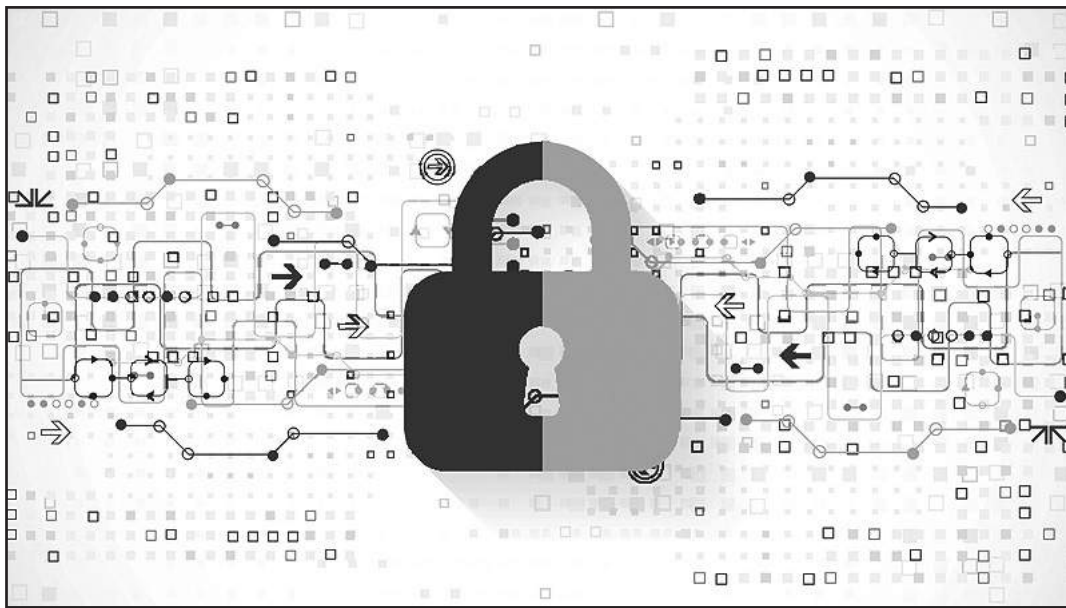


# وضعیت نظارت بر فضای مجازی

## در کشورهای جهان\*



### اشاره

موضوع نظارت بر فضای مجازی که بارها در فرمایش‌ها و سخنان حکیمانه رهبر معظم انقلاب و نیز متخصصان و دست‌اندرکاران این حوزه، مورد توجه و تأکید قرار گرفته، از مباحث مهم و کلیدی در حوزه فناوری اطلاعات و ارتباطات است و تمام کشورهایی که وارد این عرصه می‌شوند، ناچارند که بر فضای مجازی نظارتی حساب‌شده داشته باشند تا در سایه آن، هم از فواید این حوزه بهره‌مند شوند و هم بدنه اجتماعی و فرهنگی خویش را از آسیب‌های این فضای مواج حفظ کنند. نظر به اهمیت این مسئله، مناسب دیدیم نگاهی به وضعیت این مقوله در کشورهای مختلف جهان داشته باشیم و آنگاه ضرورت توجه به این موضوع را در کشور خودمان نیز یادآور شویم.

نوشتار حاضر، با استفاده از برخی منابع و مقالات موجود در فضای مجازی که در این باره به نگارش درآمده است، تهیه و تدوین داده شده که امید است مورد استفاده علاقه‌مندان و خوانندگان عزیز قرار بگیرد.

---

\* این مقاله به همت تحریریه فصلنامه ره‌آورد نور، با استفاده از برخی مقالات و وبگاه‌های مرتبط با این بحث، جمع‌آوری، تلخیص و ویرایش شده است.

## سخن نخست

برخی از مسئولان و صاحب‌نظران، به‌ویژه در حوزه قدرت و سیاست، ضعف امنیتی دولت‌های الکترونیک و آسیب‌پذیر بودن آنها در برابر حملات مخرب آنلاین را به عنوان مانعی بزرگ برای تحقق آن می‌دانند؛ اما باید گفت که تلاش و صرف هزینه در جهت تحقق و پیشبرد دولت الکترونیک، با توجه به مزایا و بازدهی فراوان آن در کوتاه‌مدت، خود پیش‌شرط لازم برای احساس نیاز به ایجاد امنیت در آن است. علاوه بر این، تجربه کشورهای پیشرو در این حوزه، استفاده از گواهی‌نامه‌های امنیتی موجود و نیز دسترسی آسان به فناوری‌های حفاظتی قدرتمند، تضمینی برای قدرت، قوت و استحکام لایه‌های امنیتی در تعاملات درون و برون‌سازمانی دولت‌های الکترونیک محسوب می‌شوند.

به نظر می‌رسد، تهدید اصلی و بالفعل کشور در مورد اینترنت، فقدان گفتمان امنیتی در مورد این پدیده است. اینترنت که به طور بالقوه می‌تواند هم تهدید و هم فرصتی طلایی برای امنیت فرهنگی و سیاسی باشد، به وسیله‌ای برای فشار سیاسی و اقتصادی تبدیل شده است.

در چنین فضایی، بررسی وضعیت امنیت و روش‌های نظارت بر فضای مجازی در کشورهای دیگر، راهکار خوبی برای نیل به یک امنیت مطلوب در کشور خودمان است.

از ابتدای زندگی بشر، امنیت، یکی از دغدغه‌های اصلی انسان‌ها بوده است و امروزه با گسترش اینترنت و فضاهای شبکه‌ای در کشورمان، لزوم امنیت برای فعالیت در این فضاهای مجازی بیش‌ازپیش احساس می‌شود. ترس و بیم از تخریب مبانی اخلاقی و اجتماعی، و نداشتن امنیت روانی و فرهنگی ناشی از هجوم اطلاعات آلوده و مخرب از طریق اینترنت و فضاهای مجازی، واکنشی منطقی است؛ زیرا هر جامعه‌ای چارچوب‌های اطلاعاتی خاص خود را دارد. طبیعی است که هر نوع اطلاعاتی که این حدودمرزها را بشکند، می‌تواند سلامت و امنیت جامعه را به خطر اندازد. برخلاف وجود جنبه‌های مثبت شبکه‌های جهانی، سوء استفاده از این شبکه‌های رایانه‌ای توسط افراد هنجارشکن، امنیت ملی را در کشورهای مختلف با خطر جدی روبه‌رو ساخته است. از این رو، به‌کارگیری روش‌ها و راهکارهای مختلف برای پیشگیری از نفوذ داده‌های مخرب و مضر و گزینش اطلاعات سالم در این شبکه‌ها رو به افزایش است. همین موضوع، مقوله نظارت بر فضای مجازی را به مسئله‌ای بسیار مهم در کشورها بدل نموده است.

خوشبختانه، با وجود هیاهوی بسیاری که شبکه جهانی اینترنت و فضاهای سایبر را غیرقابل کنترل معرفی می‌کند، فناوری لازم برای کنترل این شبکه و انتخاب اطلاعات سالم، رو به گسترش و تکامل است و دولت‌ها می‌توانند به‌راحتی به مدیریت و کنترل این فضا همت گمارند تا از آسیب‌های گوناگون آن در عرصه‌های سیاسی، نظامی، اجتماعی و فرهنگی امان یابند و حتی بسیار اثرگذار در این فضا حاضر شوند.

کنترل دستیابی و نحوه استفاده از منابعی که به اشتراک گذاشته شده‌اند، از مهم‌ترین اهداف یک نظام امنیتی در شبکه است. با گسترش شبکه‌های رایانه‌ای، به‌خصوص اینترنت، نگرش به امنیت اطلاعات و سایر منابع به اشتراک گذاشته‌شده، وارد مرحله جدیدی گردیده است. نبود نظام مناسب امنیتی، گاهی پیامدهای منفی و دور از انتظاری را به دنبال دارد.

بدیهی است که توفیق در ایمن‌سازی اطلاعات، منوط به حفاظت از اطلاعات و نظام‌های اطلاعاتی در مقابل حملات است. بدین منظور، از سرویس‌های امنیتی متعددی استفاده می‌گردد. سرویس‌های انتخابی باید پتانسیل لازم در خصوص ایجاد یک نظام حفاظتی مناسب، تشخیص به‌موقع حملات، و واکنش سریع را داشته باشند. حفاظت مطمئن، تشخیص به‌هنگام و واکنش مناسب، از جمله مواردی هستند که باید همواره در ایجاد یک نظام امنیتی رعایت شود.



## سیاست‌های نظارتی کشورها در فضای مجازی

به گزارش سرویس فضای مجازی خبرگزاری صداوسیما، یک هفته پس از انتخابات ریاست جمهوری ۲۰۱۶ آمریکا که تمام سازمان‌های اطلاعاتی این کشور هم‌صدا با دولت اوباما، روسیه را به دخالت سایبری، به قصد ضربه زدن به هیلاری کلینتون، متهم کردند، مجلس چین سخت‌گیرانه‌ترین قانون امنیت سایبری را تصویب کرد. وقتی از یکی از مقامات عالی‌کنگره خلق چین، از ضرورت چنین کنترل‌هایی پرسیدند، گفت: «این قانون، برای چین به عنوان یک قدرت بزرگ اینترنتی، ضروری است.»

طبق افشاگری‌های سه سال گذشته ادوارد اسنودن، دولت آمریکا بزرگ‌ترین شنود و رصد اینترنتی را انجام می‌دهد. حالا حتی کشورهایی مانند: سوئد، هند، کره جنوبی، مالزی و کانادا که نمادهای مردم‌سالاری و آزادی بیان محسوب می‌شوند، گسترده‌ترین میزان فیلترینگ اینترنت را اعمال می‌کنند و در حقیقت، نسبتی مستقیم بین قدرت کشورها و میزان کنترلشان بر اینترنت وجود دارد.

**موضوع نظارت بر فضای مجازی که بارها در فرمایش‌ها و سخنان حکیمانه رهبر معظم انقلاب و نیز متخصصان و دست‌اندرکاران این حوزه، مورد توجه و تأکید قرار گرفته، از مباحث مهم و کلیدی در حوزه فناوری اطلاعات و ارتباطات است و تمام کشورهایی که وارد این عرصه می‌شوند، ناچارند که بر فضای مجازی نظارتی حساب‌شده داشته باشند تا در سایه آن، هم از فواید این حوزه بهره‌مند شوند و هم بدنه اجتماعی و فرهنگی خویش را از آسیب‌های این فضای موج حفظ کنند**

تجربه کشورهای توسعه‌یافته در مواجهه با اینترنت، نشان می‌دهد که این کشورها نیز مانند ایران مایل بر حکمرانی بر فضای مجازی هستند؛ هدفی که با تحقق شبکه ملی اطلاعات برای کشورمان دست‌یافتنی است.

«حاکمیت داده»، اصلی‌ترین رویکرد کشورها در مدیریت فضای مجازی به حساب می‌آید و مرور تجربیات کشورهای توسعه‌یافته و نیز کشورهایی که در خصوص اینترنت، دغدغه‌های مشابه با ما دارند، نشان می‌دهد که این کشورها نیز مایل به مدیریت فضای اینترنت هستند. آنها تمامی توان خود را به کار می‌گیرند تا از اطلاعاتشان محافظت کنند و برایشان مهم است که اطلاعات کاربرانشان برای تحلیل به خارج از کشورشان منتقل نشود.

برای تحقق مفهوم حکمرانی فضای مجازی، حکومت‌ها سعی می‌کنند حاکمیت سرزمینی خود را در فضای مجازی بازتعریف و اعمال کرده، سیاست‌هایی را برای شکل‌دادن به فعالیت‌ها در فضای مجازی تدوین و اجرا نمایند و رویه‌های عمل قانونی و مشروع را در فضای مجازی تعیین، و روابط میان بازیگران و گروه‌های اجتماعی مختلف را تنظیم کنند.

در کشور ما نیز نقطه مطلوب در بحث حکمرانی اینترنت و مدیریت بر فضای سایبری، شبکه ملی اطلاعات است و شورای عالی فضای مجازی نیز در تبیین سند ضرورت الزامات شبکه ملی اطلاعات، ۲ محور از ۶ محور این الزامات را به موضوع استقلال و مدیریت فضای مجازی اختصاص داده است؛ به این معنا که بتوانیم بدون وابستگی به کشورهای دیگر، با توسعه زیرساخت‌های فناورانه، این فضا را مدیریت نماییم و در بحث حکمرانی داده و صیانت از انتقال داده‌ها، به نحوی عمل کنیم که اطلاعات کاربران به خارج از کشور درز پیدا نکند.

با این حال، بسیاری از کارشناسان و فعالان حوزه فناوری اطلاعات معتقدند که عزم کافی برای اعمال پذیرش حاکمیت فضای مجازی در ایران وجود ندارد و مسئولان، یک وحدت رویه را برای اعمال پذیرش حاکمیت فضای مجازی دنبال نمی‌کنند؛ برای مثال، آمریکا در حالی برای وضع قوانین برای فعالیت شبکه‌های اجتماعی اقدام می‌کند که در کشور ما شبکه‌های خارجی بدون هیچ‌گونه مجوزی فعالیت می‌کنند و به دلیل نبود حاکمیت سایبری داخلی در کشور، قوانین و مقرراتی نیز برای آنها متصور نیست.

پژوهشگاه فضای مجازی، در سلسله گزارش‌هایی به بررسی وضعیت حکمرانی برخی کشورهای توسعه‌یافته و در حال توسعه پرداخته است. این گزارش، نشان می‌دهد که نسبت مستقیمی



● میان قدرت کشورها و میزان حکمرانی آنها در فضای مجازی و  
● میزان کنترلشان بر اینترنت وجود دارد.

برسد.  
این کشور با ضریب نفوذ بیش از ۶۰ درصدی اینترنت، حدود ۶۷۴ میلیون نفر کاربر شبکه‌های اجتماعی دارد که با توجه به اصل حاکمیت سایبری که یکی از رویکردهای اصلی در مدیریت فضای مجازی آن به حساب می‌آید، پلتفرم‌هایی مانند: فیس‌بوک، یوتیوب و توییتر را مسدود کرده و شبکه‌های اجتماعی محلی از جمله «وی‌چت» و «وی‌بو» کاربران بسیاری را به خود جذب کرده‌اند.

وضعیت فضای مجازی در چین، نشان از اقدامات متعدد نهادهای حاکمیتی این کشور برای مواجهه با چالش‌ها و فرصت‌های متعدد در حوزه‌های مختلف فضای مجازی دارد. اخیراً نیز کارگروه حکمرانی ویژه اپلیکیشن‌های موبایل تحت هدایت وزارت صنعت و فناوری اطلاعات و برخی نهادهای دیگر این کشور، پیش‌نویس لایحه روش ارزیابی اپلیکیشن را برای جمع‌آوری و استفاده از داده‌های شخصی ارائه کرده است. این برای نخستین بار در جهان است که تلاش می‌شود تا نوع تخطی از حفاظت از داده‌های شخصی در اپلیکیشن‌ها مشخص شود.

از دیگر سیاست‌های حاکمیتی فضای مجازی در این کشور، می‌توان به ۴ مقوله حاکمیت اقتصادی و فنی، حاکمیت فرهنگی، حاکمیت امنیتی و حاکمیت مدیریتی و حقوقی اشاره کرد که بر مبنای آن، بر رقابت تنگاتنگ صنعت و کسب‌وکارهای چین با شرکت‌های سخت‌افزاری و نرم‌افزاری و خدمات‌دهندگان آمریکایی و نیز حرکت به سوی خودکفایی در خصوص زیرساخت‌ها و تجهیزات فنی فضای مجازی تأکید شده است.

رقابت تنگاتنگ محتوای چینی با محتوای غیرچینی در رسانه‌های نوین فعال در چین و کاهش وابستگی به زیرساخت و خدمات آمریکایی و وضع قوانین تقویت حاکمیت در فضای مجازی، از دیگر

● نگاهی گذرا به ساختار حکمرانی و مدیریت فضای مجازی در این کشورها نشان می‌دهد که همه آنها برای آینده حکمرانی داده تا سال ۲۰۳۰ برنامه دارند و حکمرانی فضای مجازی را در قالب سه مفهوم: «حکمرانی از طریق فضای مجازی»، «حکمرانی در فضای مجازی» و «حکمرانی بر فضای مجازی» دنبال می‌کنند.

## ● ۱. چین

● رهبران حزب کمونیست با برپایی «دیوار آتش بزرگ» یا همان دیوار مجازی چین، به هیچ‌وجه با یک اینترنت تمام‌غربی کنار نیامدند. در عوض، اینترنت را از نو به شکل کاملاً چینی به نام «هولیان ونگ» اختراع کردند و آن را به طور کامل به خدمت خود درآوردند. از ده‌های زرد به لطف پیشرفت نجومی فناوری‌هایش، با بومی‌سازی تقریباً کامل شبکه مجازی در داخل جامعه یک میلیارد و چهارصد میلیون نفری چین، عملاً در جنگ اطلاعاتی با آمریکا و دیگر رقبایش پیروز شد؛ درحالی‌که غربی‌ها چین را به جهت فرق قائل نشدن میان فیلترینگ پورنوگرافی با فیس‌بوک، بی.بی.سی، ویکی‌پدیا و محدود ساختن خدمات گوگل، به عنوان بزرگ‌ترین فیلترکننده اینترنت متهم می‌کنند. این کشور، مابه‌ازای چینی همه جذابیت‌های اینترنتی را برای کاربران داخلی فراهم آورده و هیچ کم‌وکاستی برای آنها نگذاشته؛ تا جایی که بزرگ‌ترین جامعه مجازی جهان، با ۱۴۰ میلیون کاربر دائم را از آن خود کرده است.

● چین به عنوان میزبان بزرگ‌ترین جامعه آنلاین در جهان، تا سال ۲۰۱۹ حدود ۸۴۰ میلیون نفر جمعیت اینترنتی به ثبت رسانده و پیش‌بینی می‌شود که تا سال ۲۰۲۳، این رقم به ۹۷۵ میلیون نفر



**از آنجاکه نیاز اساسی جوامع در حال رشد به دریافت اطلاعات مفید و سازنده را نمی‌توان نادیده گرفت و از سویی، باید از تخریب مبانی اعتقادی و اجتماعی جامعه نیز با حساسیت تمام جلوگیری کرد، کنترل و نظارت کارشناسی شده و استفاده از تجارب دیگر کشورها در این باره، بهترین راهکار مواجهه با فضای مجازی است.**

**راهکار دیگر را می‌توان راه‌اندازی شبکه ملی اطلاعات برشمرده که نقطه بسیار مطلوب برای بهره‌مندی بهینه و اثربخش از فضای مجازی و شبکه‌های اجتماعی است**



سیاست‌های این کشور به شمار می‌رود. این کشور سیاست‌های توسعه اینترنت ملی، راه‌اندازی سرویس‌های اجتماعی تحت وب به جای خیل عظیم سرویس‌های آمریکایی، توسعه و تقویت شدید توان سایبری و شکل دادن به فضای مجازی از طریق بسترسازی مناسب برای استارت‌آپ‌ها را دنبال می‌کند.

دولت چین برای چشم‌انداز سال ۲۰۲۰، به فکر ایجاد فضایی است که در آن، همه‌چیز به هم متصل، انسان و ماشین در تعامل و امکانات زمینی و فضایی نیز یکپارچه باشند. چین این فضا را به صورت یک اکوسیستم تصور کرده است و تمامی لایه‌های فضای مجازی (زیرساخت، خدمات و محتوا) را شامل می‌شود. چین برای تحقق چنین فضایی، ایجاد یک زیرساخت واحد، فراگیر، پُر ظرفیت، پُر سرعت و امن را به عنوان اولویت خود در لایه زیرساخت مشخص نموده است.

طرح پنج‌ساله سیزدهم توسعه اقتصادی و اجتماعی چین، در چشم‌انداز ۲۰۱۶ تا ۲۰۲۰ تعریف شده است و سال پایانی خود را سپری می‌نماید. بررسی این طرح و رصد میزان موفقیت دولت چین در تحصیل چشم‌اندازهای خود، با توجه به ویژگی‌های مشترک حکمرانی با آن دولت و چرخش روابط خارجی نظام به سوی کشورهای شرقی، نقشه راه مناسبی برای بازبینی در سیاست‌ها و رویکردهای جمهوری اسلامی ایران نسبت به فضای مجازی و کارکردهای آن خواهد بود.

طرح سیزدهم توسعه چین بر هفت محور تمرکز دارد:

– **نوآوری:** جهش در زنجیره تولید با رهاکردن صنعت سنگین قدیمی و بازسازی آن بر مبنای زیرساخت‌های مدرن متمرکز بر اطلاعات و توسعه مبتنی بر نوآوری؛

– **تعادل:** توزیع و مدیریت بهتر منابع به منظور پُر کردن شکاف‌های رفاهی بین حومه‌شهر و شهر؛

– **سبزسازی:** توسعه صنعت فناوری محیط زیست و همچنین، زندگی زیست‌محیطی و فرهنگ محیط زیست، به منظور دستیابی به بهبود کلی در کیفیت محیط زیست و اکوسیستم‌ها؛

– **پیشگامی:** مشارکت عمیق‌تر در ساختارهای قدرت فراملی، همکاری بیشتر بین‌المللی؛

– **اشتراک:** ترغیب مردم به تسهیم ثمرات رشد اقتصادی و پُر کردن شکاف‌های رفاهی موجود؛

– **بهداشت و درمان:** پیاده‌سازی برنامه اقدام سلامت ۲۰۲۰؛

– **جامعه نسبتاً مرفه:** ساختن جامعه‌ای نسبتاً مرفه از هر حیث.

دولت چین برای این دوره پنج‌ساله، سیاست‌های «خلاقیت توده‌ها»، «ساخت چین ۲۰۲۵»، «نیاز اقتصاد به قانون»، «بهبودسازی دفاع ملی»، «شهرسازی جدید ملی» و «اصلاح سیاست تک‌فرزندی به دو فرزند» را انتخاب نموده است. این دولت، ذیل سیاست «ساخت چین ۲۰۲۵»، به عدم وجود یک بستر واحد برای فناوری‌های حیاتی خود اشاره نموده است و رفع این مشکل را به عنوان یکی از اقدامات دارای اولویت خود انتخاب می‌کند. چین مفهوم «اینترنت+» را برای حل این معضل خلق کرده است.

به‌طور کلی، دولت چین نگاه اکوسیستمی به فضای سایبر دارد و توسعه زیرساخت را برای بازسازی صنایع و افزایش قدرت اقتصادی خود دنبال می‌کند. این دولت در فرآیند این توسعه، ملاحظات ویژه‌ای از قبیل: ۱. اطمینان از درک کامل روندهای توسعه‌ای



و ترویج خشونت بوده است، اما علاوه بر سیاست‌های غیراخلاقی و سیاست‌هایی که حق تألیف را رعایت نمی‌کنند، در عربستان و بگاه‌های منتسب به شیعیان ایران، حزب الله و اخوان المسلمین فیلتر می‌شوند.

همچنین، در دوره‌های مختلفی در این کشور دسترسی به پلتفرم‌های تماس اینترنتی مانند «اسکایپ» و برخی شبکه‌های اجتماعی مانند «تلگرام» به صورت کامل قطع یا با اختلال مواجه شده است. علاوه بر این، افرادی که از طریق صفحات «فیس‌بوک» یا «توییتر» شهروندان را به تجمعات ضد دولتی مانند اعتراضات در مناطق شیعه‌نشین دعوت کرده‌اند، تحت تعقیب قرار گرفته‌اند.

عربستان سعودی مانند سایر کشورها، از تکنولوژی شرکت‌های غربی مانند Smartfilter که آمریکایی است، استفاده می‌کند تا به طور خودکار، وبگاه‌ها را بر اساس مواد خاصی فیلتر کند. در همین حال، بر مبنای دستورعمل‌های یک کمیته امنیتی تحت نظارت وزارت اطلاعات این کشور، پایگاه‌هایی که انتقاد از دولت عربستان سعودی دارند و یا بگاه‌هایی که ایدئولوژی شیعه را تبلیغ می‌کنند نیز مسدود می‌شوند.

در سال ۲۰۱۱، دولت عربستان سعودی قوانین و مقررات اینترنتی جدیدی را به تصویب رساند که همه روزنامه‌ها و وبلاگ‌نویسان آنلاین را مجاز به دریافت مجوز ویژه از وزارت اطلاعات کرده است.

دولت عربستان سعودی، برنامه‌های آنلاین مانند «اسکایپ» و «واتساپ» را به دلیل ترس از اینکه فعالان ضد حکومتی ممکن

فناوری اطلاعات توسط حاکمیت؛ ۲. تعمیق یکپارچه‌سازی فناوری اطلاعات در توسعه اجتماعی و اقتصادی؛ ۳. تقویت و توسعه هم‌زمان مسائل امنیتی و گسترش فناوری اطلاعات را در نظر گرفته است.

## ۲. عربستان سعودی

دیکتاتوری سعودی، یک‌ونیم میلیون کاربر اینترنتی دارد که دوسوم آن را زنان تشکیل می‌دهند. با توجه به نگاه بسته وهابیون حاکم بر این کشور، واحد خدمات اینترنت سعودی (آیسو) کار اصلی‌اش به جای دسترسی دادن، مسدودسازی گسترده تارنماهای مذهبی، سیاسی، جنسی، حقوق بشری، پزشکی، فکاهی، فیلم و موسیقی است.

عربستان سعودی، تمام ترافیک اینترنت بین‌المللی را از طریق یک مزرعه پروکسی واقع در شهر علم و فناوری پادشاه عبدالعزیز هدایت می‌کند که یک فیلتر محتوا بر اساس نرم‌افزار محاسبه امن روی آن وجود دارد.

از اکتبر سال ۲۰۰۶ کمیسیون ارتباطات و فناوری اطلاعات این کشور (CITC)، ساختار DNS و فیلتر کردن را در عربستان سعودی برعهده دارد. البته پایه قانونی اولیه برای فیلتر کردن، محتوای قطعنامه شورای وزیران این کشور مربوط به تاریخ ۱۲ فوریه ۲۰۰۱ است.

طبق گزارش وبگاه این کمیسیون، در سال ۲۰۱۷ حدود یک میلیون و دویست هزار پایگاه در این کشور فیلتر شده است. اگرچه دلیل این فیلترینگ محتواهای غیراخلاقی، نفرت‌پراکنی

است از این سیستم عامل استفاده کنند، در سال ۲۰۱۳ مسدود کرد؛ اما دولت به عنوان بخشی از اصلاحات اقتصادی کشور برای تقویت کسب و کار و تنوع بخشیدن به اقتصاد، این ممنوعیت را در سال ۲۰۱۷ لغو کرد.

به طور کلی، مهم‌ترین شاخصه‌های حکمرانی فضای مجازی در کشور عربستان سعودی را می‌توان توجه به گسترش خدمات دولت الکترونیک، ایجاد محیطی جذاب برای سرمایه‌گذاری در بخش ICT، تلاش برای افزایش سهم این بخش در تولید ناخالص داخلی غیرنفتی و کوشش برای کاهش درصد خروج درآمدهای صنعت اطلاعات و ارتباطات از کشور عنوان کرد.

سناریوی حکمرانی فضای مجازی این کشور نیز شامل حاکمیت بر مردم، فقدان نهادهای دموکراتیک و البته عدم موضع‌گیری در قبال ایالات متحده در حوزه فضای مجازی است.

### ۳. کره جنوبی

کره جنوبی، در فهرست کشورهای با فضای مجازی تحت نظارت برای سانسور اینترنت قرار داده می‌شود؛ یعنی درحالی‌که شهروندان آزادی بیان دارند، اما لزوماً حقوق مربوط به حریم خصوصی آنها به طور کامل رعایت نخواهد شد. در این کشور که دارای بالاترین نفوذ فعال رسانه‌های اجتماعی در میان کشورهای آسیایی است، شبکه‌های اجتماعی مانند: فیس‌بوک، Kakaostory، توئیتر، لاین، اینستاگرام و KakaoTalk به طور گسترده استفاده می‌شوند.

تصمیم برای سانسور اینترنت در کشور کره جنوبی، از طریق دو کمیته ارتباطات کره (KCC) و کمیته استانداردهای ارتباطات کره (KCSC) صورت می‌گیرد و مواردی از قبیل: محتوای مستهجن، موارد مضر برای افراد زیر سن قانونی، تقلب در اینترنت، موارد مربوط به ستایش کره شمالی و محتوای ضد دولتی و ضد قوای نظامی، از جمله محتواهایی است که توسط این دو کمیته مسدود می‌شوند.

علاوه بر این دو کمیته، در کره سازمان حکمرانی اینترنتی (KISO) نیز وجود دارد که متشکل از مهم‌ترین پلتفرم‌های اینترنتی کشور کره مانند SK Daum Kakao Naver Communications و KT است. این شرکت‌ها، به عنوان بخشی از همکاری این سازمان با دولت، اغلب از یک روش به اصطلاح موسوم به «تأیید نام واقعی» استفاده می‌کنند. منظور از تأیید نام واقعی، نیاز به ارائه اطلاعات شخصی کاربران پیش از قرار دادن اطلاعات در

فضای مجازی به صورت آنلاین است.

دولت کره جنوبی اعلام کرده که مردم این کشور حق دارند انتقادات خود از سیاست‌های دولت یا رهبران سیاسی را در فضای مجازی ابراز کنند؛ مشروط به آنکه اظهارات آنها موجب تهدید امنیت ملی و تهمت نباشد.

اقدام به سانسور دولتی در خصوص برخی از موضوعات در فضای مجازی، در هر کشوری از جهان انجام می‌شود. با این حال، در کره جنوبی تقابل میان ارزش‌های دموکراتیک و سطح سانسور در دولت، همواره وجود دارد.

حرکت به سوی تبدیل شدن کره جنوبی به کشوری پیشرو در بخش نرم‌افزاری حوزه فناوری‌های فضای مجازی در جهان، و توجه به صنعت و تجاری‌سازی صنایع به مثابه پیشران فضای مجازی و اتخاذ رویکرد ارتقای کیفیت زندگی برای جامعه از طریق امکانات فضای مجازی، این کشور را به الگوی حکمرانی فضای مجازی در آسیای شرقی تبدیل کرده است.

این الگوی توسعه‌ای، بر اصل «دولت راهبر، همکاری آزادانه» تأکید دارد و سناریوی حکمرانی فضای مجازی کشور کره جنوبی، مبتنی بر تحقق این الگو شکل گرفته است.

### ۴. مالزی

مالزی، یک کشور چندقومی، چندنژادی و چندمذهبی است و ضرورت ایجاد هارمونی و همزیستی مسالمت‌آمیز بین اقوام، نژادها و پیروان ادیان مختلف ایجاد می‌کند تا اینترنت و فضای سایبری نیز همانند سایر فناوری‌ها از مکانیسم‌های خاص نظارتی و کنترل برخوردار باشند.

بیش از ۸۷ درصد مردم مالزی، در سال ۲۰۱۸ به اینترنت و شبکه‌های اجتماعی دسترسی داشته‌اند که ۹۱ درصد آن از طریق تلفن هوشمند بوده است. در این کشور، فیس‌بوک و واتساپ، محبوب‌ترین شبکه‌های اجتماعی محسوب می‌شوند.

در حال حاضر، کمیسیون ارتباطات و مولتی مدیای مالزی، متولی رصد و نظارت بر رسانه‌های این کشور، از جمله اینترنت و فضای مجازی است و این کمیسیون، از مکانیسم‌های قانونی و ابداعی مختلفی برای کنترل اینترنت و شبکه‌های اجتماعی استفاده می‌کند. بر این اساس، «فیلترینگ» و «حذف محتوا»، دو مکانیسم اصلی این کمیسیون برای اطمینان از سلامت و صیانت از فضای مجازی در این کشور محسوب می‌شود.

## ۶. روسیه

در سال ۲۰۰۴، تنها ۸ درصد از جمعیت کشور روسیه به اینترنت دسترسی داشتند؛ اما این آمار در سال ۲۰۱۵، به حدود ۷۰ درصد رسید و اکنون روسیه با ۱۰۹ میلیون نفر کاربر اینترنتی، بیشترین جمعیت کاربران اینترنتی را در بین کشورهای اروپایی دارد و نرخ نفوذ اینترنت در این کشور، ۷۶ درصد است.

در زمینه استفاده از شبکه‌های اجتماعی، آمار نشان می‌دهد نرخ نفوذ شبکه‌های اجتماعی در بین کاربران روسی، ۴۹ درصد است و در حال حاضر، ۷۰ میلیون کاربر روسی فعال در شبکه‌های اجتماعی وجود دارد.

با توجه به نفوذ فضای مجازی در کشور روسیه، سیاست‌های حاکمیتی در این حوزه، شامل رقابت تنگاتنگ صنعت و کسب‌وکارهای روسیه با شرکت‌های سخت‌افزاری و نرم‌افزاری و خدمات‌دهندگان آمریکایی و گسترش پژوهش کاربردی در سخت‌افزار و خدمات و نیز رقابت تنگاتنگ محتوای روسی با محتوای غیرروسی در رسانه‌های نوین فعال در روسیه است. از سوی دیگر، این کشور برای کاهش وابستگی به شبکه، زیرساخت و خدمات آمریکایی و وضع قوانین تقویت حاکمیت در فضای مجازی تلاش می‌کند.

حکومت روسیه برای مواجهه با فضای مجازی در حوزه حاکمیت سایبری، اسناد راهبردی را تدوین نموده و منابع متعددی را برای ایجاد توازن فنی و مشارکت منصفانه با دولت‌ها فراهم کرده است. همچنین، تأکید بر چندجانبه‌گرایی در مدل حکمرانی اینترنت جهانی در چارچوب سازمان ملل و مقابله با هژمونی آمریکا بر بستر اینترنت موجود و نیز توجه به الگوی مستقل توسعه فضای مجازی بر اساس ساختار و اقتضائات بومی و اعمال محدودیت و فیلترینگ در برابر پلتفرم‌های خارجی که حاضر به همکاری و رعایت الزامات قانونی داخلی نیستند، از دیگر اقدامات روسیه در حوزه حاکمیت سایبری است.

این کشور برای تقویت هرچه بیشتر حاکمیت سایبری، اینترنت ملی را تحت قانونی موسوم به «حاکمیت اینترنت روسیه» راه‌اندازی کرده و امکان استقلال کامل فضای مجازی را تحت یک شبکه اینترنت محلی با عنوان «رون» فراهم کرده است. راه‌اندازی سرویس‌های مشابه با سرویس‌های جذاب تحت وب آمریکایی، از جمله دیگر کارهای موفق حکومت روسیه در راستای حفظ و توسعه حاکمیت فضای مجازی است.

این کشور، با وجود رسیدن به سال ۲۰۲۰، همچنان دوران گذار تکنولوژیک را تجربه می‌کند و در ارزیابی نوع مواجهه مالزی با فضای سایبر، می‌توان به‌وضوح غلبه رویکرد دفاعی و امنیتی را ملاحظه کرد که البته، این موضوع، لزوماً منفی نیست؛ بلکه وابستگی شدید حوزه‌های کلیدی زیرساخت اطلاعاتی ملی به فناوری‌های نوین اطلاعاتی و ارتباطی، ایجاب می‌کند که رویکرد دفاعی و امنیتی در این کشور با هدف اطمینان از کارایی و عملکرد این حوزه‌ها در مرکز ثقل هرگونه برنامه‌ریزی و سیاست‌گذاری قرار گیرد.

وجه مثبت حکمرانی سایبری در مالزی، رویکرد ایجابی این کشور برای استفاده از ظرفیت‌ها و فرصت‌های فضای مجازی برای توسعه همه‌جانبه است و این کشور، حاکمیت فناوری در عصر سایبری را به رسمیت شناخته و به همین دلیل، در اغلب سیاست‌گذاری‌ها، بر دستیابی به آخرین فناوری‌ها و نیز استفاده حداکثری از ظرفیت‌های فناوری و نوآوری تأکید کرده است.

## ۵. هند

پس از حملات تروریستی سال ۲۰۰۸ در بمبئی، موضوع امنیت برای دولت هند، اهمیت بسیار بیشتری پیدا کرده است. به همین دلیل، فیلترینگ وبگاه‌ها و محتواهای افراط‌گرایانه و جدایی‌طلبانه، شدت یافته است. همچنین، در این کشور پایگاه‌های ناقض حق تألیف و محتواهای پورنوگرافی، به طور کامل فیلتر می‌شوند.

در خصوص سناریوهای حکمرانی فضای مجازی کشور هند، می‌توان به تأکید بر استقلال نهاد تنظیم‌گر از دولت، رویکرد اقتصادی و تلاش برای ایجاد شغل و افزایش نقش فناوری ارتباطات در تولید ناخالص داخلی، و پلتفرم دولت الکترونیک (Digital India) اشاره کرد. توجه به امنیت فضای مجازی و حفظ حاکمیت سرزمینی دیجیتال نیز از دیگر موضوعات است.





می‌توان شامل مواردی چون: توجه به اصل حاکمیت سایبری و توسعه اینترنت ملی و افزایش دسترسی و پهنای باند و فیلترینگ و سانسور فضای مجازی جهت کنترل فضای سیاسی دانست.

از سوی دیگر، مدیریت ارتباطات با اتحادیه اروپا و جامعه بین‌المللی، توسعه و تقویت میزان تخصص و آگاهی منابع انسانی در زمینه امنیت سایبری و اختصاص بخش بسیاری از منابع به تحقیق و توسعه در فناوری‌های راهبردی و بنیادی فضای مجازی و نیز تلاش گسترده و ایجاد زیرساخت‌های مناسب برای ارائه خدمات از طریق دولت الکترونیک، از دیگر سناریوهای این کشور در حوزه فضای مجازی است.

ترکیه برای بهبود در کیفیت خدمات و حفاظت از جامعه از خطرات اینترنت و توسعه فناوری‌های ارتباطات ماهواره‌ای و ملی و توسعه ارتباطات بومی و ملی G5 و فراتر از نسل جدید فناوری‌های در حال توسعه مانند اینترنت اشیا، تلاش می‌کند.

#### ۸. لهستان

موج تغییرات سیاسی و گذار به جناح راست در اروپا، باعث افزایش



#### ۷. ترکیه

حاکمیت ترکیه پس از کودتا در ژوئیه ۲۰۱۶م، قوانین سانسور و فیلترینگ را به شدت در فضای مجازی و رسانه‌های اجتماعی اعمال کرده است. با توجه به حجم این محدودیت و همچنین تصویب قوانین سخت برای فعالان فضای مجازی، به نظر می‌رسد که حاکمیت ترکیه در حوزه فضای مجازی، در مقیاس وسیعی بر مردم حکومت می‌کند.

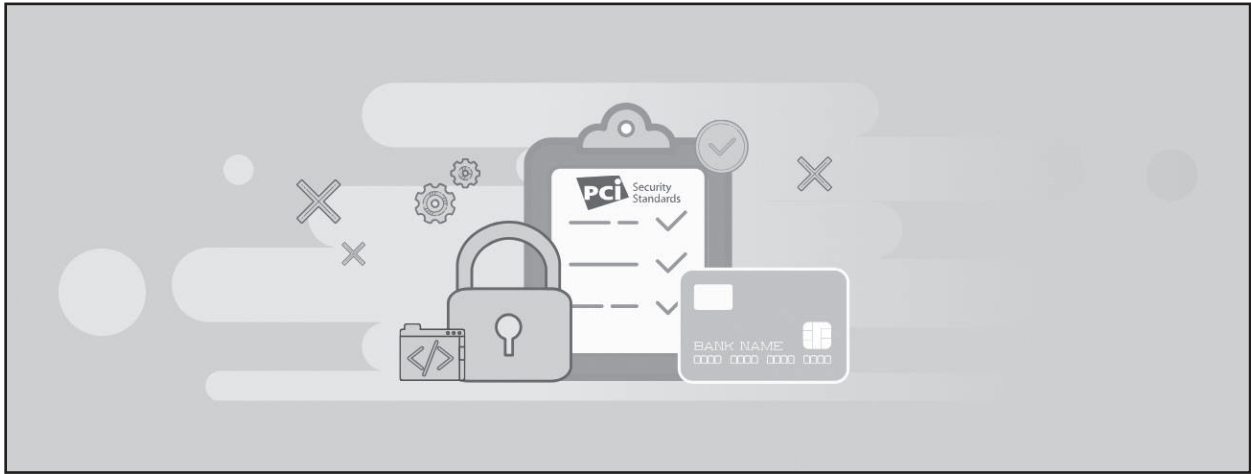
تمام ترافیک اینترنت کشور ترکیه، از طریق زیرساخت Turk Telecom عبور می‌کند که امکان کنترل متمرکز بر محتوای آنلاین و تسهیل اجرای تصمیمات فیلترینگ را به حکومت ترکیه می‌دهد.

یک سازمان مستقل پژوهشی دیجیتال در ترکیه با نام - Tu keyBlocks نیز وجود دارد که محدودیت‌های دسترسی به اینترنت و ارتباط آنها با حوادث سیاسی در ترکیه را کنترل می‌کند و از مهم‌ترین اقدامات آن، می‌توان به سانسور ویکی‌پدیا و از بین بردن دسترسی به امکانات ذخیره‌سازی ابری از جمله گوگل درایو و Dropbox اشاره کرد.

سانسور آنلاین و کنترل‌های دیجیتال بر رفتار عمومی در زمان تلاش بر کودتای نظامی سال ۲۰۱۶ و حوادث سانسور جمعی به دنبال حوادث تروریستی بمب‌گذاری آنکارا در سال ۲۰۱۵ و دستکاری ترافیک‌های اینترنتی در زمان جنگ، از جمله اقدامات این نهاد است.

به‌طور کلی، سناریوی حکمرانی فضای مجازی کشور ترکیه را

**وضعیت فضای مجازی در چین، نشان از اقدامات متعدد نهادهای حاکمیتی این کشور برای مواجهه با چالش‌ها و فرصت‌های متعدد در حوزه‌های مختلف فضای مجازی دارد. اخیراً نیز کارگروه حکمرانی ویژه اپلیکیشن‌های موبایل تحت هدایت وزارت صنعت و فناوری اطلاعات و برخی نهادهای دیگر این کشور، پیش‌نویس لایحه روش ارزیابی اپلیکیشن را برای جمع‌آوری و استفاده از داده‌های شخصی ارائه کرده است**



## ۹. ایرلند

پس از تلاش ایرلند برای مسدود کردن برخی از پایگاه‌ها به اشتراک‌گذاری فایل در فوریه سال ۲۰۰۹، سانسور اینترنت در این کشور به یک مسئله بحث‌برانگیز تبدیل شد. البته فراتر از این مسائل، در این کشور هیچ محدودیت دولتی در دسترسی به اینترنت و هیچ گزارش موثقی مبنی بر اینکه دولت ایمیل‌ها یا چت روم‌ها را تحت نظارت مستقیم قرار داده است، وجود ندارد.

قانون ایرلندی به آزادی بیان برای همه اقشار جامعه در عمل احترام می‌گذارد و افراد و گروه‌ها می‌توانند در بیان دیدگاه‌ها به واسطه اینترنت، از جمله از طریق پست الکترونیکی آزادانه فعالیت کنند. این در حالی است که در این کشور، ایجاد مرکز اینترنت امن‌تر ایرلند (SIC)، نقش مشارکتی در ایجاد یک اینترنت امن را ایفا می‌کند. این مرکز، یک کنسرسیوم از سازمان آموزش و پرورش، سازمان رفاه کودکان، دولت و صنعت تشکیل شده است.

سناریوی حکمرانی فضای مجازی کشور ایرلند، شامل: توجه به اصل حاکمیت فضای مجازی و امنیت سایبری در چارچوب اتحادیه اروپا، همکاری و مشارکت در جلسات بین‌المللی حوزه ارتباطات و فضای مجازی و توجه به رشد اقتصاد دیجیتال و افزایش دسترسی و پهنای باند می‌شود.

در همین حال، فیلترینگ و سانسور فضای مجازی با محوریت اخلاقی (نوجوانان و کودکان)، مدیریت ارتباطات با اتحادیه اروپا و جامعه بین‌المللی و توسعه و تقویت میزان تخصص و آگاهی جامعه درباره فضای مجازی و تلاش گسترده و ایجاد زیرساخت‌های مناسب جهت ارائه خدمات از طریق دولت الکترونیک و توجه به استراتژی دیجیتال ملی، توسعه ارتباطات بومی، و در نهایت، گسترش زیرساخت‌های ارتباطی، از جمله گسترش شبکه فیبر، از دیگر اقدامات حاکمیت سایبری این کشور محسوب می‌شود.

سیستم‌های نظارت بر گردش آزاد اطلاعات، سانسور محتواهای مشخص در فضای مجازی، و در نتیجه، کاهش آزادی‌های فردی در استفاده از اینترنت شده است. کشور لهستان نیز از این قاعده مستثنا نبوده است.

در سال‌های اخیر، قوانین محدودکننده‌ای برای استفاده اینترنت آزاد وضع شده که بیشتر آنها به عنوان «قوانین مبارزه با تروریسم سایبری» تصویب و به عموم معرفی شده‌اند.

بعضی از فعالان جامعه مدنی در حوزه سایبری معتقدند که قوانین نظارتی و ضد تروریسم به گونه‌ای مبهم وضع شده‌اند که به دولت اجازه می‌دهد از آنها برای محدود کردن محتواهای خاص و کنترل گردش محتوا و بایگانی هویت کاربران فضای سایبری استفاده کند.

از جمله قوانین چالش‌برانگیز لهستان، توانایی دولت این کشور در قطع کامل سیستم‌های مخابراتی و ارتباطاتی در هنگام بروز «تهدیدهای تروپستی» است. همچنین، در سال ۲۰۱۶م، مکانیسمی برای فیلترینگ موضوعی محتواها و اپلیکیشن‌های خطرناک وضع شد که مجلس لهستان نیز با آن موافقت کرد و آن را به تصویب رسانید.

در این کشور، دولت همچنین به دنبال تصویب لایحه‌ای است که بر اساس آن، شرکت‌های اینترنت خانگی موظف باشند اطلاعات افرادی را که به محتواهای ممنوع دسترسی پیدا می‌کنند و یا از وبگاه‌های فیلترشده استفاده می‌کنند، در اختیار دولت قرار دهد.

به‌طور کلی، سناریوهای حکمرانی فضای مجازی کشور لهستان را می‌توان در قالب موضوعاتی همچون حرکت به سوی دیجیتالی‌سازی تمامی امور، همسویی کامل با قوانین و ارزش‌های اتحادیه اروپایی تقسیم‌بندی کرد.



**تجربه کشورهای توسعه یافته در مواجهه با اینترنت، نشان می‌دهد که این کشورها نیز مانند ایران مایل بر حکمرانی بر فضای مجازی هستند؛ هدفی که با تحقق شبکه ملی اطلاعات برای کشورمان دست‌یافتنی است.**

**«حاکمیت داده»، اصلی‌ترین رویکرد کشورها در مدیریت فضای مجازی به حساب می‌آید و مرور تجربیات کشورهای توسعه یافته و نیز کشورهایی که در خصوص اینترنت، دغدغه‌های مشابه با ما دارند، نشان می‌دهد که این کشورها نیز مایل به مدیریت فضای اینترنت هستند**



#### ۱۰. آلمان

فیلترینگ اینترنت در آلمان، بر اساس قانون فدرال و رأی دادگاه‌ها صورت می‌گیرد. با این حال، از آنجاکه ساختار اطلاعاتی آلمان عملاً زیرمجموعه آمریکاست، مسدودسازی محتوای سیاسی، به‌ویژه در مورد مسائل سیاسی ضد صهیونیستی مثل نفی هولوکاست، اولویت دارد.

در سال ۲۰۰۹م مجلس آلمان، قانونی در خصوص محدود کردن دسترسی به اینترنت وضع کرد. هدف این قانون، ایجاد محدودیت در دسترسی به پورنوگرافی کودکان در اینترنت بود. البته فهرست سیاه وبگاه‌ها در آلمان، فقط محدود به

پورنوگرافی کودکان نیست و شامل مواردی نیز می‌شود که به نفی هولوکاست، نژادپرستی و نفرت‌پراکنی مربوط هستند.

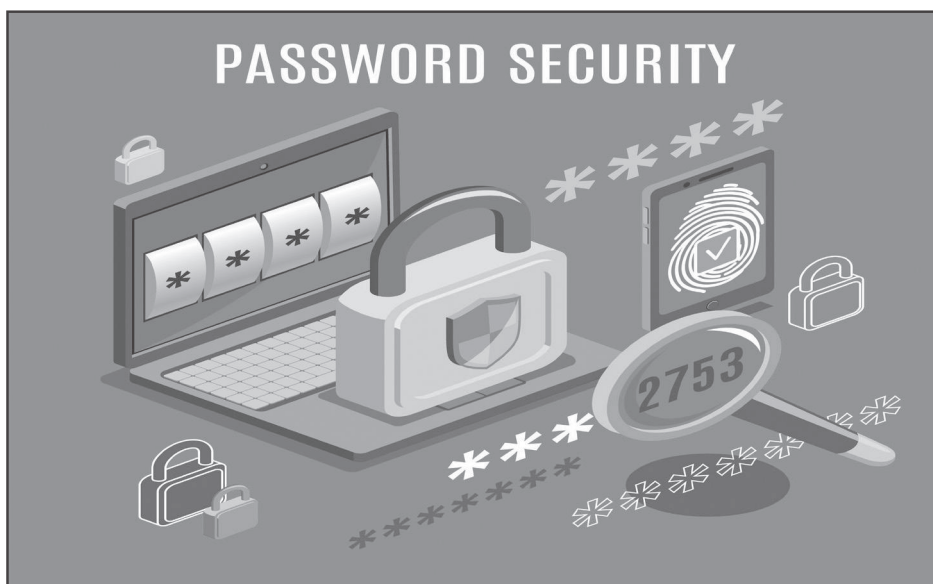
بخش تحقیقات جرایم فدرال در BKA، این فهرست را در اختیار آی.اس.پی‌ها قرار می‌دهد تا دسترسی به آنها محدود شود.

به‌طورکلی، سناریوهای حکمرانی فضای مجازی آلمان، شامل این موارد است: توجه به امنیت سایبری و توسعه زیرساخت‌های فضای مجازی، استفاده از ظرفیت اقتصادی فضای مجازی، تدوین استراتژی امنیت سایبری و تربیت نیروهای پلیس زبده برای کنترل محتوای فضای مجازی، استفاده از ظرفیت علمی آکادمیک برای کنترل محتوای فضای مجازی و دیپلماسی اروپایی بین‌المللی سایبری.

#### ۱۱. استرالیا

کشوری که نامش معادل کل قاره اقیانوسیه است، در سال‌های اخیر برنامه جاه‌طلبانه‌ای را برای کنترل اینترنت آغاز کرده است؛ تا آنجا که در این زمینه، استرالیا بیش از متحدان غربی‌اش با چین به عنوان بزرگ‌ترین سانسورکننده اینترنت مقایسه می‌شود. استرالیا با هدف ارتقای شاخص‌های افزایش ایمنی اینترنت برای خانواده‌ها، ممنوعیت محتوای مجرمانه سایبری را به طور جدی با طرح‌هایی سراسری با عنوانی همچون «دیوار آتش بزرگ» و «دیوار آتش ضد خرگوش» (برگرفته از نام دیوار ضد خرگوش در تاریخ این کشور) و با سنگین‌ترین جریمه‌ها اجرا کرده است.

در آخرین اقدام، نهاد مدیریت ارتباطات و رسانه استرالیا (آسما)،



دسترسی به سرویس‌های گوگل را محدود ساخت. در واقع، بزرگ‌ترین جزیره جهان، جایی است که مردم به جای نرم‌افزارهای فیلترشکن، به طور داوطلبانه از فیلترینگ استفاده می‌کنند.

## ۱۲. بریتانیا

بزرگ‌ترین مرکز کنترل اینترنت در جهان، یا به اختصار GCHQ، در ساختمان «دوناتی» چلتنهم انگلیس قرار دارد. این مقر مرکزی رصد و جاسوسی بین‌المللی دولت بریتانیا، هم‌زمان با همه سرویس‌های جاسوسی جهان، به‌ویژه همتایان آمریکایی‌اش، تبادل اطلاعات دائمی دارد.

جی.سی.ای.کیو، به انگلیسی‌ها امکان می‌دهد تا دسترسی افراد و آی.پی‌ها به اینترنت را به صورت هوشمند کنترل کنند. در عین حال، چندین بنیاد نظارت بر اینترنت، از جمله «ای دابلیو اف» نیز در این کشور در سطحی بین‌المللی در زمینه فیلترینگ فضای سایبری، به‌ویژه در مورد: پورنوگرافی کودکان، نژادپرستی و مسائل تروریستی فعال‌اند. همچنین، با سامانه مسدودسازی محتوا به سبک کلینفید، دسترسی بیش از ۹۰ درصد خطوط پرسرعت اینترنتی به چنین محتوایی مسدود شده‌اند و در صورت تخلف، خطوط خانگی قطع می‌شوند.



**حرکت به سوی تبدیل شدن کره جنوبی به کشوری پیشرو در بخش نرم‌افزاری حوزه فناوری‌های فضای مجازی در جهان، و توجه به صنعت و تجاری‌سازی صنایع به مثابه پیشران فضای مجازی و اتخاذ رویکرد ارتقای کیفیت زندگی برای جامعه از طریق امکانات فضای مجازی، این کشور را به الگوی حکمرانی فضای مجازی در آسیای شرقی تبدیل کرده است**



## ۱۳. آمریکا

پس از حوادث یازدهم سپتامبر ۲۰۰۱م، کنترل‌های دولتی بر کاربران اینترنت در هیچ کشوری به گستردگی آمریکا، آن هم با چنین روش‌های کاملاً حرفه‌ای و نامحسوس انجام نشده است. دولت بوش پسر، در تاریخ ۲۴ اکتبر ۲۰۰۱، قانونی تحت عنوان «لایحه میهن‌پرستی» را در قالب مبارزه با تروریسم تصویب کرد که به موجب آن، کنترل و نظارت بر تبادل داده‌های برخط یا اینترنتی کاربران، رنگ قانونی به خود گرفت. با وجود برخی مخالفت‌ها، این قانون با شدت بیشتری در سال ۲۰۰۳ توسط دیوان عالی ایالات متحده به تصویب رسید. «اف.بی.آی» یا اداره تحقیقات فدرال پلیس آمریکا، موظف است همه اطلاعات مربوط به کاربران اینترنتی را حتی برای تحقیقات غیررسمی، جمع‌آوری کند.

حتی باراک اوباما که با شعارهای آزادی‌خواهانه و گرایش نولیبرالی در انتخابات ریاست جمهوری پیروز شده بود و شعارهایی همچون «اینترنت باز» و «حق استفاده از اینترنت معادل حقوق بشر» سر می‌داد، در نهایت، قانون کنترل اینترنت را امضا کرد. او با ورود به کاخ سفید، نه تنها تغییری در سیاست نقض حریم خصوصی افراد، به‌ویژه در زمینه اینترنت ایجاد نکرد، بلکه در سال ۲۰۱۵ همان قانون «میهن‌پرستی» را با افزودن موارد شنود و جاسوسی از ارتباطات سایبری و مکالمات تلفنی شهروندان آمریکایی، به مدت ۵ سال دیگر تمدید کرد.

قانون توقف سرقت آنلاین (سوپا) و قانون حفاظت از دارایی معنوی (پیپا)، به دولت آمریکا قدرت خواهند داد به صورت بالقوه میلیون‌ها تارنما را تعطیل کند. روزنامه نیویورک تایمز در سرمقاله خود آورده است: «نتیجه اجرای دو قانون فوق، پدید آمدن پدیده‌ای مانند دیوار آتش بزرگ چین در آمریکاست.»

از سوی دیگر، نرم‌افزارهای جست‌وجوگر محتوا با امکان فعال کردن «قفل والدین»، جلوگیری از دسترسی کودکان به تارنماهای غیراخلاقی را در آمریکا ممکن ساخته است. لایحه محافظت کودکان از اینترنت (سیپا)، مدارس و کتابخانه‌های عمومی را موظف می‌کند که برای انجام فعالیت‌های اینترنتی، فیلترهای مربوط به تارنماهای غیراخلاقی، گپ برخط، شبکه‌های اجتماعی و اتاق‌های گفت‌وگو را در رایانه‌هایشان نصب کنند. شرکت‌های میزبانی وب نیز موظف‌اند نام دامنه‌هایی را که در فهرست سیاه وزارت خزانه‌داری آمریکا قرار گرفته‌اند، مسدود نمایند.

دانش‌آموزان مدارس، به صورت یک بحران درآمدی است و آنها به این نتیجه رسیده‌اند که دو راه در پیش رو دارند: بستن راه‌های دسترسی به اینترنت یا کنترل آن. از آنجاکه نیاز اساسی جوامع در حال رشد به دریافت اطلاعات مفید و سازنده را نمی‌توان نادیده گرفت و از سویی، باید از تخریب مبانی اعتقادی و اجتماعی جامعه نیز با حساسیت تمام جلوگیری کرد، کنترل و نظارت کارشناسی شده و استفاده از تجارب دیگر کشورها در این باره، بهترین راهکار مواجهه با فضای مجازی است.



#### ۱۴. فرانسه

در اتحادیه اروپا، فرانسه شدیدترین نظارت‌های حکومتی بر فضای سایبری را دارد. طبق قانون‌های هادویی و لوپسی مصوب سال ۲۰۰۹، کاربران ناقض قوانین شبکه، از دسترسی به آن محروم می‌شوند و علاوه بر فهرست بلندی از تارنماهای غیراخلاقی یا ایدئولوژیک مسدود، شهروندان حق جست‌وجوی برخی عبارات را در موتورهای جست‌وجو ندارند. اینترنت مدارس نیز بسیار محدود هستند.

#### سخن پایانی

به نظر می‌رسد که در حال حاضر، تهدید اصلی کشور در مورد فضای مجازی، فقدان گفتمان امنیتی در مورد این پدیده است. فقدان دانش جامع‌نگر در مورد صورت مسئله و عدم وجود مطالعات سیاست‌گذاری مقایسه‌ای در کشور، حاکمیت روش آزمون خطا و اعمال سلاقی فردی و سازمانی را به دنبال داشته است. مسئولیت‌پذیری دولت در سیاست‌گذاری علمی، کارشناسانه و همه‌سونگر و بهره‌گیری از تمام توان علمی کشور، شرط اصلی تحقق بیشترین منافع و کمترین آسیب‌ها از فضای مجازی در ایران است.

برای جلوگیری از آثار مخرب ارتباط با پایگاه‌های ضداخلاقی و ضدفرهنگی باید به سویی حرکت کنیم که سایت‌های مفید، جذابیت پیدا کند؛ یعنی ابتدا در حد توان باید در زمینه سایت‌های مفید و درعین‌حال جذاب سرمایه‌گذاری کنیم. از طرف دیگر، باید موارد منفی را سد کنیم؛ یعنی از نفوذ سایت‌های مخرب، به این سو جلوگیری کنیم. در کشورهای غربی، مثل انگلیس، مسئله استفاده از سایت‌های مستهجن توسط

راهکار دیگر را می‌توان راه‌اندازی شبکه ملی

اطلاعات برشمرد که نقطه بسیار مطلوب برای بهره‌مندی بهینه و اثربخش از فضای مجازی و شبکه‌های اجتماعی است.

بررسی اقدامات کشورهای یادشده در خصوص مدیریت فضای اینترنت، نشان می‌دهد که کشور ما با خلأ آینده‌پژوهی و نگرش جامع در حوزه مدیریت فضای مجازی و حاکمیت داده مواجه است. این در حالی است که در مفهوم شبکه ملی اطلاعات، تعریف واحدی از حاکمیت و استقلال جمهوری اسلامی ایران در فضای مجازی گنجانده شده و باید از سوی مسئولان جدی گرفته شود. ■

#### منابع

۱. مقاله «نظارت بر فضای مجازی در کشورهای مختلف جهان»، وبگاه خبرگزاری صداوسیما، دسترسی: ۱۳۹۹/۷/۱، نشانی: [www.iribnews.ir](http://www.iribnews.ir)
۲. هاتف، مهدی. ۱۳۸۸. «چالش‌ها و چشم‌اندازهای امنیت در فضای مجازی». دوماه‌نامه توسعه انسانی پلیس، شماره ۱.
۳. «نقشه راه چین برای فضای مجازی در افق ۲۰۲۰»، برگرفته از وبگاه مرکز ملی فضای مجازی، دسترسی: ۱۳۹۹/۶/۲۵، نشانی: [www.majazi.ir](http://www.majazi.ir)
۴. بخشی‌پور، معصومه. «شبکه ملی اطلاعات، نقطه ایده‌آل حکمرانی سایبری». وبگاه خبرگزاری مهر، گروه دانش و فناوری، دسترسی: ۱۳۹۹/۴/۲۰، نشانی: [www.mehrnews.com](http://www.mehrnews.com)