اگر حزب ما نتواند بر موانع ایجادشده توسط اینترنت غلبه کند، در بلندمدت قادر به حفظ قدرت خود نخواهد بود».

این گزارش به ارائهٔ تصویری اجمالی از ورود دولت-حزب چین به عرصه اینترنت و مواجههٔ آن با صنعت جهانی فناوری‌های دیجیتال و تکامل سیاست‌های آن

۱. Party-state

برای مدیریت فضای سایبری به‌مثابه یک کل درهم‌تنیده می‌پردازد. در ادامه، به شناسایی بازیگران اصلی و نقش و جایگاه آن‌ها در حکمرانی فضای سایبری چین پرداخته می‌شود. با اینکه هنوز موازی‌کاری‌های بوروکراتیک و تعاریف نامشخص در نظام حکمرانی چین وجود دارد؛ اما به‌اندازهٔ‌کافی ثبات یافته است که بتوان جنبه‌های اصلی آن را توضیح داد. این مسئله در مورد عرصه دگرگون‌شوندهٔ تنظیم‌گریِ این کشور در حوزه فضای مجازی نیز صادق است؛ عرصه‌ای که مهم‌ترین عناصر آن، به‌ویژه قوانین سخت‌گیرانه حاکم بر مدیریت و انتقال فرا مرزیِ داده‌ها، در بخش بعدی گزارش شرح داده شده است.

بازیگران و قوانین اصلی کشور چین در حوزه حکمرانی فضای مجازی عبارت‌اند از:

نهادهای اصلی حکمرانی فضای مجازی کشور چین

۱) کمیسیون مرکزی امنیت سایبری و توسعه جامعه اطلاعاتی

معادل انگلیسی	Central Commission for Cybersecurity and Informatization (CCCI)
حوزه مسئولیت	• تعیین سیاست‌های کلان و همچنین حل اختلافات بوروکراتیک در جهت هماهنگی میان نهادهای مختلف در حوزه فضای سایبری چین

۲) اداره فضای مجازی چین

معادل انگلیسی	Cyberspace Administration of China (CAC)
حوزه مسئولیت	• دفتر پشتیبانی و بازوی اجرایی کمیسیون مرکزی امنیت سایبری و توسعه جامعه اطلاعاتی • نظارت، هماهنگی و تنظیم سیاست‌ها میان نهادهای مختلف دولتی و شبه‌نظامی • مسئول اصلی اجرای قانون حفاظت از اطلاعات شخصی از طریق توسعه مقررات و استانداردهای فرعی • بررسی‌های امنیت سایبری در زیرساخت‌های اطلاعاتی حیاتی (CII) • مسئول تنظیم مقررات صادرات اطلاعات شخصی به خارج از مرزهای چین و توسعه نظام‌های انتقال برون‌مرزی داده، ویژه «مناطق آزمایشی تجاری خدمات نوآورانه» • مسئول اصلی اجرای برنامه پنج ساله ملی توسعه جامعه اطلاعاتی (FYPNI)

۳) وزارت صنعت و فناوری اطلاعات

معادل انگلیسی	Ministry for Industry and Information Technology (MIIT)
حوزه مسئولیت	• اختیارات نظارتی در حوزه DNSها • توسعه زیرساخت دیجیتال و فناوری‌های پیشرو • مسئول «مناطق آزمایشی تجاری خدمات نوآورانه»

۴) آکادمی فناوری اطلاعات و ارتباطات چین

معادل انگلیسی	China Academy for Information and Communication Technologies (CAICT)
حوزه مسئولیت	• تحقیق و توسعه در حوزه کاربردهای فناوری در زمینه فضای سایبری به‌ویژه از طریق همکاری‌های بین‌المللی

۵) کمیته فنی ملیِ استانداردسازی امنیت اطلاعات

معادل انگلیسی	National Information Security Standardization Technical Committee (TC۲۶۰)
حوزه مسئولیت	• یکی از نهادهای متخصص در حوزه سیاست‌گذاری و انتشار مقررات و استانداردهای فضای سایبری چین

۶) وزارت امنیت عمومی

معادل انگلیسی	Ministry of Public Security (MPS)
حوزه مسئولیت	• نظارت بر سیستم حفاظت چندسطحی برای درجه‌بندی امنیت اطلاعات • متولی اصلی پیاده‌سازی عملیاتی امنیت سایبری در چین • نظارت بر نقض قوانین حفاظت از اطلاعات شخصی

۷) وزارت امنیت کشور

معادل انگلیسی	Ministry of State Security (MSS)
حوزه مسئولیت	• بررسی تیم‌های امنیت سایبری داخلی • مدیریت پایگاه داده آسیب‌پذیری ملی برای امنیت اطلاعات

۸) وزارت امور خارجه

معادل انگلیسی	Ministry of Foreign Affairs (MFA)
حوزه مسئولیت	• مسئول دیپلماسی سایبر کشور چین

۹) ارتش آزادی بخش خلق

معادل انگلیسی	People's Liberation Army (PLA)
حوزه مسئولیت	• استفاده نظامی از فضای سایبری • حضور در کمیسیون مرکزی امنیت سایبری و توسعه جامعه اطلاعاتی

قوانین و مقررات اصلی حکمرانی فضای مجازی در چین

۱) قانون امنیت سایبری

معادل انگلیسی	Cybersecurity Law (CSL)
معرفی اجمالی	• در سال ۲۰۱۷ اجرایی شد. • اپراتورها را ملزم به رعایت سیستم حفاظت چندسطحی (MLPS) کرد. • اپراتورها ملزم هستند تا اقداماتی شامل ایجاد سیستم مدیریت امنیت داخلی، اقدامات امنیتی فنی و آموزش امنیت سایبری را اجرا کنند. • وضعیت امنیت سایبری در زیرساخت‌های اطلاعاتی حیاتی (CII) توسط اداره فضای مجازی چین بررسی می‌شود. • اطلاعات شخصی و داده‌های مهم که توسط زیرساخت‌های اطلاعاتی حیاتی در قلمرو سرزمینی چین جمع‌آوری یا تولید شده‌اند، بایستی در سرزمین چین ذخیره گردد.

۲) قانون امنیت داده

معادل انگلیسی	Data Security Law (DSL)
معرفی اجمالی	• از سال ۲۰۲۱ اجرایی شد. • این قانون یک چارچوب نظارتی جامع برای داده‌ها است. • این قانون امنیت ملی و توسعه اجتماعی را در اولویت قرار می‌دهد و سعی دارد با ایجاد چارچوبی نهادی، از داده‌ها به‌عنوان عاملی برای تولید استفاده شود. • قانون امنیت داده شامل هرگونه اطلاعات به اشکال الکترونیکی یا دیگر اشکال می‌شود. • طبق این قانون، دولت موظف است تا یک سیستم طبقه‌بندی‌شده برای حفاظت از داده‌ها ایجاد کند. • قانون امنیت داده اجرای یک سیستم کنترل صادرات داده را هدایت می‌کند.

۳) پیش‌نویس مقررات مدیریت امنیت داده‌های آنلاین

معادل انگلیسی	Draft Online Data Security Management Regulation (ODSMR)
معرفی اجمالی	• این پیش‌نویس در نوامبر سال ۲۰۲۱ منتشر شد. • سعی در ایجاد وضوح بیشتر در مواد قانون امنیت داده دارد. • این پیش‌نویس گستره‌ی ماده ۳۵ قانون امنیت سایبری را پیرامون شرایط بررسی امنیت سایبری گسترش می‌دهد. • پیش‌نویس مقررات مدیریت امنیت داده آنلاین دارای صلاحیت فراسرزمینی گسترده‌ای است.

۴) قانون حفاظت از اطلاعات شخصی

معادل انگلیسی	Personal Information Protection Law (PIPL)
معرفی اجمالی	• از سال ۲۰۲۱ اجرایی شد. • این قانون پاسخگوی تقاضای رایج در چین برای حفاظت اثربخش‌تر از داده‌های شخصی در مواجهه با سوءاستفاده‌های گسترده از سوی کنشگران غیردولتی است. • مدیریت اطلاعات شخصی «اشخاص حقیقی» درون مرزهای چین مشمول قانون حفاظت از اطلاعات شخصی است. • این قانون در قبال فعالیت‌های خارج از چین که هدف آن‌ها ارائه محصولات و خدمات به اشخاص حقیقی داخلی چین است، مدعی صلاحیت قضایی فرامرزی است. • این قانون به‌جای ایجاد حقوق اساسی یا اصول کلی قانونی، به تنظیم‌گری طبقات کنشگران و روابط آن‌ها برمبنای داوری‌ها درباره ریسک‌ها اقدام می‌کند. • اداره فضای مجازی چین درباره مواد این قانون هم اختیار سیاست‌گذاری و هم اختیار نظارت دارد.

۵) اقدامات ارزیابی امنیتی انتقال داده به خارج

معادل انگلیسی	Outbound Data Transfer Security Assessment Measures (ODTSAM)
معرفی اجمالی	• این سند از سپتامبر ۲۰۲۲ اجرایی می‌شود. • مفاد اقدامات مذکور در این سند، تعهدات مربوط به ارسال داده به خارج از چین در کل قانون امنیت سایبری، قانون امنیت داده و قانون حفاظت از اطلاعات شخصی را یکپارچه و تلفیق می‌کند.

در نهایت، در بخش نتیجه‌گیری به سیستم حکمرانی فضای سایبری چین و افق توسعه آینده آن در بافتار بین‌المللی پرداخته می‌شود. یادگیری نحوه مواجهه با این سیستم برای کشورهای خارجی و همچنین بازیگران خصوصی امری اجتناب‌ناپذیر است و با وجود روند سلطه‌طلبانه‌ترشدنِ اهداف حزب-دولتِ چین و فقدان افقی از بهبود روابط سیاسی با کشورهای غربی، روزبه‌روز دشوارتر خواهد شد. بااین‌حال، مدل منحصربه‌فرد چین در این حوزه در مواجهه با همان چالش‌هایی شکل گرفته است که سایر جوامع در فضای سایبری با آن‌ها روبرو هستند؛ ازاین‌رو، شناخت این مدل درس‌هایی برای دیگر کشورها خواهد داشت.

در ادامه، ترجمه گزارش «حکمرانی فضای مجازی چین؛ سیر تحولات، ویژگی‌ها و روندهای آینده»[۱] نوشته‌ی جان لی[۲]، مدیر شرکت مشاوره «ایست‌وِست فیوچرز»[۳]، منتشرشده از سوی مؤسسه روابط بین‌الملل فرانسه[۴] ارائه شده است.[۵]

۱. Cyberspace Governance in China: Evolution, Features and Future Trends
۲. John Lee
۳. East West Futures
۴. The French Institute of International Relations (IFRI)
۵. گزارش فعلی، حاصل ترجمه بخش اصلی گزارش مبدا می باشد که پیرامون سیر تحولات، ساختار مدیریت و قوانین حکمرانی فضای مجازی چین است. بخش پایانی گزارش مبدا به دلیل فاصله داشتن از هدف گروه زاویه، ترجمه نشده است.


D&G
新疆棉

۲) مقدمه

گسترش روزافزون فعالیت‌های جاری در بستر شبکه‌های دیجیتال، حکمرانی فضای سایبری را تبدیل به عنصری کلیدی در عرصه تجارت و سیاست بین‌المللی کرده است. علی‌رغم تأثیر منفی تنش‌های سیاسی بر جریان‌های برون‌مرزیِ اطلاعات و کالاها که زیربنای جهانی‌شدن هستند، دولت‌ها در حال گسترش کنترل خود بر فعالیت‌های جاری در فضای سایبری هستند. دراین‌میان، بزرگ‌ترین خطوط شکاف‌های بین‌المللی در اطراف چین شکل گرفته است؛ کشوری که روابط سیاسی آن با کشورهای غربی روزبه‌روز متخاصمانه‌تر شده و درعین‌حال جامع‌ترین سیستم تنظیم‌گری و مدیریتی جهان را برای حکمرانی فضای سایبری ایجاد کرده است.

در ماه‌های اخیر، رونماییِ پکن از مجموعه قوانین جامعی ناظر به حکمرانی داده و همچنین تشدید سیاست‌های تنظیم‌گری شرکت‌های فناوری اینترنتی این کشور، توجهات زیادی را به خود جلب کرده است. با وجود اینکه پیشرفت‌های چین، جایگاه

این کشور را در فناوری‌های نوظهور و بازارهای دیجیتال در سطح جهان تقویت کرده، درعین‌حال باعث ایجاد چالش‌ها و ریسک‌هایی در ارتباط با انطباق‌پذیریِ بازیگران خارجی شده است؛ بازیگرانی که تلاش می‌کنند با چین، تطبیق پیدا کنند. این‌گونه رفتارهای مقامات چینی را باید با نظر به شرایط سیاسی و اقتصادی کنونی این کشور توضیح داد و امید داشت که تغییر این شرایط منجر به بازگشت دولت چین به نگرشی آزادتر نسبت به اقتصاد دیجیتال شود.

بااین‌حال، اگر برای یافتن پاسخ این پرسش‌ها نگاه خود را صرفاً معطوف به شرایط کنونیِ این کشور کنیم، روندهای بلندمدت را از دست خواهیم داد. نظام حکمرانی فضای سایبری چین محصول دهه‌ها تکامل و مواضع ریشه‌دار رهبران چین در مورد رابطه بین فضای سایبری و اولویت‌های ملی است. عناصر جدیدی مانند قانون امنیت داده چین[۱] یا بررسی‌های امنیت سایبری شرکت‌های فناوری اینترنتی را باید نه به‌مثابهٔ عناصری مستقل و مجزا، بلکه به‌عنوان بخشی از یک چارچوب بزرگ‌تر و درحال‌تکامل در نظر گرفت. ناظران خارجی باید به‌جای توجه به سرکوب شرکت‌های فناوری اینترنتی توسط چین و تخمین‌هایی در مورد آینده بر اساس آن، به دنبال درک نگاه دولت-حزب چین به فضای سایبری و درک نحوه‌ای باشند که اهداف سیاستیِ بلندمدت، سیستم حکمرانی فضای سایبری این کشور را شکل داده‌اند.

این سیستم اگرچه درحال‌حاضر جامعیت دارد، اما طراحی آن دارای نقص‌های بسیاری بوده و در تصمیم‌گیری‌ها اختیارعملِ بیش‌ازحدی به مقامات چینی می‌دهد و هنوز به تدقیقِ بسیاری از جزئیات نیاز دارد. از بسیاری جهات، هنوز نمی‌توان فضای روشنی از اقتدار بوروکراتیک و یا الزامات مشخصی برای تطبیق‌پذیری در آن مشاهده کرد. اما این سیستم به‌طورفزاینده‌ای خود را بر هر جنبه‌ای از مبادلات خارجی با چین

۱. China's Data Security Law (DSL)

تحمیل خواهد کرد؛ چراکه استفاده از فضای مجازی برای فعالیت‌های انسانی در سراسر جهان روزبه‌روز درحال فراگیرترشدن است.

این گزارش به‌طور خلاصه نشان می‌دهد که چگونه سیاست فضای سایبری دولت-حزب چین در طول دهه‌ها تکامل یافته و به شکل کنونی خود رسیده است. سپس عناصر اصلی سیستم حاکمیت فضای سایبری چین، یعنی بازیگران نهادی، قوانین و مقررات، تشریح شده و به‌طورخاص به پیامدهای تبادل برون‌مرزی داده‌ها[۱] خواهیم پرداخت.

۱. Cross-border data transfers

۳) سیر حکمرانی فضای سایبری در چین

اولویت دادن به توسعه و امنیت

۳-۱) سال‌های اولیه: استفاده از فناوری خارجی اما با خصوصیات چینی

گسترش اینترنت در چین و ارتباطات این کشور با دنیای خارج از ابتدا به‌گونه‌ای طراحی شد که امکان اِشراف و کنترل دولت بر کل شبکه در سراسر کشور را فراهم کند. این شبکه از نظر فیزیکی برای تسهیل فیلترکردن ترافیک برون‌مرزی با استفاده از تجهیزات و نرم‌افزارهای ارائه‌شده توسط شرکت‌های آمریکایی (به ویژه سیسکو[۱]) ساخته شده بود. چین از روش‌هایی که شرکت‌های خصوصی در سایر نقاط جهان برای بررسی و کنترل انتقال داده‌های دیجیتال استفاده می‌کنند، برای نظارت و سانسور ارتباطات این کشور با شبکه‌های خارجی در ابعاد ملی بهره می‌گرفت. همچنین، یک سیستم سانسور داخلی، پشتیبان این فرایند بود؛ سیستمی که

۱. Cisco

مسئولیت را به شرکت‌ها و مؤسساتی که خدمات اینترنتی در سطح مصرف‌کننده ارائه می‌کنند، واگذار کرده است. این سیستم به‌طور تاریخی به‌شدت بر سانسور و رویکردهای گزینشیِ مقامات ایالتی در مورد مداخله در موارد سیاسیِ دارای اولویت متکی بوده است.

بنابراین، اینترنت چینی را باید نه به عنوان یک اینترنت مستقل، بلکه همچون شاخه‌ای از اینترنت جهانی در نظر گرفت که در مرزهای بین‌المللی کنترل می‌شود. ازاین‌جهت، اینترنت چین را می‌توان با نحوه کنترل‌های مهاجرتی و گمرکی در مرزهای فیزیکی کشورها مقایسه کرد. اگرچه الزامات فنی فیلترکردن محتوا، تبعاتی برای کارآمدی اینترنت چین خواهد داشت، اما شبکه‌های چینی ازآنجاکه اساساً مبتنی بر فناوریِ مشابه با سایر نقاط جهان شکل گرفته‌اند، به‌لحاظ تاریخی همواره امکان تعامل و همکاری با شبکه‌های خارجی را داشته‌اند. تا پیش از دهه ۲۰۰۰، این فناوری تقریباً به‌طور کامل در اختیار شرکت‌های مربوط به اقتصادهای توسعه‌یافته، به‌ویژه ایالات متحده، بوده است.

مقامات چینی درعینِ‌اینکه مکانیسم‌هایی را برای کنترل دسترسی جمعیت خود به فضای سایبری طراحی می‌کردند، از اواخر دهه ۱۹۹۰ شروع به گسترش سریع زیرساخت اینترنت نمودند. اما به‌غیر از سانسور سیاسی، کنش‌گران دولتی در ابتدا توجه چندانی به تنظیم‌گری فضای سایبری نوظهور چینی و یا توسعه محصولات و خدمات برای استفاده از آن نداشتند. این خلاء توسط کارآفرینان خصوصی پر می‌شد که از آزادسازی اقتصادی و ضرورت دستیابی به رشد و توسعه برای دولت‌های محلی بهره می‌بردند. آزادشدن سفرهای بین‌المللی به اتباع چینی این امکان را داد تا برای تحصیلات رسمی و کسب تجربه کاری در بخش فناوری اطلاعات و ارتباطات، به ایالات متحده بروند؛ اتفاقی که باعث دستیابی آن‌ها به مهارت‌ها و ایده‌هایی شد که با افزایش جمعیت آنلاین چین، تبدیل به محل مناسبی برای کسب درآمد گردید.

فارغ از اینکه سیاست دولتیِ آگاهانه‌ای برای دور نگه داشتن پرچم‌داران بازار خارجی در جهت تقویت رشد جایگزین‌های داخلی وجود داشته است یا نه، تأثیرات نظام سانسور و محدودیت‌های سیاسی مانع از ورود و استقرار پلتفرم‌های بزرگ اینترنتیِ ایالات متحده در فضای سایبری چین شد. سایر شرکت‌های خارجی نیز اغلب قادر به سازگاری با شرایط و اقتضائات محلی و یا تمهیدِ اقدامات لازم برای موفقیت در رقابت بی‌رحمانه بازارهای آنلاین چین نبودند. بااین‌وجود، فعالیت شرکت‌هایی مانند مایکروسافت و اپل در چین به توسعه شرکت‌های فناوری اطلاعات و ارتباطاتِ این کشور در بخش‌های نرم‌افزار و سخت‌افزار کمک کرد. به‌عنوان مثال، عملیات تولیدی اپل در چین، نیروی محرک توسعه یک شبکه تأمین‌کننده از شرکت‌های چینی برای رقابت جهانی و ارتقای مهارت نیروی کار آن‌ها بوده است.

۳-۲) توسعه جامعه اطلاعاتی: ایجاد قابلیت‌های چین در فناوری‌های دیجیتال

زمینه سیاستیِ همه این فعالیت‌ها، جهت‌گیری رأس نظام سیاسی چین بود که کاربرد گسترده آی‌سی‌تی را یک اولویت سیاستیِ ملی قلمداد می‌کرد. در سال ۱۹۹۲ بود که توسعه اقتصاد اطلاعات به عنوان یک هدف مهم سیاستی شناسایی شد. اولویتی که رهبران ارشد چین برای پیوستن به اقتصاد جهانی مبتنی بر فناوری اطلاعات و ارتباطات تعیین کرده بودند، به‌نحو نمادینی در جلساتی که در اواسط دهه ۱۹۹۰ بین «بیل گیتس» و «جیانگ زِمین»، دبیر کل حزب کمونیست و رئیس جمهور چین برگزار شد، نمود پیدا کرد.

دستورالعمل دولت چین برای این گسترش کاربرد آی‌سی‌تی، «توسعه جامعه اطلاعاتی»[۱] است. در سال ۲۰۰۰، دفتر سیاسی دولت تصمیم گرفت که ارتقاء چین به

۱. informatization

یک «جامعه اطلاعاتی»[۱] که همراه با تأثیرات دگرگون‌کننده‌ای برای بهره‌وری اقتصادی خواهد بود، در صدر اولویت‌های سیاستی این کشور قرار بگیرد. در سال ۲۰۰۶ شورای دولت[۲]، بالاترین ساختار در قوهٔ مجریه، راهبرد ملی پانزده ساله در توسعه اطلاعات[۳] را تصویب کرد. ازآن‌پس، توسعه آی‌سی‌تی همواره یکی از موضوعات ثابت در بیانیه‌های سیاستیِ ملی این کشور در دو دهه گذشته بوده است. دراین‌میان می‌توان به سند «اینترنت پلاس»[۴]، ناظر به «درهم‌تنیدگی عمیق»[۵] اینترنت با تمام جنبه‌های اقتصاد و جامعه چین و نیز دستورالعمل «ساخت چین ۲۰۲۵»[۶] اشاره کرد که در سال ۲۰۱۵ توسط دولت و در راستای کمک به صنعت چین در رسیدن به مرزهای فناوری در طیف وسیعی از صنایع برجستهٔ مرتبط با آی‌سی‌تی تصویب شد.

زیربنای این تعهد بلندمدت، فرایند مشروعیت‌بخشی نظری حزب کمونیست[۷] به سیاست‌های خود بوده است؛ سیاست‌هایی که مدت‌هاست دستورکارِ «توسعه جامعه اطلاعاتی» را به‌عنوان یک روند تاریخی جهانی شناسایی کرده است که چین، اگر به‌دنبال مدرن‌شدن و صیانت از خود در برابر قدرت‌های متخاصم خارجی است، باید خود را در مسیر آن حفظ کند. از زمان آغاز رهبری شی جین‌پینگ[۸] در سال ۲۰۱۲، سیاسی‌شدن مجدد و افزایش کنترل حزب در سراسر جامعه چین در تعارضی بنیادین با «جامعه اطلاعاتی»، آنچنان‌که در دموکراسی‌های لیبرال درک می‌شود، قرار داشته است. اما پافشاری شی جین‌پینگ بر اصل «توسعه جامعه اطلاعاتی» نشان‌دهندهٔ اطمینان رهبران حزب به توان خود در رفع این تناقض مبنایی بوده

۱. information society
۲. State Council
۳. National Informatization Development Strategy (NIDS)
۴. Internet Plus
۵. deep integration
۶. Made in China 2025
۷. The Chinese Communist Party (CCP)
۸. Xi Jinping

است: «آب در هاون کوبیدن»[۱]؛ استعاره‌ای که بیل کلینتون در مورد چالش سیاست‌گذاریِ رفتارهای اجتماعی در فضای سایبری به‌کار برده بود.

این چارچوب سیاستی گسترده با اقدامات ملموس، هرچند با درجات موفقیت متفاوت، هماهنگ شده است؛ اقداماتی که هدف آن‌ها تقویت روند توسعه و به‌کارگیری فناوری‌ها و زیرساخت‌های آی‌سی‌تی در چین است. به‌عنوان مثال، از اواسط دهه ۲۰۰۰، حاکمیت ملی شروع به تقویت توسعه فناوری‌های «اینترنت اشیا»[۲]، تقویت بخش‌های «تحقیق و توسعه» در نقاط خاصی که از حمایت بلندمدتِ حکومت‌های محلی برخوردار بودند و همچنین استفاده از دستاوردها برای حمایت از پیشرفت‌های فناورانهٔ پرچم‌داران صنعت چین، شرکت‌هایی مانند هوآوی، کرد. در سال‌های اخیر، دولت توسعه سریع «زیرساخت‌های نوع جدید» را برای ارتقای اتصال دیجیتال در مقیاس ملی، به ویژه دستیابی به بیشترین سرعت در به‌کارگیری تجهیزات شبکه‌های مخابراتی نسل پنجم[۳] در جهان، در دستور کار خود قرار داده است.

۳-۳) امنیتی‌سازی[۴]: ایجاد توازن مجدد در توسعه فضای سایبری چین

یکی از نتایج خلاء اولیه تنظیم‌گری فضای سایبری چین این بود که روند رشد زیرساخت‌های آی‌سی‌تی و صنایع مرتبط، از توسعه قابلیت‌های امنیت سایبریِ متناظر با آن سبقت گرفت. مدت مدیدی است که تمرکز دولت بر سانسور سیاسی، بسیاری از منابع موجود برای اقدامات حفاظتی در فضای سایبری را جذب کرده و خود دستگاه سانسور تبدیل به یک عامل آسیب‌پذیری شده است. راهبرد ملی

۱. Nail Jell-O to the wall
۲. Internet of Things (IoT)
۳. 5G
۴. Securitization

پانزده ساله در توسعه اطلاعات در سال ۲۰۰۶ خطرات ناشی از اتکای بیش‌ازحد به واردات فناوری و عدم سرمایه‌گذاری در توسعه قابلیت‌های داخلی را شناسایی و دستورالعمل سابق در مورد ایجاد یک سیستم ملی و چندسطحی برای امنیت اطلاعات[۱] را در دستورکار خود قرار داد. در اواخر دهه ۲۰۱۰، چین توانسته بود صنعت امنیت سایبری متنوعی را شکل دهد و شرکت‌های چینی با سوابق گوناگون، خدماتی را به مشتریان در تمام سطوح در سراسر فضای سایبری چین ارائه می‌کردند.

شی جین‌پینگ رهبری کشور را در همان سالی بر عهده گرفت که افشای اطلاعات ادوارد اسنودن، نفوذ گسترده دولت ایالات متحده به شبکه‌های چینی را آشکار کرده بود؛ نفوذی که از طریق همکاری اصلی‌ترین ارائه‌دهندگان خدمات آی‌سی‌تی در بخش خصوصی آمریکا ممکن شده بود. در مقابل، رهبری جدید چین اقداماتی را برای مقابله با شکاف موجود در تقسیم وظایف مربوط به امنیت سایبری در میان سازمان‌های دولتی در پیش گرفت. پکن مسئلهٔ امنیت سایبری را تا حد یک هدف سیاستی، چیزی هم‌سطحِ هدف «توسعه جامعه اطلاعاتی»، ارتقاء داده و نظارت متمرکز در سطح بالا را در دستورکار خود قرار داد. گام کلیدی در این مسیر، تأسیس «کمیسیون مرکزی امنیت سایبری و توسعه جامعه اطلاعاتی»[۲] در اوایل سال ۲۰۱۴ به ریاست شی جین‌پینگ و گردهم‌آوردن نمایندگان ارشد سیستم بوروکراتیک، دانشگاه و ارتش چین بود. دفتر اجرایی این کمیسیون «اداره فضای مجازی چین»[۳] نام گرفت که علاوه بر ارائه پشتیبانی اداری به این کمیسیون، به‌تدریج مسئولیت‌های مختلفی را که در بخش‌های بعدی شرح خواهیم داد، برعهده گرفته است.

افشاگری‌های اسنودن مقامات چینی را بر آن داشت که در تأمین و توسعه فناوری‌های آی‌سی‌تی، به‌خصوص در «فناوری‌های مهم» مانند پردازنده‌های رایانه‌ای

۱. multi-level national information security system
۲. Central Commission for Cybersecurity and Informatization (CCCI)
۳. Cyberspace Administration of China (CAC)

و سیستم‌عامل‌های نرم‌افزاری، با جدیت بیشتری به‌دنبال جایگزین‌کردن توسعه ظرفیت‌های داخلی به‌جای واردات باشد. رهبر این کشور همچنین کمبود شدید نیروی کار متخصص در حوزه امنیت سایبری در کشور را تشخیص داده و اقداماتی را برای ارتقای روند تربیت نیروی کار ماهر در این زمینه و طراحی رویکردی جامع به امنیت سایبری براساس تجربه‌های بین‌المللیِ موفق، آغاز کرد. اما چین حرکت خود در این مسیر را از سطوح پایینی شروع کرده و میزان رشد این مجموعه نیروی کار هنوز فاصله زیادی با نقطه‌ای دارد که کشور را قادر به برآورده‌کردن الزامات اساسی امنیت سایبری در بخش‌های بزرگی از زیرساخت‌های دیجیتال نماید.

یکی از تحلیل‌گران آمریکایی در سال ۲۰۱۵ برآورد می‌کرد که در آینده نیز ویژگی‌های بارز محیط فنی امنیت سایبری چین همچنان همان «توسعه صنعتی سایبری نامتوارن، دفاع سایبری گسسته، تبادل نامتوازن اپراتورهای سایبری و تسلط بازوهای غرب در حوزه فناوری اطلاعات بر بازار این کشور» باشد. مطالعه تطبیقی قابلیت‌های سایبری ملی که در سال ۲۰۲۱ منتشر شد، مشخص کرد که هسته دفاع سایبری چین نسبتاً ضعیف بوده و این کشور هنوز در مراحل اولیه ایجاد تاب‌آوری در زیرساخت‌های اطلاعاتی حیاتی خود قرار دارد. با شکل‌گیری روند نزولی در روابط سیاسی، ایالات متحده آمریکا نیز شروع به حمله به وابستگی‌های خارجی چین در فناوری‌های اساسی آی‌سی‌تی نموده و به‌این‌ترتیب، این نقاط‌ضعف امنیتی تشدید شدند. احساس آسیب‌پذیری عمیق، سیاست‌ها و قوانینی را شکل داد که دیگر توسط مقامات چینی برای به‌دست‌آوردن اِشراف و کنترل بر محیط فضای سایبری چین هدایت می‌شد؛ حتی زمانی که به‌ظاهر به دنبال بهره‌برداری از آن برای اهداف توسعه ملی بودند.

«راهبرد ملی امنیت سایبری» که در سال ۲۰۱۶ توسط اداره فضای مجازی چین منتشر شد، این احساس آسیب‌پذیری در برابر دو جبههٔ مختلف را منعکس می‌کرد: نخست، در برابر بازیگران خارجیِ دارای قابلیت‌های برتر در بهره‌برداری از شبکه‌های رایانه‌ای و جنگ سایبری، و دوم، در برابر مخالفت‌های سیاسی داخلی در بستر اینترنت. این راهبرد به «دو وضعیت مهم» (تهدیدات داخلی و خارجی) پرداخته و امنیت سایبری را به‌عنوان یک فعالیت اجتماعی-فنیِ جامع تعریف می‌کند. درعین‌حال، این راهبرد مهر تأییدی است بر تأکید شی جین‌پینگ بر استفاده از فضای سایبری در جهت پیشبرد توسعه ملی به‌عنوان ارزشی همسان و درهم‌تنیده با امنیت سایبری.

همچنین در سال ۲۰۱۶ چین «قانون ملی امنیت سایبری»[۱] خود را به تصویب رساند و چارچوبی از الزامات را معرفی کرد که متعاقباً در مقررات و سیاست‌های تابعه صورت‌بندی شده بود. در اواخر دهه ۲۰۱۰، دولت پیش‌نویس قوانین و سیاست‌های جدید مربوط به فضای سایبری را برای همفکری عمومی منتشر کرد. این قوانین با پشتیبانی سیستم کمیته‌های فنی مرتبط با دولت و مؤسسات دانشگاهی چین و همچنین با نظر به تجربیات آموخته‌شده از مدل‌های خارجی، مانند «مقررات عمومی حفاظت از داده‌ها»[۲] در اتحادیه اروپا، طراحی شده بود. به موازات آن، اقتصاد دیجیتال چین گسترش قابل‌توجهی پیدا کرد؛ جمعیت عظیم و روبه‌رشدِ آنلاینِ این کشور که طیف گسترده‌ای از فعالیت‌ها را از طریق «سوپر اپلیکیشن‌های»[۳] آنلاین و تحت‌کنترل شرکت‌های خصوصی چینی انجام می‌دادند، باعث شد تا دو مورد از آن‌ها (علی‌بابا و تنسنت) به جرگهٔ بزرگ‌ترین شرکت‌های جهان از لحاظ ارزش بازار بپیوندند.

۱. national Cybersecurity Law (CSL)
۲. European Union's General Data Protection Regulation (GDPR)
۳. super-apps

۳-۴) توسعه متوازن، خوداتکایی و تحول اهداف دولت-حزب برای فضای سایبری

کنفرانس حزب کمونیست در سال ۲۰۱۷ نشان‌دهنده رویگردانی از مسئله رشد اقتصادی کلان به‌سمت الگوی جامع توسعه پایدارتر و متوازن از نظر اجتماعی بود. بیانیه‌های سیاستی همچنین به‌طور فزاینده‌ای بر ادغام اقتصاد دیجیتال با اقتصاد واقعی و سامان‌دهیِ دوباره منابع در این بخش و فاصله‌گرفتن آن‌ها از پلتفرم‌های اینترنتی و انباشت قدرت انحصاری توسط شرکت‌ها و حرکت به سمت ساخت «فناوری‌های مهم»، مانند نیمه‌هادی‌ها، تأکید می‌کردند. تمرکز بر حصول اطمینان از اینکه توسعه اقتصاد دیجیتال در خدمت اقتصاد واقعی و منافع جامعه به‌عنوان یک کل قرار دارد، عامل زمینه‌ساز اصلی در سرکوب کسب‌وکارهای فناوری اینترنتی چین در سال ۲۰۲۱ بود؛ سرکوبی که در واقع از نظر گستره، اقداماتی کاملاً محدود بود. همزمان با این روندها، با توجه به گسترش نسبتاً سریع اقتصاد دیجیتال چین، به‌نحوی که ابعاد آن در سال ۲۰۱۹ تقریباً دو برابر نرخ رشد تولید ناخالص داخلی این کشور تخمین زده می‌شد، برای جبران کندشدن رشد اقتصادی چین، اولویت به این حوزه اختصاص یافت.

در سال ۲۰۲۰، ادبیات رسمی چین از مفهوم «جریان دوگانه»[۱] به‌عنوان یک هدف راهبردی برای توسعه اقتصادی این کشور پرده‌برداری کرد. به گفته شی جین‌پینگ، هدف این است که فعالیت‌های داخلی به تدریج نقش محوری در اقتصاد چین پیدا کند. این تحول سیاستی در مقابل رونمایی ایالات متحده از کنترل‌های صادراتی گسترده خود انجام شد؛ کنترل‌هایی که با هدف‌قراردادن هوآوی، توانایی این شرکت در تولید محصولات پیشرفته را تضعیف کرده و درنتیجه، آسیب‌پذیری‌های ناشی از وابستگی مداوم به ارائه‌دهندگان خارجی «فناوری‌های مهم» را تشدید کرد.

۱. dual circulation

مقامات چینی درحال افزایش تلاش خود برای کمک به شرکت‌های داخلی درجهت جبران فاصله خود از پیشگامان جهانی در بخش نیمه‌هادی‌ها بوده و شرکت‌های خصوصی در حوزه آی‌سی‌تی بیش‌ازپیش در تلاش برای جایگزینی واردات هستند. افزایش «خوداتکایی» ملی اکنون دیگر به‌طور مداوم در گفتمان رسمی سیاست فناوری مورد تأکید قرار می‌گیرد.

بااین‌حال، رهبران ارشد چین به وضوح درک می‌کنند که شکاف‌های میان توانایی کشور نسبت به پیشگامان فناوری در بسیاری از جنبه‌های آی‌سی‌تی برای سال‌های آینده ادامه خواهد داشت و چین برای دستیابی به اهداف توسعه دیجیتال این کشور به پیوندهای بین‌المللی برای همکاری در فضای سایبری نیاز دارد. شی جین‌پینگ در سخنرانی خود در دفتر سیاسی در اکتبر ۲۰۲۱، دستور داد که چین باید «به شدت در همکاری‌های بین‌المللی در زمینه اقتصاد دیجیتال مشارکت کند». در ژانویه ۲۰۲۲، وزیر صنعت و فناوری اطلاعات چین گزارشی را در روزنامه خلق منتشر کرد و در آن اظهار کرد که سیاست‌های دولتی «گشایش همه‌جانبه در بخش تولید»[۱]، سرمایه‌گذاری خارجی در تولید متوسط و بالا و همکاری بین‌المللی را در زنجیره‌های صنعتی ترویج می‌کند.

از سال ۲۰۲۱ و اوایل سال ۲۰۲۲، چین «قانون امنیت داده‌ها»[۲]، «قانون حفاظت از اطلاعات شخصی»[۳] و مقررات مختلفی در مورد فعالیت‌های تجاری در فضای سایبری، مثل حکمرانی الگوریتم‌های توصیه در خدمات اینترنت‌محور، را به تصویب رساند. این قوانین نشان‌دهنده تشدید همه‌جانبه کنترل بر پلتفرم‌های اینترنتی عظیم چینی و «گسترش بی‌قاعده سرمایه»[۴] آن‌ها بود؛ به‌نحوی که سازمان‌های

۱. all-round opening-up in the manufacturing sector
۲. Data Security Law (DSL)
۳. Personal Information Protection Law (PIPL)
۴. disorderly expansion of capital

دولتی بیش‌ازپیش به ابزارهایی برای نظارت و نظم‌بخشیدن به فعالیت‌های این شرکت‌ها مجهز شدند. این شرکت‌ها، به‌ویژه علی‌بابا، علناً مورد توبیخ قرار گرفتند و مشمول جریمه‌ها، تغییر ساختار اجباری و سایر مجازات‌های اداری شدند. سال ۲۰۲۱ احتمالاً توسط مقامات چینی به عنوان سال مناسب بین سال اول همه‌گیری کووید ۲۰۲۰ و بیستمین کنفرانس حزب در سال ۲۰۲۲ تلقی می‌شد که در آن انتظار می‌رفت شی جین‌پینگ برای یک دوره رهبری جدید تأیید شود تا اقدامات نظارتی لازم را برای به‌حداقل‌رساندن پیامدهای اقتصادی و سیاسیِ مرتبط انجام دهد.

در آخرین هفته سال ۲۰۲۱، دولت ملی تصویب مجموعه دیگری از مقررات و سیاست‌های مرتبط با فضای سایبری را در دستور کار قرار داد که مهم‌ترینِ آن‌ها چهاردهمین «برنامه پنج‌ساله ملی توسعه جامعه اطلاعاتی»[۱] بود. این سند که توسط «کمیسیون مرکزی امنیت سایبری و توسعه جامعه اطلاعاتی» تدوین شده است، درواقع راهنمایی راهبردی «برای توسعه جامعه اطلاعاتی در همه بخش‌ها و وزارتخانه‌ها» تا سال ۲۰۲۵ است. این برنامه داده‌ها را به عنوان «عامل تولید» تعیین می‌کند و آن را در عرض زمین، کار و سرمایه در چارچوب نظریِ مارکسیستی چین قرار می‌دهد. همچنین، مطابق با اصل «جریان دوگانه»، چهاردهمین برنامه پنج‌ساله توسعه جامعه اطلاعاتی از طراحی یک «اکوسیستم» متنوع و متعامل از بازیگران اقتصاد دیجیتال چین حمایت می‌کند. این برنامه ده اولویت سیاستی را تعیین می‌کند که شامل مواردی همچون توسعه زیرساخت، بهره‌برداری از داده‌ها به‌عنوان یک عامل مولد، دیجیتال‌سازی خدمات دولتی و تقویت همکاری بین‌المللی در حکمرانی فضای سایبری جهانی می‌شود.

در نهایت، چین نه از طریق چشم‌انداز پیشینی و یک فرایند پیشاپیش طراحی‌شده، بلکه از طریق یک فرایند تکامل منعطف به سیستم فعلی حکمرانی فضای سایبری

۱. Five-Year Plan for National Informatization (FYPNI)

خود دست پیدا کرده است. بااین‌حال، این روند توسعه نه‌تنها رهنمودهای سیاستی روشنی را برای مداخله دولت در فضای سایبری، بلکه یک سیستم نهادی جامع و چارچوب تنظیم‌گری برای مدیریت آن ایجاد کرده است. بخش بعدی به دو عنصر اخیر با جزئیات بیشتری نگاه می‌کند.

۴) اصلی‌ترین بازیگران نهادی در «کیک» حکمرانی فضای مجازی در چین

چین به‌خوبی توانسته است یک «xitong» یا یک گروه‌بندی کارکردی از سازمان‌های دولتی برای هماهنگ‌کردن یک حوزه سیاستی خاص در جهت عملیاتی‌کردن حکمرانی فضای سایبری ایجاد کند. به‌مانند چارچوب تنظیم‌گری که در ادامه تشریح خواهد شد، این سیستم نیز بیشتر از یک مجموعه لِگو، به یک کیک شبیه است: رابطه دقیق بین بازیگران و میزان اختیارات آن‌ها به‌وضوح تعریف نشده و هم‌پوشانی‌های بوروکراتیک قابل‌توجهی همراه با اضافه‌کاری‌های آشکار وجود دارد. در ادامه به معرفی مهم‌ترین آژانس‌ها و دستگاه‌های کلیدی که بازتابی از تثبیت اولویت‌های دولت-حزب چین برای فضای سایبری هستند، می‌پردازیم.

۴-۱) کمیسیون مرکزی امنیت سایبری و توسعه جامعه اطلاعاتی[۱] (CCCI)

کمیسیون مرکزی امنیت سایبری و توسعه جامعه اطلاعاتی به ریاست اسمی شی جین‌پینگ و ریاست مشترک سایر اعضای کمیته دائمی دفتر سیاسی، بر کل فضای مجازی نظارت دارد. میزان ورود این کمیسیون به جزئیاتِ مسائل سیاستی روشن نیست؛ اما صِرف وجود آن باعث می‌شود که جنگ‌های بوروکراتیک در دید رهبری عالی کشور قرار گرفته و درنتیجه، انگیزه‌ها برای پیگیری و تشدید آن‌ها فروکش کند. همچنین این کمیسیون بستری برای حل اینگونه اختلافات به‌شیوه‌ای مقتدرانه فراهم می‌کند. نام‌گذاری این کمیسیون حاوی این پیام روشن است که امنیت یک ارزش فراگیر بوده و از «توسعه جامعه اطلاعاتی» جدایی‌پذیر نیست. همان‌طور که شی جین‌پینگ در نشست افتتاحیه کمیسیون در سال ۲۰۱۴ اعلام کرد: «امنیت سایبری و اطلاعات دو بال یک پرنده هستند... نه امنیت ملی بدون امنیت سایبری قابل‌تحقق است و نه مدرن‌سازی بدون توسعه جامعه اطلاعاتی».

۴-۲) اداره فضای مجازی چین[۲] (CAC)

این سازمان به‌عنوان نهاد پشتیبانِ «کمیسیون مرکزی امنیت سایبری و توسعه جامعه اطلاعاتی» که در آغاز شکل‌گیریِ خود وظیفه سانسور آنلاین را برعهده داشت، به‌خوبی مهیای برعهده‌گرفتن مجموعه‌ای از وظایف و اختیارات شده است؛ از نظارت بر نهادهای دولتی و نیمه‌دولتی گرفته تا هماهنگی‌های سیاستی و تنظیم‌گری. مسئولیت‌های این سازمان چندان متعین و دقیق نیست، اما جایگاه آن در صدر نظام سایبری کشور، منجر به گسترش تدریجی فعالیت‌های آن شده است. این سازمان در مسئولیت‌های تنظیم‌گرانه خود در هماهنگی با بوروکراسی‌های

۱. Central Commission for Cybersecurity and Informatization (CCCI)
۲. Cyberspace Administration of China (CAC)

خطی عمل می‌کند؛ اما برخلاف آن‌ها، ملزم به تبعیت از مکانیسم‌های پاسخگویی در برابر قوانین اداری چین، در مواردی مانند راه‌حل‌های قابل‌اجرا یا الزام به انتشار دلایل تصمیم‌ها، نیست. نمونه‌ای از گسترهٔ وسیع مسئولیت‌ها و صلاحیت‌های اداره فضای مجازی چین را می‌توان در یکی از فعالیت‌های نظارتی آن مشاهده کرد: درحال‌حاضر مدیریت سیستم نام دامنه[۱] در چین و اجرای «قانون حفاظت از اطلاعات شخصی»[۲] از طریق توسعه مقررات و استانداردهای فرعی را برعهده دارد و بررسی‌های امنیت سایبری در «زیرساخت‌های اطلاعاتی حیاتی»[۳]، مانند اپراتورها و ارائه‌دهندگان پلتفرم‌های اینترنتی[۴]، را انجام می‌دهد.

برطبق تعریف ناقصی که در قوانین و مقررات فعلی وجود دارد، «زیرساخت‌های اطلاعاتی حیاتی» عبارتند از زیرساخت‌های مهم شبکه و انواع سیستم‌های اطلاعاتی در صنایع و بخش‌های مهمی همچون مخابرات و خدمات اطلاعاتی، انرژی، حمل و نقل و غیره. آسیب‌دیدن، اختلال در عملکرد یا نشت اطلاعات در این بخش‌ها می‌تواند تبعاتی جدی برای امنیت ملی به‌همراه داشته باشد. خدماتی که شرکت‌های ارائه‌دهنده پلتفرم‌های اینترنتی در چین ارائه می‌دهند، با خدمات شرکت‌های آمریکایی مانند گوگل، آمازون و اوبر قابل‌مقایسه است. در کشور چین، طیفی از شرکت‌ها در این دسته می‌گنجند؛ از شرکت‌های خدمات‌دهنده نسبتاً کوچک گرفته تا کسب‌وکارهای گسترده، مانند علی‌بابا[۵] و تنسنت[۶]؛ این دستهٔ اخیر مشمول تعهدات قانونی متفاوتی هستند که در ادامه به آن‌ها خواهیم پرداخت.

۱. DNS
۲. The China Personal Information Protection Law (PIPL)
۳. critical information infrastructure (CII)
۴. internet platform providers (IPP)
۵. Alibaba
۶. Tencent

اداره فضای مجازی چین مسئول تنظیم مقررات صادرات اطلاعات شخصی به خارج از مرزهای چین و پیگیری «صورت‌بندی قواعد و استانداردهای ملموس و عینی حفاظت از اطلاعات شخصی» است. این نهاد همچنین بر توسعه «نظام‌های انتقال برون‌مرزی داده» نظارت می‌کند که در مناطق آزمایشی در سراسر چین به توسعه نوآورانه تجارتِ خدمات اختصاص یافته‌اند.

قانون جدید امنیت داده چین این سازمان را مسئول هماهنگی کلان در حوزه امنیت داده‌های شبکه و سایر فعالیت‌های تنظیم‌گرانهٔ مرتبط و همچنین طراحی اقدامات امنیتی در جهت حکمرانی صادرات «اطلاعات مهم» به خارج از مرزهای چین در همکاری با سایر سازمان‌ها کرده است. در کنار این مسئولیت‌ها، به نظر می‌رسد اداره فضای مجازی چین با برعهده‌گرفتن مسئولیت اصلی اجرای «برنامه پنج ساله ملی توسعه جامعه اطلاعاتی»[۱]، نقش خود را به‌عنوان نهاد هماهنگ‌کننده اصلی چین برای سیاست‌های مربوط به فضای سایبری تثبیت کرده است. این امر احتمالاً بیشتر مدیون ماهیت «دوگانهٔ» آن است؛ این سازمان به‌طور همزمان زیرمجموعه قوه مجریه چین و نیز حزب کمونیست این کشور محسوب می‌شود. ارتقاء کمیسیون مرکزی امنیت سایبری و توسعه جامعه اطلاعاتی به سطح «کمیسیون مرکزی» در سال ۲۰۱۸، جایگاه آن را مستقیماً ذیل کمیته مرکزی حزب کمونیست چین قرار داد. این نزدیکی به رهبران سطح بالای چین، احتمالاً بدین معنی است که اداره فضای مجازی (به‌عنوان دفتر اجرایی این کمیسیون) به‌عنوان محملی برای تحقق سیاست‌های حزب و ازاین‌جهت که بیش از ملاحظات تکنوکراتیک، به دیدگاه‌های رهبران سطح اول کشور اهمیت می‌دهد، مورد علاقه و توجه آنان قرار گرفته است.

۱. Five-Year Plan for National Informatization

باوجود انبوه کارکردهای عملی و فنی اداره فضای مجازی چین، همه مدیران این نهاد درعین‌حال نقش معاونت را در دپارتمان مرکزی پروپاگاندای حزب کمونیست چین برعهده داشته‌اند. این مسئله نشان می‌دهد که در خوانش رهبران این کشور از امنیت سایبری، فعالیت ایدئولوژیک همچنان جایگاهی محوری دارد. این نهاد تا سال ۲۰۱۴ نقش اداره پروپاگاندا را در مورد ارتباطات آنلاین برعهده داشته است. این امر نیز بازتابی از دیدگاه حزب در مورد اینترنت به‌عنوان میدان اصلی نبرد و جبهه اصلی در نبرد ایدئولوژیک علیه قدرت‌های خارجی و مخالفان داخلی است. اهتمام ایالات متحده آمریکا به تقویت «آزادی اینترنت» به‌عنوان یک اصل سیاستیِ بین‌المللی و نقش شبکه‌های اجتماعی در انقلاب‌های مشهور جهان عرب و کشورهای پساشوروی، باعث تشدید هراس رهبران چین از قابلیت‌های اینترنت در براندازی نظام‌های سیاسی شده است. نشر «انرژی مثبت»[۱] (که به‌معنای تفکر ایدئولوژیکِ درست است) در فضای سایبری چین یکی از درون‌مایه‌های واحدی است که به‌عنوان مثال، در مقررات جدید الگوریتم‌های توصیه[۲] به چشم می‌خورد.

۳-۴) وزارت صنعت و فناوری اطلاعات[۳] (MIIT)

اگرچه برخی از وظایف وزارت صنعت و فناوری اطلاعات به اداره فضای مجازی چین واگذار شده، اما این وزارتخانه همچنان نفوذ خود را بر بخش گسترده‌ای از عرصه فضای سایبری چین، ازجمله در ساخت شبکه‌های مخابراتی و اقدامات امنیتی مرتبط و همچنین اختیارات نظارتی بر سیستم نام دامنه، حفظ کرده است. این مرجعیت در حوزه زیرساخت‌های دیجیتال باعث می‌شود که وزارت صنعت و فناوری اطلاعات مسئول ارزیابی میزان تحقق بخش‌های مختلف فضای سایبری چین، به‌عنوان مثال از طریق توسعه اینترنت اشیاء و استانداردگذاری‌های فنیِ

۱. positive energy
۲. recommendation algorithms
۳. Ministry for Industry and Information Technology (MIIT)

مرتبط با آن، باشد. این وزارتخانه به‌همراه سایر سازمان‌های مربوط به حوزه امنیت عمومی در چین به‌طور مشترک اقدام به انتشار یک دفترچه راهنما در مورد آن دسته از محصولات حوزه آی‌سی‌تی می‌کند که بر طبق قانون امنیت سایبری[۱]، باید از طرف نهادهای مسئول مورد بازرسی قرار گرفته و گواهی امنیتی دریافت کنند. این وزارتخانه همچنین مسئول توسعه بسترهای اختصاصی داده در «مناطق آزمایشی تجاری خدمات نوآورانه» است. در این مناطق چارچوب‌های تبادل برون‌مرزی داده نسبت به سایر نقاط احتمالاً از محدودیت کمتری برخوردار هستند.

۴-۴) آکادمی فناوری اطلاعات و ارتباطات چین[۲] (CAICT)

آکادمی فناوری اطلاعات و ارتباطات یک سازمان تحقیقاتی وابسته به وزارت صنعت و فناوری اطلاعات کشور چین است. این سازمان نقش برجسته‌ای در شکل‌دادن به کاربردهای فناوری در فضای سایبری، ازجمله از طریق همکاری‌های بین‌المللی دارد. به‌عنوان مثال، یکی از دستورکارهای این آکادمی که در همکاری با اتحادیه صنایع هوش مصنوعی انجام می‌شود، ارزیابی و صدور مجوز برای سیستم‌های هوش مصنوعی است. همچنین این سازمان اخیراً شروع به صدور گواهی «هوش مصنوعی قابل‌اطمینان»[۳] برای نرم‌افزارهای تشخیص چهره[۴] کرده است. علاوه‌براین، این آکادمی نمایندهٔ پکن در معاهده‌ای است که میان چین و آلمان، در قالب طرح «صنعت ۴»[۵]، به‌ویژه در حوزه توسعه صنایع هوشمند، شکل گرفته است. درنهایت، آکادمی فناوری اطلاعات و ارتباطات چین توانسته است در داخل مرزهای این کشور یک سیستم حل‌مسئله دیجیتال را در حوزه اینترنت صنعتی راه‌اندازی کند.

۱. cybersecurity law (CSL)
۲. China Academy for Information and Communication Technologies (CAICT)
۳. trustworthy AI
۴. facial recognition software
۵. Industrie 4.0:
یک ابتکار ملی برای آلمان در زمینه هوشمندسازی فرایند تولید و تحقق کارخانه دیجیتال است.

۴-۵) کمیته فنی ملیِ استانداردسازی امنیت اطلاعات[۱] (TC۲۶۰)

آکادمی فناوری اطلاعات و ارتباطات صرفاً یکی از چندین نهاد فنی است که تمرکز خود را بر تخصص لازم برای صورت‌بندی سیاست‌ها، مقررات و استانداردهای فضای سایبری چین قرار داده است و به‌نحوی از انحاء با مجموعه دولت ارتباط دارد. کمیته فنی ملیِ استانداردسازی امنیت اطلاعات نمونه دیگری از اینگونه نهادها است که معاون اداره فضای مجازی چین در رأس آن قرار داشته و رهبران ارشد نهادهای مختلف را گرد هم آورده است؛ نهادهایی همچون وزارت صنعت و فناوری اطلاعات، وزارت امنیت عمومی، اداره رمزنگاری و اداره تنظیم مقررات بازار می‌باشد. در سیستم ساختارمند استانداردهای کشور چین، استانداردهای رسمی به روش‌های مختلف بر عملیاتی‌سازی و تنظیم‌گری فناوری تأثیر می‌گذارند. کمیته امنیت اطلاعات پیش‌نویس استانداردهایی را برای دستورالعمل‌های شناسایی «داده‌های مهم» (یک اصطلاح کلیدی که در قانون امنیت سایبری و قانون امنیت داده[۲] توضیحی در مورد آن داده نشده است) و به‌طور کلی طبقه‌بندی داده‌ها[۳] منتشر کرده است.

۴-۶) وزارت امنیت عمومی[۴] (MPS)

یکی دیگر از بازیگران کلیدی این عرصه، وزارت امنیت عمومی است که فرماندهی پلیس چین را بر عهده دارد. این وزارتخانه که پیشینه آن به سال ۱۹۹۴ بازمی‌گردد، بر سیستم حفاظت چندلایه[۵] چین نظارت می‌کند. این سیستم درواقع یک سطح‌بندی ملی برای امنیت اطلاعات است که الزامات امنیتی مختلفی را برای همه شبکه‌های دیجیتال تعیین می‌کند؛ الزاماتی که هرچه حساسیت اطلاعات بالاتر رود، بیشتر

۱. National Information Security Standardization Technical Committee (TC260)
۲. Data Security Law (DSL)
۳. data classification
۴. Ministry of Public Security (MPS)
۵. China's multi-level protection system

خواهند شد. وزارت امنیت عمومی برای اطمینان از پیرویِ سرویس‌های ارائه‌دهنده خدمات اینترنتی از این الزامات، امکان دسترسی فیزیکی یا از راه دور به سیستم‌های دیجیتال، کپی‌برداری از داده‌ها و درخواست ارائه توضیح در مورد نحوه پیکربندی سیستم‌ها را دارد.

علی‌رغم قدرت و نفوذ زیاد اداره فضای مجازی چین، همچنان وزارت امنیت عمومی نقش خود را به‌عنوان متولی اصلی عملیاتی‌سازی امنیت سایبری در چین، به‌ویژه برای زیرساخت‌های اطلاعاتی حیاتی، حفظ کرده است. قانون امنیت داده، در حوزه حکمرانی داده، با عبارت «اجرای وظایف نظارتی امنیت داده توسط مقامات امنیت عمومی»، وظیفه این وزارتخانه در رابطه با حکمرانی داده را به‌رسمیت‌شناخته است. به‌علاوه، این وزارتخانه بازرسی‌های دوره‌ای برای اجرای سیستم نظارتی فضای سایبری را رهبری می‌کند. در سال ۲۰۱۹ وزارت صنعت و فناوری اطلاعات، اداره فضای مجازی، وزارت امنیت عمومی و اداره تنظیم مقررات بازار، به‌همراه کمیته فنی ملیِ استانداردسازی امنیت اطلاعات و اتحادیه‌های صنعتی اقدام به تشکیل یک «کارگروه حکمرانی اپلیکیشن‌ها» نمودند که مسئول پیگرد و مجازات نقض قوانین حفاظت از اطلاعات شخصی بود.

۴-۷) وزارت امنیت کشور[۱] (MSS)

وزارت امنیت کشور، به‌عنوان سرویس اطلاعات و ضداطلاعات خارجی چین، یکی دیگر از بازیگران مهم اکوسیستم امنیت سایبری در این کشور است. در کنار وزارت امنیت عمومی، وزارت امنیت کشور نیز قادر به ارزیابی تیم‌های امنیت سایبری ثابتی است که همه اپراتورهای زیرساخت‌های اطلاعاتی حیاتی ملزم به تشکیل آن‌ها هستند. این وزارتخانه با «مرکز ارزیابی امنیت فناوری اطلاعات چین»[۲] مرتبط

۱. Ministry of State Security (MSS)
۲. China Information Technology Security Evaluation Centre (CNITSEC)

است که پایگاه داده آسیب‌پذیری ملی چین برای امنیت اطلاعات را مدیریت می‌کند و آزمایش آسیب‌پذیری نرم‌افزارها را انجام می‌دهد. در سال ۲۰۰۳، مایکروسافت به این مرکز دسترسی محدودی به کد منبع ویندوز برای چنین آزمایشی داد. محققان حدس می‌زنند ممکن است این مرکز به وزارت امنیت کشور در توسعه قابلیت‌های بهره‌برداری از شبکه کامپیوتری کمک کرده باشد. در سال ۲۰۲۱، ایالات‌متحده و دولت‌های هم‌پیمان آن، وزارت امنیت کشور چین را متهم به مشارکت در بهره‌برداری از شبکه کامپیوتری بین‌المللی برای اهداف تجاری کردند.

۴-۸) وزارت امور خارجه[1] (MFA)

اینگونه به‌نظر می‌رسد که وزارت امور خارجه جایگاه خود را به‌عنوان نماینده کشور برای تعامل با مخاطب خارجی در حوزه دیپلماسی سایبری تعریف کرده است؛ البته این وزارتخانه تا چندی پیش مجبور بود با مداخلات مستقیم اداره فضای مجازی چین در گفتگوهای بین‌المللی مقابله کند. وزارت امور خارجه یک بخش اختصاصی برای مدیریت دیپلماسی سایبری را، به‌عنوان بدیل اداره «هماهنگ‌کننده امور سایبری وزارت امور خارجه ایالات‌متحده»[2]، تأسیس کرده است. همچنین این وزارتخانه مشارکت کشور در فرایندهای گفتگوی سازمان ملل برای توسعه هنجارهای بین‌المللی فضای سایبری را رهبری کرده و نهادهای تخصصی مرتبط با این حوزه را توسعه داده است.

۱. Ministry of Foreign Affairs (MFA)
۲. US State Department's Coordinator for Cyber Issues

۴-۹) ارتش آزادی‌بخش خلق[۱] (PLA)

در اینجا باید از ارتش چین هم یاد کنیم. «داده‌های ارتش» از محدوده قانون امنیت داده مستثنی هستند و این یعنی ارتش آزادی‌بخش خلق ملزم به پیروی از تعهدات مدیریت داده که اکثر بازیگرانِ این عرصه از آن‌ها تبعیت می‌کنند، نیست. بااین‌حال، نماینده ارتش در «کمیسیون مرکزی امنیت سایبری و توسعه جامعه اطلاعاتی» حضور دارد و او کسی نیست به‌جز «زو کیلیانگ»[۲]، رئیس ستاد کل و نایب رئیس کمیسیون نظامی مرکزی و معاون «شی جین‌پینگ»[۳] در امور نظامی. بهره‌برداری نظامی از فضای سایبری احتمالاً در درجه نخست توسط واحد پشتیبانی راهبردی ارتش و کمیسیون امنیت ملی، به ریاست «شی جین‌پینگ»، مدیریت می‌شود.

۱. People's Liberation Army (PLA)
۲. Xu Qiliang
۳. Xi Jinping

۵) نظام تنظیم‌گری فضای سایبری در چین

ایجاد یک سیستم جامع برای رصد و شکل‌دهی به فعالیت‌ها

نظام حکمرانی فضای سایبری چین اکنون بر پایه سه قانون «امنیت داده»، «امنیت سایبری» و «حفاظت از اطلاعات شخصی» استوار است. این سه قانون چارچوبی برای مجموعه‌ای از اقدامات جدید فراهم می‌کنند که بیش‌از هر زمان دیگری بر مدیریت داده‌ها، تنظیم‌گری برخی فعالیت‌های خاص و بخش‌های اقتصادی متمرکز شده‌اند. نظام تنظیم‌گری چین هم مانند ساختار نهادیِ این حوزه که پیش‌ازاین توضیح دادیم، سرشار از اصطلاحات مبهم و هم‌پوشانی در وظایف است. بااین‌وجود، چین اکنون دارای جامع‌ترین سیستم اعمال نظارت، کنترل و شکل‌دهی به فعالیت‌ها در فضای سایبری توسط حکومت است. حکومت در مسیر انجام این وظایف بعضاً از بازیگران خارجی در داخل مرزهای کشور بهره می‌برد. این نظام به‌گونه‌ای طراحی شده است که همزمان از منافع شهروندان و منافع عمومی، معرفی‌شده توسط دولت-

حزب، حفاظت کرده و درعین‌حال از حداکثر پتانسیل فضای سایبری برای ارتقای توسعه اقتصادی بهره ببرد.

اقدام بحث‌برانگیز اخیر چین در سرکوب شرکت‌های فناوری اینترنتی این کشور نیز، با توجه به مقیاس محدود آن و تلاشی که برای کنترل آسیب‌های اجتماعی جدیِ اقدامات آن‌ها انجام داد، آشکارا در همین چارچوب قرار می‌گیرد. تقریباً همه اقدامات تنبیهی در این ماجرا بر آن دسته از فعالیت‌های بزرگ‌ترین پلتفرم‌های اینترنتی اِعمال شد که دارای تبعات اجتماعی منفی پنداشته می‌شدند. اینگونه اقدامات می‌توانند همزمان اهداف سیاسی و مقاصد تکنوکراتیک داشته باشند. به‌عنوان مثال، جریمه شرکت علی‌بابا، شرکت ANT و مدیر پیشین علی‌بابا، یعنی جک ما که بعد از سخنرانی عمومی او و انتقاد آشکار از نهادهای تنظیم‌گر حکومتی انجام شد، به‌وضوح هشداری به دیگران در مورد به‌چالش‌کشیدن اقتدار دولت-حزب بود. بااین‌حال، اقدامات تنظیم‌گرانه‌ای که نسبت به شرکت ANT انجام شد، احتمالاً همزمان به‌دنبال کاهش میزان ریسکی بوده‌اند که به بازارهای مالی و اوراق قرضه چین وارد می‌شده است. به‌طورکلی بسیاری از اقدامات تنظیم‌گرانه، رفتار انحصارطلبانه در حوزه فناوری‌های اینترنتی را هدف قرار می‌دهند.

۵-۱) قانون امنیت سایبری[۱]: قواعد بنیادی در راستای تأمین امنیت فضای مجازی

قانون امنیت سایبری که در سال ۲۰۱۷ تصویب شد، همه اپراتورها را ملزم به پیروی از «سیستم حفاظت چندسطحی»[۲] و اجرای تمهیداتی همچون ایجاد سیستم مدیریت امنیت داخلی، اقدامات امنیتی فنی و آموزش امنیت سایبری می‌کند. بر طبق ماده ۲۸ این قانون، اپراتورهای شبکه باید «پشتیبانی و کمک فنی به نهادهای امنیت

۱. Cybersecurity Law (CSL)
۲. multi-level protection system (MLPS)

عمومی و امنیت ملی ارائه کنند». این ماده قانونی، باعث ایجاد نگرانی کشورهای خارجی پیرامون جاسوسی کشور چین و نقش بالقوه ارائه‌دهندگان خدمات فناوری اطلاعات و ارتباطات چینی مانند هوآوی شده است. طی این قانون وظایفی بر ارائه‌دهندگان خدمات فناوری اطلاعات و ارتباطات تحمیل شده که عبارتند از:

- رعایت اجباری گواهینامه امنیتی؛
- بازرسی توسط مقامات ایالتی در مورد دسته‌های خاصی از تجهیزات و محصولات؛
- الزام کاربران به ارائه اطلاعات هویتی واقعی؛
- تدوین طرح‌های واکنش اضطراری برای حوادث امنیت سایبری.

همچنین ماده ۳۵ این قانون اعلام می‌کند اپراتورهای «زیرساخت‌های اطلاعاتی حیاتی» که محصولات و خدمات شبکه را استفاده می‌کنند و ممکن است بر امنیت ملی تأثیر بگذارند، ملزم به پذیرش بررسی‌های امنیت سایبری از طرف «اداره فضای مجازی چین» و دیگر سازمان‌های مرتبط هستند. بر طبق این ماده، مقامات چینی ورود پلتفرم Didi Chuxing در فهرست بورس نیویورک در سال ۲۰۲۱ را امری مشکل‌ساز تلقی می‌کنند. مفهوم «بررسی امنیت سایبری» که در ماده ۳۵ قانون امنیت سایبری آمده است، اکنون با مقررات بعدی به طیف گسترده‌ای از موقعیت‌ها گسترش یافته که در ادامه توضیحات مربوط به آن در خود قانون قابل مطالعه است.

ماده ۳۷ قانون امنیت سایبری دستور می‌دهد که «اطلاعات شخصی» و «داده‌های مهم» که توسط اپراتورهای زیرساخت‌های اطلاعاتی حیاتی در قلمرو سرزمینی چین جمع‌آوری یا تولید شده‌اند، باید در داخل مرزهای چین ذخیره گردند. همچنین صادرات این داده‌ها منوط به ارزیابی امنیتی توسط «اداره فضای مجازی چین» و آژانس‌های مربوطه است. با توجه به اینکه این قانون تعریفی از اصطلاحات «اطلاعات

شخصی»، «داده‌های مهم» و «اپراتورهای زیرساخت‌های اطلاعاتی حیاتی» ارائه نکرده است، الزامات مربوط به بومی‌سازی داده‌ها و کنترل صادرات آن‌ها تبدیل به مانعی در برابر تبعیت بازیگران خارجی از این قانون شده است. البته این اصطلاحات اخیراً در مقررات و استانداردهای جدیدتر چین وضوح بیشتری پیدا کرده‌اند.

برای مثال، تعریف و وظایف اپراتورهای زیرساخت‌های اطلاعاتی حیاتی توسط «مقررات حفاظت امنیتی از زیرساخت اطلاعاتی حیاتی»[۱] که در سپتامبر ۲۰۲۱ به اجرا درآمد، توضیح داده شد. بر طبق این مقررات، مسئولیت «هدایت و نظارت» جهت حفاظت از زیرساخت‌های اطلاعاتی حیاتی به وزارت امنیت عمومی تحت هماهنگی کلی با «اداره فضای مجازی چین» محول شده است؛ اما این تقسیم‌کار قادر به حل منازعات بوروکراتیک چین نبوده است. نکتهٔ دیگر در همین مورد این است که «مقررات حفاظت امنیتی از زیرساخت‌های اطلاعاتی حیاتی» رابطه مقررات جدید در خصوص «نظام حفاظتی زیرساخت‌های اطلاعاتی حیاتی» با «نظام حفاظتی چندسطحی» را روشن نکرده است.

بااین‌حال، «مقررات حفاظت از زیرساخت‌های اطلاعاتی حیاتی» سیستمی از اقدامات را برای شناسایی و ایمن‌سازی این نوع زیرساخت‌ها ارائه کرده که بسیار فراتر از چیزی است که تاکنون توسط اتحادیه اروپا و ایالات‌متحده انجام شده است. سازمان‌های دولتی ملزم به تدوین قواعدی برای شناسایی زیرساخت‌های اطلاعاتی حیاتی در صنعت هستند تا اپراتورهای شناسایی‌شده را نسبت به وظایف خود مطلع نمایند. این اپراتورها بایستی تعهداتی شامل گزارش حوادث امنیت سایبری یا شناسایی تهدیدات برای اداره فضای مجازی و وزارت امنیت عمومی، انجام ارزیابی ریسک سالانه «زیرساخت‌های اطلاعاتی حیاتی» و ایجاد نهادهای مدیریت امنیتی اختصاصی با پرسنل مورد تأیید وزارت امنیت عمومی و وزارت امنیت کشور را رعایت کنند.

۱. Critical Information Infrastructure Security Protection Regulations (CIISPR)

در ژانویه ۲۰۲۲، «اداره فضای مجازی چین» نسخه نهایی «اقدامات بررسی امنیت سایبری»[۱] را صادر کرد که در ماه بعد از آن اجرایی شد. این سند، دامنه ماده ۳۵ قانون امنیت سایبری را به‌نحوی گسترش داد که فعالیت‌های ارائه‌دهندگان پلتفرم‌های اینترنتی[۲]، مانند ارائه‌دهندگان سوپراپلیکیشن‌های چین (برای مثال علی‌بابا و تنسنت)، را نیز در بر بگیرد. ارائه‌دهندگان پلتفرم‌های اینترنتی که اطلاعات شخصی بیش از یک میلیون کاربر را در اختیار دارند و قصد دارند در بورس‌های خارجی عرضه شوند، بر طبق مقررات جدید باید مورد بررسی قرار گیرند.

۲-۵) قانون امنیت داده[۳]: چارچوبی جامع برای تنظیم‌گری داده‌ها

«قانون امنیت داده» در سپتامبر ۲۰۲۱ اجرایی شد. این قانون یک چارچوب تنظیم‌گری جامع برای داده‌ها، به‌استثنای داده‌های مربوط به اسرار دولتی و نظامی، است که امنیت ملی و توسعه اجتماعی را در اولویت کار خود قرار داده است. دایره هدف قانون امنیت داده شامل فعالیت‌های مربوط به مدیریت داده در قلمرو سرزمینی این کشور است؛ فعالیت‌هایی که در این قانون با عباراتی مانند «جمع‌آوری، ذخیره‌سازی، استفاده، پردازش، انتقال، ارائه، افشا و غیره» توصیف شده‌اند. داده‌های مشمول این قانون شامل «هرگونه اطلاعات به اشکال الکترونیکی یا دیگر اشکال» می‌شود. اگرچه محتوای قانون امنیت داده در جهت ایمن‌سازی داده‌هاست؛ اما با ایجاد چارچوبی نهادی، سعی در استفاده از داده‌ها به‌عنوان عاملی برای تولید و توسعه دارد.

۱. Cybersecurity Review Measures (CRM)
۲. internet platform providers (IPPs)
۳. Data Security Law (DSL)

«قانون امنیت داده» دولت را ملزم به طراحی یک سیستم طبقه‌بندی و درجه‌بندی‌شده برای حفاظت از داده‌ها با توجه به «درجه اهمیت آن در توسعه اقتصادی و اجتماعی» می‌کند. این امر مستلزم ایجاد سازوکارهای جداگانه برای ارزیابی ریسک، نظارت، اشتراک‌گذاری اطلاعات و هشدار اولیه است. بخشی از این اقدامات نظارتی با چارچوب «اقدامات بررسی امنیت سایبری» که در بخش قبل توضیح داده شد، مطابقت دارد. سازمان‌های دولتی بایستی فهرستی از «داده‌های مهم» را در حوزه‌های مسئولیت خود ایجاد کنند. تمرکززدایی از تعریف «داده‌های مهم» مزیت دیگری دارد که به‌طور بالقوه جنگ‌های بوروکراتیک بر سر این موضوع را کاهش خواهد داد. در ژانویه ۲۰۲۲، «کمیته فنی ملیِ استانداردسازی امنیت اطلاعات»[۱] استاندارد جداگانه‌ای پیرامون «الزامات امنیتی برای مدیریت داده‌های مهم»[۲] را در دست توسعه داشت. در این استاندارد جدید، برای شناسایی داده‌های مهم بر پیامدهای سوءاستفاده از داده‌ها به‌جای نوع داده‌ی درحال پردازش تأکید شده است.

قانون امنیت داده دسته‌ای از «داده‌های ملی مهم» را معرفی می‌کند که براساس «امنیت ملی» و «منافع عمومی» تعریف شده‌اند و باید مشمول یک سیستم مدیریت سخت‌گیرانه‌تر شوند. این قانون همچنین بخشی را به داده‌های دولتی اختصاص می‌دهد که نه فقط بر اقدامات امنیتی بلکه بر حفاظت از حقوق و باز بودن داده‌ها برای استفاده در خدمات توسعه اقتصادی و اجتماعی تأکید دارد.

علاوه‌بر موارد فوق، این قانون سازمان‌های دولتی را ملزم به تشکیل «سیستم‌های مدیریت تراکنش داده‌ها، استانداردکردن تراکنش داده‌ها و ایجاد بازار مبادلات داده» نیز می‌کند. این فرایندها مکمل مراقبت‌های «قانون حفاظت از اطلاعات شخصی» در تلاش برای تنظیم‌گری بازار سیاه عظیم اطلاعات شخصی در چین و آسیب‌های

۱. TC260
۲. Security Requirements for Handling of Important Data

اجتماعی حاصل از آن است. آن‌ها همچنین درحال پیگیریِ اقدامات سازمانی و فرهنگی مداومی هستند که مانع از اشتراک‌گذاری داده‌ها در چین، حتی توسط شرکت‌های پیشرو، می‌شود. برخی برآوردها حاکی از این است که چین یک‌چهارم داده‌های جهان را تا سال ۲۰۲۵ تولید خواهد کرد. قانون امنیت داده با الزام دولت به حمایت از اقدامات مربوط به استانداردسازی داده، تحقیق، آموزش، نوآوری و توسعه زیرساخت، تمرکز و انسجام بوروکراتیک را برای بهره‌برداری از این منبع افزایش می‌دهد. این مقررات از مداخلات دولتی برای بهینه‌سازی بازار پشتیبانی می‌کند؛ مداخلاتی که اکنون شامل یک پلتفرم ملی اشتراک‌گذاری داده است.

قانون امنیت داده اجرای یک سیستم کنترل صادرات داده را هدایت می‌کند؛ اگرچه رابطه آن با «اقدامات بررسی امنیت سایبری» و یا «قانون کنترل صادرات یکپارچه چین» در سال ۲۰۲۱ همچنان نامشخص است. قانون امنیت داده ارائه داده‌ها به مقامات خارجی را با شرایطی مشابه «قانون حفاظت از اطلاعات شخصی» محدود می‌کند؛ اما صلاحیت فراسرزمینی «قانون امنیت داده» نسبت به «قانون حفاظت از اطلاعات شخصی» گسترده‌تر بوده و فعالیت‌های مربوط به پردازش داده‌ها در خارج از قلمرو چین که به امنیت ملی، منافع عمومی یا حقوق شهروندان یا سازمان‌های جمهوری خلق چین آسیب می‌زند، را نیز پوشش می‌دهد.

با انتشار پیش‌نویس «مقررات مدیریت امنیت داده‌های آنلاین»[۱] در نوامبر ۲۰۲۱، برخی از مقررات موجود در قانون امنیت داده وضوح بیشتری پیدا کرد. در این پیش‌نویس، فعالیت‌های ممنوع برای کنترل‌کنندگان داده[۲] فهرست شده و از کنترل‌کنندگان «داده‌های مهم» می‌خواهد که یک نهاد داخلی برای مدیریت امنیت

۱. Online Data Security Management Regulations (ODSMR)

۲. data handlers
این عبارت معادل همان کنترل‌گر داده (data controller) در قوانین اتحادیه اروپا است؛ اما در اینجا برای ایجاد تمایز به کنترل‌کنندگان داده ترجمه شده است.

داده با وظایف معین، مانند ارسال گزارش به مقامات محلی حاوی محتوای مشخص از جمله روش‌ها و مکان ذخیره‌سازی داده‌های مهم، ایجاد کنند.

پیش‌نویس «مقررات مدیریت امنیت داده‌های آنلاین» گستره ماده ۳۵ قانون امنیت سایبری را توسعه داده و بررسی امنیت سایبری را در شرایط زیر الزامی کرده است:

- در مواردی که اپراتورهای پلتفرم‌های اینترنتی، حجم زیادی از منابع داده مربوط به امنیت ملی، توسعه اقتصادی یا منافع عمومی را جمع‌آوری یا نگهداری کنند و یا داده‌هایی که به‌صورت قطعی یا احتمالی بر امنیت ملی تأثیرگذار هستند را ادغام، سازماندهی مجدد یا جداسازی کنند؛
- مواردی که کنترل‌کنندگان داده اطلاعات شخصی بیش از یک میلیون نفر را در اختیار گرفته و در بازارهای خارج از کشور عرضه کنند؛
- مواردی که کنترل‌کنندگان داده در هنگ‌کنگ ثبت می‌شوند و بر امنیت ملی به‌صورت قطعی یا احتمالی تأثیرگذار هستند؛
- سایر فعالیت‌های کنترل‌کنندگان داده که به‌صورت قطعی یا احتمالی بر امنیت ملی تأثیرگذار هستند.

علاوه‌براین، پیش‌نویس «مقررات مدیریت امنیت داده‌های آنلاین» دارای صلاحیت فراسرزمینی گسترده‌ای است و بر فعالیت‌هایی که در خارج از کشور چین در حوزه

کنترل داده‌های شهروندان یا سازمان‌های چینی انجام می‌شود نیز اِعمال می‌شود؛ البته فعالیت‌هایی که واجد این ویژگی‌ها باشند:

- شامل داده‌های مهم در کشور چین باشند؛
- به‌منظور ارائه خدمات یا محصولات در چین استفاده شده باشند؛
- رفتار افراد یا سازمان‌های مستقر در چین را تجزیه و تحلیل کرده باشند؛
- مشمول سایر قوانین و مقررات اداری چین شده باشند.

۵-۳) قانون حفاظت از اطلاعات شخصی[۱]: کنترل سوءاستفاده از اطلاعات شخصی

قانون حفاظت از اطلاعات شخصی نتیجه تحول آهسته چین از مقررات بخشی و تکه‌تکه در حوزه حفاظت از داده‌ها، به‌سوی نظامی فراگیر است که اطلاعات شخصی را به‌منزله موضوعی منحصربه‌فرد و مستقل، مقررات‌گذاری می‌کند. این قانون در پاسخ به تقاضای همگانی در چین برای حفاظت مؤثرتر از داده‌های شخصی در مواجهه با سوءاستفاده‌های گسترده از سوی بازیگران غیردولتی شکل گرفته است. تدوین این قانون نشانهٔ شناخت بین‌المللی از اهمیت این موضوع و توجه به گسترش روزافزون موارد مشابه در مقررات کشورهای دیگر، به‌ویژه مقررات عمومی حفاظت از داده[۲] اتحادیه اروپا، بوده است.

مدیریت اطلاعات شخصی «اشخاص حقیقی» درون مرزهای چین در ذیل قانون حفاظت از اطلاعات شخصی قرار می‌گیرد. این قانون بین «data handlers» و

۱. Personal Information Protection Law (PIPL)
۲. GDPR

«entrusted persons»، تقریباً مشابه «کنترل‌گران داده»[۱] و «پردازش‌گران داده»[۲] مندرج در «مقررات عمومی حفاظت از داده اروپا»، تمایز قائل می‌شود. قانون حفاظت از اطلاعات شخصی، مشابه مقررات عمومی حفاظت از داده‌ها، در قبال فعالیت‌های خارج از چین که هدف آن‌ها ارائه محصولات یا خدمات به اشخاص حقیقی داخل چین یا انجام فعالیت‌های تحلیلی و سنجشی درمورد اشخاص حقیقی داخل چین است، مدعی صلاحیت قضایی برون‌مرزی است. الزامات بومی‌سازی داده‌ها برای اطلاعات شخصی در ماده ۳۷ قانون امنیت سایبری به آستانه‌های کمّی مرتبط شده‌اند که باید از سوی اداره فضای مجازی چین مشخص شوند، درحالی‌که نهادهای دولتیِ کنترل‌کننده اطلاعات شخصی، باید آن‌ها را داخل چین ذخیره کنند. در ادامه، مواد قانون حفاظت از اطلاعات شخصی درباره صادرات داده‌های فرامرزی را مرور می‌کنیم.

این قانون به‌جای تدوین حقوق اساسی یا اصول کلی قانونی، اقدام به تنظیم‌گری طبقات کنشگران و روابط آن‌ها بر مبنای قضاوت خود در مورد خطرات و صدمات احتمالی می‌کند. قانون حفاظت از اطلاعات شخصی علاوه‌بر رضایت افراد، طیفی از دلایل قانونی برای کنترل اطلاعات شخصی، نظیر «مبانی قراردادی» و «انجام تکالیف و مسئولیت‌های قانونی» را به رسمیت می‌شناسد. برای کنترل‌کنندگان اطلاعات شخصی الزامی کلی وجود دارد تا افراد را پیشاپیش از برخی جزئیات، به‌ویژه هدف و روش‌های کنترل اطلاعات، مطلع کنند. اپراتورهای پلتفرم‌های بزرگ عهده‌دار تکالیف دیگری هم هستند؛ این در حالی است که سازمان‌های دولتی وظیفه تدوین قواعد و استانداردهای تخصصی (و احتمالاً نه‌چندان چالش‌برانگیز) کنترل‌کنندگان اطلاعات شخصی با مقیاس کوچک را بر عهده دارند. قانون حفاظت از اطلاعات شخصی مواد

۱. data controllers
۲. data processors

خاصی برای کنترل اطلاعات شخصی از سوی نهادهای دولتی دارد که عموماً منوط به وظایف جهان‌شمول هستند.

میزان عملی‌بودن الزامات این قانون در برابر کارگزاران دولتی، بستگی دارد به اینکه آیا چین از «دوگانگی بین محرمانگی بازیگران بخش خصوصی و محرمانگی دولت» دور می‌شود یا خیر. نهادهای دولتیِ کنترل‌کننده اطلاعات شخصی، مشمول مقررات قانونی و در حیطه مسئولیت‌های آن‌ها قرار می‌گیرند و به افراد حق اقامه دعوی در مورد نقض حقوق از سوی کنترل‌کنندگان اطلاعات شخصی داده می‌شود. قانون حفاظت از اطلاعات شخصی، برخلاف مقررات عمومی حفاظت از داده‌ها در اتحادیه اروپا، هیچ ناظر مستقلی برای حفاظت از داده‌ها ایجاد نمی‌کند؛ بلکه همچنان اداره فضای مجازی چین درباره مواد این قانون، هم اختیار سیاست‌گذاری و هم اختیار نظارت دارد.

بعضی از اقدامات حفاظتی و اجرایی قانون مذکور به طرز چشمگیری فراتر از مقررات عمومی حفاظت از داده در اتحادیه اروپا هستند. به‌خصوص الزامات رضایت[۱] قانون حفاظت از اطلاعات شخصی چین بسیار چالش‌برانگیزتر از الزامات رضایت مقررات عمومی حفاظت از داده در اروپا هستند. قانون حفاظت از اطلاعات شخصی در تعریف «اطلاعات شخصی حساسِ» مشمول محافظت‌های اضافی، رویکردی مبتنی بر ریسک را اتخاذ می‌کند که گسترده‌تر از مشابه آن در مقررات عمومی حفاظت از داده در سایر کشورها است. جریمه‌های عدم رعایت قانون مذکور شامل مجازات شخصی مدیران شرکت و جریمه‌های مالی تا پنج درصد سود سالانه شرکت‌ها می‌شوند.

۱. consent requirements

۵-۴) به‌سوی نظامی مداخله‌گر برای کنترل انتقال داده فرامرزی

در ژوئیه سال ۲۰۲۲، «اداره فضای مجازی چین» نسخه نهایی «اقدامات ارزیابی امنیتی انتقال داده به خارج»[۱] را منتشر کرد. این رهنمود که از اول سپتامبر ۲۰۲۲ اجرایی می‌شود، برای فعالیت‌های انتقال داده فرامرزیِ باقیمانده‌ای که باید با مفاد سند فوق انطباق پیدا کنند، شش ماه دوره مهلت در نظر گرفته است. مفاد اقدامات مذکور تعهدات مربوط به ارسال داده به خارج از چین در کل «قانون امنیت سایبری»، «قانون امنیت داده» و «قانون حفاظت از اطلاعات شخصی» را یکپارچه و تلفیق می‌کند. مفاد این سند، همه کنترل‌کنندگان داده‌ها را ملزم می‌کند تا برای هرگونه انتقال برون‌مرزی داده، ارزیابی خودشان از رعایت قوانین را به اجرا درآورند. مطابق ماده ۳۵ قانون امنیت سایبری، تبادلات برون‌مرزی در چهار حالت مشمول تعهد دیگری برای بررسی امنیت سایبری از سوی دولت هم خواهند بود:

- جایی که کنترل‌کنندگان داده اقدام به ارائه داده‌های مهمی به خارج از کشور کنند؛
- اپراتورهای زیرساخت‌های اطلاعاتی حیاتی و کنترل‌کنندگان داده که اطلاعات شخصی بیش از یک میلیون نفر را کنترل کرده و اقدام به ارائه اطلاعات شخصی به خارج از کشور کنند؛
- کنترل‌کنندگان داده اقدام به ارائه اطلاعات شخصی بیش از ۱۰۰٫۰۰۰ نفر یا اطلاعات شخصی حساس بیش از ۱۰٫۰۰۰ نفر از اول ماه ژانویه سال قبل به خارج از کشور کرده باشند؛
- سایر شرایطی که اداره فضای مجازی چین ارزیابی امنیت انتقال داده در آن‌ها را الزامی کرده باشد.

۱. Outbound Data Transfer Security Assessment Measures (ODTSAM)

«اقدامات ارزیابی امنیتی انتقال داده به خارج»، ابهام موجود در مفاد فوق پیرامون مشخص کردن «اپراتورهای زیرساخت‌های اطلاعاتیِ حیاتی» و «داده‌های مهم» را برطرف نمی‌کند. رهنمود مذکور اصطلاحات «ارائه به خارج از کشور» یا «صادرات داده» که نیازمند بررسی امنیت سایبری هستند، را نیز شفاف‌سازی نمی‌کند. «اقدامات ارزیابی امنیتی انتقال داده به خارج» برای طبقه «داده‌های ملی مهم» که در قانون امنیت داده ارائه شده است، نیز به مرجعی استناد نمی‌کند. بااین‌حال، «اقدامات ارزیابی امنیتی انتقال داده به خارج» معیارهای اصلی حاکم بر بررسی امنیت سایبری را هم فهرست می‌کند؛ معیارهایی که به‌خصوص شامل محیط امنیت سایبری (ازجمله سیاست‌ها و مقررات) کشور یا ناحیه است که طرف دریافت‌کننده در آن قرار دارد. فهرست مذکور این موضوع را نیز دربرمی‌گیرد که آیا تصریح مسئولان امنیت داده‌ها در قرارداد میان کنترل‌کنندگان داده و طرف دریافت‌کننده صورت می‌گیرد یا خیر. محتوای چنین قراردادهایی نیز تشریح شده و دارای اهمیت است؛ این قراردادها در واقع چارچوب‌های زمانی و دوره‌های اعتبار بررسی‌های امنیت سایبری را مشخص کرده و شرایطی را برای ارزیابی‌های مجدد تعیین می‌کنند.

علاوه‌براین قانون حفاظت از اطلاعات شخصی موضوعات دیگری را راجع به انتقال برون‌مرزی اطلاعات شخصی ارائه می‌کند:

- «گواهی در حال انجام حفاظت از اطلاعات شخصی» تحت قواعدی که باید صادر شوند؛
- استفاده از «قرارداد استاندارد انتقال فرامرزی اطلاعات شخصی» که باید از سوی اداره فضای مجازی چین تدوین شود؛
- شرایط بیان‌شده توسط قراردادهای بین‌المللیِ پذیرفته‌شده از سوی چین.

معیار آخر احتمالاً نشانه‌ای از قصد مذاکره چین در مورد توافق‌نامه‌های انتقال فرامرزی داده با حوزه‌های قضایی خارجی است که با چین در راستای پیوستن به معاهدات تجاری چندجانبه موجود (معاهداتی که با جریان‌های فرامرزی داده سروکار دارند) هماهنگ است. بدون تأیید مقامات چینی و حتی در صورت الزام معاهده‌ای بین‌المللی، امکان ارسال اطلاعات شخصی ذخیره‌شده در چین به نهادهای قضایی خارجی یا مجریان قانون خارجی وجود ندارد. در مورد معیار دوم، اداره فضای مجازی چین در ژوئیه سال ۲۰۲۲ پیش‌نویس «قرارداد استاندارد انتقال فرامرزی اطلاعات شخصی» را برای اظهارنظر دولت منتشر کرد.

این قواعد بار سنگینی را بر دوش نهادهایی که به دنبال انتقال منظم داده‌ها به خارج از چین هستند، می‌گذارد. با توجه به چارچوب بحث‌های مقامات چینی پیرامون تعادل مطلوب بین توسعه جامعه اطلاعاتی و امنیت، به نظر می‌رسد که نظام نوظهور انتقال فرامرزیِ داده، به مورد دوم یعنی امنیت، گرایش بیشتری دارد. توافق‌هایی که در آینده برای تسهیل فعالیت اقتصادی فرامرزی شکل بگیرد، احتمالاً به‌جای کنارگذاشتنِ این الزامات عمومی، بیشتر در قالب تدارک برخی مقررات خاص برای آن دسته از شهرهای چین نمود پیدا خواهد کرد که از لحاظ فناوری پیشرفته‌تر و از نظر بین‌المللی متصل‌تر هستند. چندین حوزه قضایی محلی در چارچوب یک برنامه آزمایشی مداوم برای توسعه تجارت در خدمات نوآورانه در مکان‌های منتخب سراسر چین، رژیم‌های انتقال داده برون‌مرزی محدود را آزمایش می‌کنند. فراتر از این نظام‌های محدود منطقه‌ای، به نظر می‌رسد نظام حقوقی ملی، درمورد حجم بزرگی از اطلاعات شخصی یا «داده‌های مهم» (مطابق تعریف مقامات دولتی)، به شکل روزافزونی به سمت بومی‌سازی اجباری و مؤثر داده‌ها در داخل مرزهای چین، جهت‌دهی می‌شود.

پایان

زاویه

نگاهی نو،
به حکمرانی فضای مجازی

نشانی: تهران، ضلع غربی میدان فلسطین، خیابان آیت‌الله طالقانی، پلاک ۳۹۷
تلفن: ۸۶۰۵۴۲۹۱-۰۲۱
وبسایت: www.zaviehmag.ir
شبکه‌های اجتماعی: @zaviehmag