دو فصلنامه علمی مطالعات بیداری اسلامی، دوره نهم، شماره اول (پیاپی ۱۷)، بهار و تابستان ۱۳۹۹

نوع مقاله: پژوهشی تاریخ دریافت: ۱۳۹۹/۱۰/۱۶ تاریخ پذیرش: ۱۳۹۹/۱۱/۱۳ صص: ۳۰۹-۲۸۱

واکاوی حاکمیت دولت بر فضای مجازی؛ مطالعه موردی عربستان در مواجهه با معارضان

سیدمهدی سهیلی‌مقدم[۱]

چکیده

فضای مجازی یک حیطه سیاسی اجتماعی و فناوری با ویژگی های منحصر به فرد است که از مرزهای سرزمینی و قانونی کشورها فراتر رفته است و بیشتر توسط بخش خصوصی اداره می‌شود، اما کشورهای توسعه یافته با سازوکارهایی همچون همکاری با سازمان‌های بین‌المللی و دیگر کشورها، سعی در اعمال نفوذ در این فضا هستند. این واقعیت باعث شده تا موثرترین مدل حکمرانی در کنترل جوامع مطرح شود تا با وجود کنترل‌ها همچنان آزادی‌های نسبی حفظ گردد. روش تحقیق در این مقاله با انتخاب نمونه هدفمند و تجزیه و تحلیل اطلاعات گردآوری شده، صورت گرفته است. از این رو نحوه مواجهه حاکمیت دولت عربستان با معارضان در فضای مجازی به عنوان مطالعه موردی مورد بررسی قرار گرفته است. یافته ها نشان داد که حاکمیت کنونی فضای مجازی در سیطره و سلطه استکبار جهانی است و دولت پادشاهی عربستان نیز از طریق قدرت سانسور، فیلتر و کنترل فضای مجازی امکان بهره‌مندی انقلابیون و معترضان از این بستر را با محدودیت هایی روبرو نموده است. با این وجود شناخت و سازمان دهی معارضین در این فضا، به عنوان بهترین بستر ارتباطی در جهان معاصر، می تواند نقش شتاب دهنده در روند بیداری اسلامی در جهان عرب داشته باشد.

واژه‌گان کلیدی: فضای مجازی؛ حاکمیت دولت؛ عربستان سعودی؛ فیلترینگ

[۱] دانشجوی دکتری اقتصاد و مدیریت، دانشگاه فدرال جنوبی، رستوف، روسیه.(نویسنده مسئول)
info@fadak.ir 000-0003-1602-3875

مقدمه

موضوع حکمرانی فضای مجازی سه مفهوم را به ذهن اهل فن متبادر می‌کند، اول حکمرانی از طریق فضای مجازی، انجام وظایف حکومتی مثل دولت الکترونیک دوم حکمرانی در فضای مجازی، باز تعریف حاکمیت سرزمینی در فضای مجازی مثل امنیت سایبری شهروندان و کاهش جرایم در این حوزه سوم حکمرانی بر فضای مجازی، باز تعریف سیاست های حکومتی برای شکل دادن به فعالیت ها در فضای مجازی، رویه های قانونی و مشروع همچنین روابط میان بازیگران و گروه‌های اجتماعی مختلف را تنظیم کنند. به گفته پروفسور نازلی چوکریم ، فضای مجازی با ویژگی های زمانی: موقتی بودن (نزدیک شدن به لحظه متعارف با لحظه ای نزدیک)، فیزیکی (محدودیت های جغرافیایی و موقعیت فیزیکی فراتر می‌رود)، نفوذ (نفوذ به مرزها و حوزه های قضایی)، سیال بودن (آشکار شدن تغییرات پایدار و پیکربندی ها)، مشارکت (موانع فعالیت و بیان سیاسی را کاهش می‌دهد)، انتساب (هویت بازیگران را پنهان می‌کند و پیوندهای مربوط به عمل را) و پاسخگویی (سازوکارهای مسئولیت را نادیده می‌گیرد.). به طور عام فضای مجازی را محیطی متشکل از اجزای فیزیکی و غیر فیزیکی توصیف نموده اند که با استفاده از رایانه قابلیت ذخیره اصلاح و تبادل داده ها را دارد.(Boothby, 2014, p. 123) به واقع فضای مجازی یک شبکه دیجیتالی جهانی است که تمامی‌سطوح زندگی روزمره آدمی‌نهفته و در جریان است. پس تنها اینترنت را شامل نمی‌شود بلکه زیرساخت های مهمی‌همچون شبکه های برق ، سیستم های تامین آب، معاملات بانکی و سیستم های حمل و نقل را در جوامع مدرن شامل می‌شود. در ایالات متحده و اتحادیه اروپا ، تقریباً ۹۰٪ از زیرساخت های حیاتی رایانه توسط بخش خصوصی اداره می‌شود.(Dunn Cavelty, 2014, p. 160)

طی دو دهه گذشته ، فضای مجازی به حوزه جدیدی برای تعامل انسان تبدیل شده است و ارتباطات و تبادل اطلاعاتی که ارائه می‌دهد عملاً از اندازه جهان کاسته است. تقریباً یک سوم جمعیت جهان به اینترنت دسترسی دارند و عنصر مهمی‌در انتقال و انتشار اطلاعات محسوب می‌شود و به طبع آن به عنصر مهمی‌در انتقال و انتشار قدرت تبدیل شده است.(*Ebert &*

Maurer, 2013) فضای مجازی با موضوعاتی امنیتی یا جرم و جنایت در آمیخته شده است حتی موارد جاسوسی سایبری، از دست دادن داده ها مسائلی است که روزانه عناوین خبری را متشکل می‌شوند. دولت ها ، سازمان های بین المللی، شرکت های خصوصی و فعالان حقوق بشر در تلاشند طیف گسترده ای از فعالیت هایی را که در فضای مجازی است تنظیم کنند در عین حال تعادل بین محافظت از زیرساخت های حیاتی، آزادی های مدنی، استانداردهای فنی و هزینه را تنظیم کنند.

فضای مجازی چالشی بزرگ برای ایده سنتی حاکمیت جهانی است که عمدتاً دولت محور است. این محیط به دلیل ویژگی های نامتقارن ، ناشناس و استفاده دوگانه ، درک سنتی از مفاهیم کلیدی مانند امنیت ، مرزها ، حقوق بشر ، حفظ حریم خصوصی و حاکمیت را به چالش کشانده است.(Emerson, 2016; A. Liaropoulos, 2015; A. N. Liaropoulos, 2016; Slack, 2016) این امر خصوصیات سیاسی-اجتماعی و تکنولوژیکی این حوزه جدید است که به طور مداوم در حال باز تعریف است(*Choucri, 2012, p. 7*) سرعت سریع تغییر فناوری و نحوه پاسخگویی جوامع در حوزه دیجیتال بر منافع دولتی و غیر دولتی تأثیر می‌گذارد. پیشرفت در زمینه فناوری اطلاعات ، مانند اینترنت اشیا(*Weber, 2013*)، داده بزرگ *(Cukier & Mayer-Schönberger, 2013)* و وب تاریک(*Chertoff et al., 2015*) از توانایی دولت ها و حتی سازمان های بین المللی پیشی گرفته است. روابط بخش خصوصی و دولتی در این فضای به یک پارادوکس شباهت دارد. از این رو دولت ها از بخش خصوصی می‌خواهند تا با انجام سانسور و اعمال محدویت ها و حتی نظارت مورد خواست حاکمان، در امور امنیت سایبری به دولت متبوع خود کمک کند.

هدف این مقاله برجسته کردن فرصت های فضای مجازی در سرعت بخشی و به ثمر رسیدن انقلاب ها در کشورهای عربی است. در قسمت اول ایده حاکمیت فضای مجازی در رابطه با حاکمیت دولت بررسی می‌شود مواردی همچون حاکمیت توزیع شده، حاکمیت چندجانبه و

سهامداران چند جانبه به وضوح چالش هایی را نشان می‌دهد که دولت ها هنگام تنظیم استفاده از فضای مجازی در مرزهای خود با آن روبرو می‌شوند. بخش دوم به جستجوی شواهد تجربی در مورد حاکمیت فضای مجازی در کشور عربستان می‌رود. قسمت آخر، بر تضاد قدرت بزرگ در این فضا و عدم تقارن قدرت میان غرب و جنوب جهانی تأکید دارد.

مفهوم حاکمیت به نهادهای دولتی و سازوکارهای نظارتی غیررسمی‌اشاره دارد که فعالیت های جمعی یک جامعه را هدایت و مهار می‌کنند. حکمرانی سیستمی، روشهای حاکمیتی را نشان می‌دهد که در آن مرزهای بخش دولتی و خصوصی مشخص نیست. حاکمیت معنای وسیع تری نسبت به دولت دارد. دولت دستگاه اجرایی است که می‌تواند مخالفت گسترده با سیاست های موجود داشته باشد، در حالی که حاکمیت نیاز به پذیرش اکثریت افرادی دارد که آن را تحت تأثیر قرار می‌دهند. اصطلاح حاکمیت اصطلاحی کاملاً مبهم است که به روشهای مختلفی در ادبیات روابط بین الملل استفاده شده است. منظور از حاکمیت جهانی ، ایجاد یک دولت جهانی نیست ، بلکه به تلاش های مشترک دولت ها ، سازمان های بین المللی و بازیگران غیر دولتی برای مقابله با چالش های مشترک فراتر از مرزهای ملی اشاره دارد.(*Patrick, 2014, p. 59*) حکمرانی جهانی را می‌توان به عنوان تصویری از حکمرانی در غیاب دولت درک کرد.(*Finkelstein, 1995*)

به طور خلاصه ، نکات اصلی در ادبیات مربوط به حاکمیت جهانی شامل موارد زیر می‌شود(Nye & Donahue, 2000; Paterson et al., 1992; Rosenau, 1995) اول، اینکه تغییر رویکرد از سطح ملی به سطح جهانی و به سطوح فراتر از یک دولت. دوم، اینکه سیاست جهانی چیزی فراتر از سیاست بین دولتی است و محدوده اختیارات آن فراتر از دولت افزایش یافته است. پس اگر نمایندگان از استاندارد عقلانیت، شفافیت و پاسخگویی برخوردار بوده و در یک فرایند تصمیم گیر توافق کرده اند، این قوانین فراتر از دولت قانونی هستند. پس حکمرانی جهانی بطور انحصاری توسط دولتها و سازمانهای بین المللی انجام نمی‌شود بلکه توسط بخش

خصوصی و سازمانهای غیردولتی *(NGO)* نیز انجام می‌شود. در نتیجه ، دولت ها به عنوان ابزار اصلی حاکمیت جهانی جایگزین نمی‌شوند، بلکه توسط بازیگران دیگری تکمیل می‌شوند. (Nye (& Donahue, 2000

سوالات اولیه در مواجهه با موضوع حاکمیت فضای مجازی این چنین است:(Cornish, 2015; Ron Deibert, 2015; DeNardis, 2014; Jayawardane et al., 2015; Weitzenboeck, 2014; West, 2014) آیا در وهله اول باید فضای مجازی اداره شود؟ چه کسی باید در حکومت داری نقش داشته باشد؟ فضای مجازی چگونه باید اداره شود؟ آیا حاکمیت ترکیبی که شامل مشارکت عمومی‌و خصوصی است در فضای مجازی قابل استفاده است؟ چگونه کشورها می‌توانند حاکمیت خود را در فضای مجازی اعمال کنند؟

موضوعات فوق را می‌توان در سه رویکرد اصلی طبقه بندی کرد: حاکمیت توزیع شده، حاکمیت چند جانبه و مشارکت چندجانبه*(West, 2014, p. 4)*در اوایل توسعه اینترنت، می‌توان حاکمیت را به عنوان یک سیستم توزیع شده توصیف کرد. حاکمیت در جوامع آنلاین، غیر سازمان یافته و محدود بود ، آنها ادعا می کردند که اطلاعات به صورت آزاد در این فضا قرار گرفته و قابل کنترل نیست.*(Ronald Deibert & Crete-Nishihata, 2012, pp. 341–342)* این رویکرد بازتابی از دورانی است که جوامع آنلاین در آن کوچک ، همگن و قادر به تنظیم خود هستند. در سال ۱۹۹۶ ، جان پری بارلو ، بنیانگذار بنیاد الکترونیکی مرز *(EFF)* در اعلامیه استقلال فضای مجازی اظهار داشت که "دولت ها از جمع ما استقبال نمی‌کنند ... فضای مجازی در مرزهای شما نیست ... ما هستیم قرارداد اجتماعی خود را تشکیل می‌دهیم. این حاکمیت با توجه به شرایط جهان کنونی به وجود آمده است.*(Barlow, 2016)* در دهه ۱۹۹۰، اینترنت کمتر از یک میلیون کاربر داشت و در مرحله ابتدایی توسعه قرار داشت. امروزه ،کاربران اینترنت را میلیاردی محاسبه می‌کنند که به بخشی جدایی ناپذیر از جوامع مدرن تبدیل شده است.*(Betz & Stevens, 2011)* فضای مجازی به مهمترین زیرساخت جهان رسیده است و هر جا که نیازمند قوانین و مقررات است تکمیل گشته است.

۱. مدل حاکمیت توزیع شده ، اگرچه هنوز در برخی از جوامع آنلاین محبوبت دارد، اما نمی‌تواند راه حلی جامع سیاستی و کارآمد ارائه دهد که مورد پذیرش جامعه بزرگ و متنوع کاربران فضای مجازی قرار گیرد.

کسانی که به فضای مجازی به عنوان موضوع جهانی نگاه می‌کنند بر این اعتقاد دارند که نقش حاکمیتی دولت ها در این حوزه محدود گردد. چرا که در مقایسه با خشکی، دریا، هوا و فضا ، فضای مجازی حوزه ای ساخته بشر است که فاقد فضای فیزیکی و در نتیجه فاقد مرز است. فضای مجازی شامل یک زیرساخت مشترک جهانی است، اما یک امر مشترک جهانی نیست.(Cornish, 2015, p. 158) فضای مجازی به نظر می‌رسد بدون مرز است، اما در واقع به زیرساخت های فیزیکی محدود شده که انتقال داده ها و اطلاعات را تسهیل می‌کند. چنین زیرساختهایی بیشتر متعلق به بخش خصوصی است و در قلمرو حاکمیت دولت ها واقع شده است. شکی نیست که دولت ها در تلاشند تا به اصطلاح پارادوکس مرزی را پشت سر بگذارند و مرزهای مجازی را توسعه دهند(Demchak & Dombrowski, 2014) لوئیس با صراحت فضای مجازی را به عنوان یک فضای مشترک دارای صاحبان بسیار توصیف کرده است. (Lewis, 2010) پل کورنیش فضای مجازی را به عنوان عوام مجازی که نه مالکیت خصوصی است ، نه قلمرو حاکمیتی است و نه حوزه جهانی به همان روشی که دریا و هوا در نظر گرفته می‌شود.(Cornish, 2015, pp. 158–159)

مسئله حاکمیت دولت برای طرفداران حکومت چند جانبه از اهمیت اساسی برخوردار است. رویکرد چند جانبه فضای مجازی با اصطلاحات هابزی مشاهده می‌شود. حامیان این رویکرد دولتمحور، فضای مجازی را به عنوان حوزه ای آشفته که ناامنی را تقویت می‌کند، درک می‌کنند و استدلال می‌کنند که حاکمیت تدوین کننده سیاست در فضای مجازی است. این رویکرد باعث ایجاد یک نهاد در سازمان ملل متحد (سازمان ملل) شده که مسئولیت و اداره فضای مجازی را بر عهده دارد، اما در عین حال برخی کشورها قدرت تعیین سیاست های ملی خود را به صورت

مستقل نیز دارند این مدل چندجانبه به طور سنتی توسط روسیه، چین، هند، ایران و عربستان سعودی پشتیبانی می‌شود. پس از افشای ادوارد اسنودن، حاکمیت چند جانبه حتی در برخی از کشورهای عضو اتحادیه اروپا که به دنبال محافظت از مرزهای سایبری و داده های خود از سیستم های نظارتی ایالات متحده هستند، شتاب بیشتری به خود گرفته است(West, 2014, p. 7) دولت های ملی سیاست های حفظ حریم خصوصی توسط شرکت های فراملی مانند گوگل، فیس بوک و توییتر را تهدیدی برای حاکمیت دیجیتال و در نتیجه امنیت ملی می‌دانند. (Nocetti, 2015, p. 114) گفته شده است که در دوران تضاد قدرت بزرگ، اعمال حاکمیت دولت به منظور تأمین دارایی های دیجیتال ملی و زیرساخت های مهم، می‌تواند منجر به تکه تکه شدن - بالکان سازی فضای مجازی شود. مسئله کورنیش این بود که این تکه تکه شدن در واقع یک پیشرفت منفی است و باید تهدیدی برای فضای مجازی بر شمرد یا اینکه جایگزینی معتبر برای آن معرفی شود(Cornish, 2015, p. 159) کشورها این انتخاب را دارند که از اینترنت فعلی جدا شوند و شبکه های اینترانت محلی یا ملی یا منطقه ای خود را تشکیل دهند. آنها در حال بررسی گزینه ایجاد «فضاهای سایبری ملی»، ساخت کابل های بین اقیانوسی و ذخیره داده های اینترنتی بر روی سرورها در سرزمین های ملی خود هستند. اطمینان از حفاظت و یکپارچگی داده ها از اهمیت حیاتی برخوردار است. با این وجود، ما باید ابزار محلی سازی داده ها را در نظر بگیریم. ذخیره اطلاعات در سرزمین های ملی، آنها را برای هکرهای خارجی غیرقابل مشاهده می‌کند. امروزه جغرافیا و مرزهای جغرافیایی نیست که امنیت را تعریف می‌کند، بلکه عمدتا فناوری و رمزگذاری است که امنیت را در دنیای دیجیتال تعریف می‌کند.

۲. طرفداران رویکرد چندجانبه ، حاکمیت اینترنت را به مفهوم حاکمیت وستفالیای می‌داند به این معنا که در حقوق بین‌الملل اصل بر عدم مداخله در امور داخلی کشورها است و هر دولت ملی بر قلمرو و امور داخلیش دارای حاکمیت است فارغ از این که چقدر بزرگ یا کوچک باشد و همه در حقوق بین‌الملل با هم برابر هستند. بنابراین همچون اتحادیه بین المللی ارتباطات از راه دور در نظر گرفته می‌شود. حمایت از حاکمیت دیجیتال و امنیت اطلاعات اولویت های اصلی کشورهایی

است که از مدل حاکمیت چندجانبه استقبال می‌کنند. مثال دیگری که تا حدودی با مدل چندجانبه متناسب است، سازمان همکاری شانگهای *(SCO)* است. روسیه، چین، هند، ایران و سایر کشورهای آسیای میانه سیاست های امنیتی اینترنت خود را از طریق سازمان همکاری شانگهای هماهنگ کرده و تمرینات سایبری را برای مقابله با خیزش های سیاسی مجهز به اینترنت انجام داده اند. اینترنت کاملاً کنترل شده را ترجیح می‌دهید.(Ron Deibert, 2015, p. 13)

در سال ۲۰۱۱ چین ، روسیه، تاجیکستان و ازبکستان برای اولین بار یک قانون رفتار بین المللی در مورد امنیت اطلاعات برای توجه به کشورهای عضو سازمان ملل منتشر کردند. ایالات متحده و سایر کشورهای غربی این موضوع را رد کردند، با این استدلال که این امر منجر به کنترل کشور و محتوای آنلاین توسط کشورها می‌شود. در سال ۲۰۱۵ چین، روسیه، قزاقستان، قرقیزستان، تاجیکستان و ازبکستان به طور مشترک به روزرسانی قانون رفتار بین المللی خود در زمینه امنیت اطلاعات را به دبیرکل سازمان ملل متحد ارائه داده و بر ضرورت ایجاد قانون بین المللی جدید برای فضای مجازی بار دیگر تأکید کردند.

برخلاف آنچه در بالا ذکر شد، مدل حاکمیت چند سهامدار شامل بازیگران ایالتی و غیر دولتی است که نماینده بخش تجارت و جامعه مدنی هستند. منطق این است که دولتها به تنهایی نمی‌توانند فضای مجازی را با موفقیت تنظیم کنند. بنابراین سایر بازیگران مانند شرکت های فنی، موتورهای جستجو، کاربران اینترنت و سازمان های مدنی نیز باید در حاکمیت اینترنت دخیل باشند. مایکروسافت، اپل، گوگل، یاهو، ویبو، اسکایپ، دراپ باکس، آمازون، توییتر، فیس بوک و بادو تنها برخی از شرکت های متعدد ، ارائه دهندگان فنی و موتورهای جستجو هستند که داده ها را جمع آوری و ذخیره می‌کنند. طرفداران مدل حاکمیت چندجانبه و چند ذی نفع استدلال می‌کنند که هنجارهای فضای مجازی توسط کاربران اینترنت پذیرفته می‌شود چرا که آنها بخشی از این هنجار هستند. این امر موجب افزایش مشروعیت و اقتدار نهادها، سازمان ها و شرکت ها در فضای مجازی می‌شود.*(Mihr, 2014)* با حمایت ایالات متحده، انگلیس، کانادا، استرالیا و

سازمانهایی مانند گوگل و ICANN ، مدل چند سهامدار در دوران قبل از اسنودن بسیار محبوب بوده است. پس از افشای اسنودن، حقانیت و اعتبار این روش بطور قابل توجهی تضعیف شده است.(Ron Deibert, 2015, p. 13)

حاکمیت چند جانبه و چند ذی نفعان در ITU ، *ICANN*، IGFو NETmundial بعنوان نماینده مجامع حاکمیت جهانی در نظر گرفته می‌شوند. هر مورد بینش متفاوتی در مورد کاربردها و محدودیت های حاکمیت چند جانبه و مشارکت چندجانبه برای ما فراهم می‌کند. گرچه امروزه مشارکت چندجانبه ای به عنوان رویکرد اصلی در حاکمیت اینترنت در نظر گرفته می‌شود، فقط در سال ۲۰۰۲ بود که مجمع عمومی‌سازمان ملل متحد (UNGA) نقش سایر شرکت کنندگان، به غیر از ایالت ها، را در حفاظت از فضای مجازی شناسایی کرد. به طور خاص، قطعنامه UNGA 57/239 اشاره به «دولت ها، مشاغل، سایر سازمان ها و کاربران فردی داشت که سیستم های اطلاعاتی و شبکه ای را توسعه، مالک، تأمین، مدیریت، سرویس و استفاده می‌کنند». طبق این مصوبه، شرکت کنندگان باید مسئولیت پذیری را بر عهده بگیرند و برای افزایش امنیت این فناوری های اطلاعاتی، به روشی متناسب با نقش آنها، گام بردارند (کرمر و مولر ۲۰۱۴: ۱۵). اصطلاح "ذینفعان" برای اولین بار در قطعنامه *UNGA 58/199* از سال ۲۰۰۳ ظاهر شد. در سال ۲۰۱۰ ، گزارش *A / 65/201* از گروه دولتی حکومتی سازمان ملل *(GGE)*، بر اهمیت «همکاری بین کشورها» بخش خصوصی و جامعه مدنی تأکید کرد، بدین ترتیب نقش برابر جامعه مدنی را در اداره فضای مجازی به رسمیت می‌شناسد.*(Kremer & Müller, 2014)*

مشارکت چند جانبه، طرفدار مشارکت همه فعالان مرتبط با حاکمیت فضای مجازی است. این بازیگران نه تنها شامل کشورها، بلکه بازیگران غیردولتی متنوعی هستند، مانند گروه های جامعه مدنی ، نمایندگان بخش خصوصی، رسانه ها و دیگر بازیگران تنظیم کننده ارتباطات در فضای مجازی. مزیت رویکرد چند ذی نفع این است که همه بازیگران مربوطه می‌توانند به صورت برابر مشارکت داشته و سخن آنها شنیده شود.*(Mihr, 2014, p. 28)*فراگیر بودن و نمایندگی از

اصول اصلی این رویکرد است. در یک سناریوی ایده آل، ذینفعان نه تنها هنجارهایی تولید نمی‌کنند و استانداردهای خاص خود را تعیین می‌کنند، بلکه عواقب یا مجازات های احتمالی عدم رعایت آنها را نیز تعریف می‌کنند.(Mihr, 2014) مالکیت چند جانبه را نباید به عنوان یک هدف به خودی خود درک کرد، بلکه باید آن را فرآیندی برای رسیدن به یک حاکمیت موثر دانست. هدف چند جانبه گرایی نمی‌تواند که جایگزین کشورها شود. علاوه بر این، ذینفعان همه به یک شکل و به یک میزان در اداره فضای مجازی مشارکت ندارند. به عنوان مثال، بازیگران جامعه مدنی ، سازمانهای بخش خصوصی و اندیشکده های جهانی ممکن است نقش اصلی را در شکل دهی و نهادینه سازی هنجارهای رفتار در فضای مجازی داشته باشند، اما تنها کشورها هستند که می‌توانند مقررات را اجرا کنند(Jayawardane et al., 2015, pp. 4–5).

سیاست قدرت بزرگ و مبارزه بر سر فضای مجازی

فضای مجازی از سیاست مصون نیست. این عقیده رایج که فضای مجازی می‌تواند یک مدینه فاضله آزادیخواهانه باشد ، در دوران اینترنت اشیا و داده های بزرگ کاملاً غیر واقعی به نظر می‌رسد. فضای مجازی منطقه غیرسیاسی بازیگران غیر دولتی نیست. برعکس، این حوزه ای است که دولت ها به دنبال اعمال حاکمیت خود هستند. در نتیجه، حاکمیت فضای مجازی به یک بازی سیاست قدرت شباهت دارد. پرونده ITU (ITU: Committed to Connecting the World, n.d.) و تا حدودی *SCO* ، به شفافیت نشان می‌دهد که حاکمیت دولت در فضای مجازی دور از انتظار نیست، بلکه در بعضی موارد به عنوان تنها منبع مناسب اقتدار در نظر گرفته می‌شود.(Choucri, 2012, p. 160) مسئله مورد بحث این نیست که آیا کشورها در فضای مجازی بر حاکمیت ادعا می‌کنند یا نه، بلکه چگونه نباید بر حاکمیت بر فضای مجازی ادعا کنند.(*Slack, 2016, p. 74*)

نکته دیگری که باید مورد توجه قرار گیرد روندهای جمعیت شناختی آینده در فضای مجازی است. در گذشته فضای مجازی تحت سلطه غرب بود، براساس آمار فعلی کاربران اینترنت و

روندهای کلیدی جمعیتی، دنیای غیر غربی در زمینه حاکمیت فضای مجازی کمتر نمایان است.(Demidov, 2014) اما در آینده نزدیک چنین نخواهد بود، امروزه فقط ۳۰٪ از جمعیت جهان به اینترنت دسترسی دارند. میلیاردها کاربر بعدی فضای مجازی از جهان غیر غربی سرچشمه می‌گیرند(Demidov, 2014, p. 9) بسیاری از این کشورها درک وستفالیایی از ایالت را پذیرفته اند که به طور سنتی از مدل حکمرانی چند جانبه طرفداری می‌کند. این کشورها مزایای مالی اینترنت باز را تشخیص می‌دهند، اما در عین حال از قدرت بالقوه اختلال آور اینترنت و خطرات امنیت سایبری ترس دارند.

تحلیل چند ذی نفع بودن کاستی هایی را از خود نشان داده است. نگرانی های موجهی در مورد عدم تعادل نمایندگی گروه های جامعه مدنی و شرکت های خصوصی، نقشی که ممکن است ایفا کنند و توانایی آنها در واقع تأثیرگذاری در تصمیم گیری وجود دارد (Dilipraj, 2014, p. 4; West, 2014, p. 9) مشارکت چندجانبه همیشه به طیف وسیع تری از دیدگاه ها یا بازنمایی جهانی تر منافع منجر نمیشود(Pohle, n.d.) این کار به منظور کاهش ارزش نقش چندجانبه نیست، بلکه قرار دادن این رویکرد در یک زمینه عملی است. از این گذشته، نیاز به ایجاد شبکه های خبره، دولتی و غیردولتی، فنی و سیاست مدار را نباید دست کم گرفت.(Slack, 2016, p. 74)

وضعیت فعلی حاکمیت فضای مجازی نشان می‌دهد که تقاضا برای حاکمیت زیاد است ، اما به نظر نمی‌رسد که یک معاهده سایبری گسترده وجود داشته باشد. به نظر می‌رسد شواهد اخیر حاکمیت فضای مجازی رویکرد پاتریک در مورد چند جانبه گرایی را تأیید می‌کند. وی استدلال می‌کند که روشهای موثر حکمرانی کمتر در نهادهای رسمی‌و بیشتر در سازمانهای منطقه ای در میان کشورهای همفکر(Patrick, 2014) اتفاق می‌افتد. بحث این است که از آنجا که هیچ معاهده ای در سازمان ملل نمی‌تواند طیف وسیعی از موضوعات مرتبط با سایبر (جنگ سایبری، جرایم اینترنتی، حمایت از حقوق شهروندی و غیره) را تنظیم کند، رویکرد عملی تر این است که به جنبه های خاصی توجه شود.

مفهوم جدیدی در حکمرانی نوین شکل گرفته است که آن را «حکمرانی خوب[۲]» نامیده‌اند که مردم را در رسیدن به منافع و مزایایی مورد نیاز کمک می‌نماید. مولفه های این حکمرانی توسط کمیسیون اقتصادی، اجتماعی آسیا و اقیانوس آرام[۳] این چنین بر شمرده شده است. مدیریت مشارکتی[۴] که مردم در تمامی فرآیندها به ویژه تصمیم‌گیری‌ها مشارکت دارند خواه مشارکت مستقیم یا خواه غیر مستقیم (به واسطه نمایندگان). حاکمیت قانون[۵] که وظیفه حکمرانان بی طرفانه و در چهارچوب های عادلانه[۶] و منصفانه عمل کرده تا به اقشار آسیب پذیر جامعه آسیب وارد نشود. پس پاسخگو[۷] بودن حاکمیت به مردم به واسطه اطلاعات شفاف[۸] در جریان قرار گیرد. این جریان اطلاعات قابل فهم در دسترس همگان قرار گیرد از این رو از قوانین و مقررات مشخصی که از پیش تعیین شده پیروی کند. استفاده بهینه، کارا[۹] و مناسب از منابعی که در اختیار حاکمیت در جهت رفع نیازهای مردم است حس مسئولیت[۱۰] حکمرانان در جهت تامین خواسته‌ها و تمایلات مردم ی تامین منافع نظرات متفاوت برای دستیابی به یک اجتماع گسترده[۱۱]

فضای مجازی برخی از این مولفه ها که در سیستم سنتی حکومت‌داری بود تحت تاثیر قرار داده است، برای نمونه، مشارکت مستقیم مردم در فرایندهای تصمیم‌گیری در سیستم سنتی حکومت داری به ندرت (انتخابات) صورت می گیرد. درحالی که فضای مجازی این امکان را فراهم می کند که همه به صورت مستقیم در تصمیم گیری ها مشارکت داشته باشند. به عبارت دیگر ابزارهای رصد فضای مجازی این امکان را برای حکمرانان فراهم می کنند که فهم صحیحی از نوع نگرش مردم به یک پدیده خاص یا پدیده ها داشته باشند. رصدی که حتی به لحظه و بی

---

[2] Good Governance
[3] Economic and Social Commission for Asia and Pacific
[4] Participation
[5] Rule of Law
[6] Inclusive Equity
[7] Responsiveness
[88] Transparency
[9] Effectiveness and Efficiency
[10] Accountability
[11] Consensus Oriented.

درنگ است. جریان دسترسی آزاد به اطلاعات به مردم و رابطه دوسویه با نخبگان حاکمیتی در فضای مجازی می‌تواند منجر به مشارکت فعال مردم و افزایش عدالت اجتماعی گردد.

فضای مجازی تنها ابزار نیست بلکه توانمند سازی[۱۲] را نیز فراهم می کند تا جامعه توانا شده و حتی بالاتر از آن توانمند شود پس اگر این ابزار از جامعه و مردم گرفته شود او توانمند باقی خواهد ماند. فضای مجازی بسیج مردمی در حل مشکلات را به همراه خواهد داشت زمانی که جامعه در تصمیمات مشارکت دارند باعث افزایش همگرایی و کاهش واگرایی می شود. از این رو فضای مجازی در تمامی هشت مولفه حکومت خوب نقش دارد و توجه به آن بسیار مهم است. اما حکمرانان عربستان به چه اندازه به این مولفه ها توجه دارند پس از پایان واکاوی حاکمیت دولت عربستان در حوزه فضای مجازی بیان خواهد شد.

حاکمیت فضای مجازی عربستان

تا پیش از سال ۱۹۹۸ استفاده از اینترنت در کشور عربستان ممنوع بود. ارایه اینترنت در این کشور از سال ۱۹۹۴ با اتصال مراکز علمی‌و پژوهشی در این کشور به شبکه جهانی آغاز گردید. دسترسی مجاز تا سال ۱۹۸۸ به طول انجامید و سال بعد از آن یعنی ۱۹۹۹ دسترسی به جامعه و مردم عربستان داده شد. تعداد کاربران اینترنت در این کشور بیش از نود و یک درصد است به عبارت دیگر از جمعیت سی و چهار میلیونی این کشور بیش از سی و یک میلیون نفر به اینترنت دسترسی دارند. (Middle East Internet Stats and Telecommunications Reports, n.d.) در مجموع سه موضوع، این بخش مورد بررسی قرار خواهد گرفت: یک. مهمترین مراکز مرتبط با حاکمیت فضای مجازی دوم. اسناد بالادستی در این حوزه و سوم. فیلترینگ در عربستان و ابعاد مختلف آن.

[12] Empowerment

الف. مراکز فضای مجازی در عربستان

کمیسیون ارتباطات و فناوری اطلاعات[۱۳] (*CITC*) مسئول وضع قوانین سیاست ها و آیین نامه ها و اجرای آنها در کشور عربستان است. همچنین مسئولیت «سامانه نام دامنه» (*DNS*) ملی است. این کمیسیون مسئول تدوین سیاست‌ها، قوانین و آیین نامه‌ها در حوزه فناوری اطلاعات و ارتباطات است. این کمیسیون دارای شخصیت حقوقی است و از نظر مالی و سازمانی مستقل است و بر مبنای قانون توسط مخابرات عربستان، در سال ۲۰۰۱ تأسیس شده است. نام این نهاد در ابتدا کمیسیون مخابرات بود، اما در سال ۲۰۰۶ به عنوان کنونی تغییر نام داد.

کمیسیون دارای هیئت مدیره ای مرکب از ۱۰ نفر است. وزیر ارتباطات و فناوری اطلاعات رئیس هیئت مدیره و نمایندگانی از وزارت ارتباطات و فناوری اطلاعات، وزارت سرمایه گذاری و تجارت، وزارت امور مالی، سازمان امنیت و شهرک علم و فناوری ملک عبدالعزیز به همراه سه نفر از بخش خصوصی سایر اعضای هیئت مدیره را تشکیل می‌دهند. ۱۰۰ درصد کارکنان این کمیسیون را شهروندان با ملیت سعودی تشکیل میدهند ۹ درصد از کارکنان این کمیسیون را زنان و ۹۱ درصد آن را مردان تشکیل می‌دهند.(*Alassim et al., 2017*) هیئت مدیره دارای سه کمیته اجرایی، نظارت و تخلقات است. ساختار کمیسیون *CITC* و به نوعی ساختار حکمرانی فضای مجازی عربستان در حوزه امنیت دانست، در چارچوبی قانونی برای خدمات کنترل والدین در دسترسی به کودکان و نوجوانان به اینترنت به عبارت دیگر به منظور حمایت از کودکان و نوجوانان از خطرات اینترنت (استفاده از محتوای مضر آن) و همکاری والدین در کاهش آسیب پذیری فرزندان ،کمیسیون از سال ۲۰۱۸ یک چارچوب قانونی برای گسترش ارائه خدمات کنترل والدین به کاربران از طریق ارائه دهندگان خدمات اینترنت صادر کرد به منظور دستیابی به یک محیط امنتر و منفعلتر برای کودکان.) (*Albugami & Ahmed, 2015*)

[13] Communications and Information Technology Commission

وزارت ارتباطات و فناوری اطلاعات[14] ***MCIT*** *(Ministry of Communications and Information Technology, n.d.)* سیاست‌هایی را در حوزه فضای مجازی و *ICT* تدوین می‌نماید و نقش مهمی‌را در اجرای سیاست ها و قوانین بر عهده می‌گیرد. این وزارت همچنین پیش نویسی از قوانینی را در این حوزه برای تصویب به کمیسیون *CITC* پیشنهاد می‌دهد. این وزارتخانه در سال ۱۹۲۶ تأسیس و مسئول تمام ابزارهای ارتباطی و فناوری اطلاعات است. وزارت ارتباطات و فناوری اطلاعات همکاری نزدیکی با کمیسیون ارتباطات و فناوری اطلاعات دارد. در راستای چشم انداز ملی ۲۰۳۰ *(Vision2030, n.d.)*، دولت عربستان و برنامه ملی تحول را تدوین کرده است . وزارت ارتباطات و فناوری اطلاعات از سه آژانس تشکیل شده است:

- الف) آژانس ظرفیت‌های دیجیتال و صنعت تکنولوژی: هدف این آژانس ایجاد یک محیط دیجیتال، متخصصین و افراد ماهر را در تحولات دیجیتالی درگیر، توسعه و جذب میکند و کارهای با کیفیت را در این حوزه افزایش می‌دهد. این امر باعث افزایش بهره‌وری ملی می‌شود، محتوای فنی محلی را توسعه می‌دهد و یک بخش تکنولوژی با سطح رقابتی در سطح جهانی ایجاد می‌کند که اقتصاد پایداری و پیشگام در سطح منطقهای و جهانی را به همراه دارد.(*AlBar & Hoque, 2019*) از وظایف اصلی این آژانس فزایش آگاهی دیجیتالی در میان شهروندان و نیروی انسانی، و تأثیر فناوری‌های دیجیتالی در حوزه اجتماعی و فرهنگی است.
- ب) آژانس ارتباطات و زیرساخت دیجیتال: توسعه زیرساخت‌های دیجیتالی با تنظیم سیاستها و مقررات و تحریک سرمایه‌گذاری برای فعال ساختن بخش فناوری اطلاعات و ارتباطات نقش مهمی‌در توسعه اقتصادی و اجتماعی دارد. از مهمترین اهداف این آژانس تصویب سیاستهای بخش *ICT* و همچنین ایجاد یک پایگاه داده برای بازار فناوری اطلاعات و ارتباطات برای بهبود روند تصمیم گیری. این آژانس در راستای تحقق اهداف فوق سه

[14] Ministry of Communications and Information Technology

وظایف را برعهده دارد، یک. برای سیاست‌های بازار و اقتصاد دو. برای تحریک گسترش باند پهن سه. برای کیفیت زیرساخت د. برای پشتیبانی از اجرای زیرساخت.

- ج) آژانس برنامه‌ریزی و توسعه: هدف خدمت به عنوان یک شریک اصلی، توانمند و پیشرو، با توجه به نیازهای وزارتخانه و کارمندان آن تأسیس شده و وظایف زیر را برعهده دارد: بالابردن کارایی و بهره‌وری کارکنان و به حداکثر رساندن کارایی خدمات عمومی‌در وزارتخانه، با ایجاد یک فرهنگ مسئولیت و صداقت در انجام کار، ایجاد یک محیط کار حرفه‌ای با سطح بالا و استفاده از منابع انسانی مدرن. همچنین برنامه‌ریزی و اجرای تمامی پروژه‌های مربوط به برنامه‌های کاربردی فناوری اطلاعات، نظارت فنی مستقیم تمام کارهای به‌روزرسانی شبکه محلی وزارتخانه یا نصب دستگاهها یا برنامه‌های جدید، طراحی و نگهداری سیستم‌های مرتبط با اینترنت و اطمینان از کیفیت کار با آنها، اطمینان از امنیت سایبری وزارتخانه و آمادگی شبکه محلی آن در برابر حملات سایبری. به طور خلاصه وظایف این آژانس در سه حوزه عملکردی برنامه‌ریزی استراتژیک، سیاستها و مطالعات و توسعه تجاری است.

مجمع مشورتی عربستان سعودی(مجلس الشوری السعودی) این مجمع به عنوان مجلس شورا (*Shura Council*) نیز شناخته می‌شود. این شورا این قدرت را دارد که قوانینی را در حوزه فضای مجازی توسط کمیته حمل و نقل، ارتباطات، فناوری اطلاعات و کمیته امور امنیتی خود به پادشاه عربستان سعودی و کابینه‌اش پیشنهاد کند. این نهاد دارای قدرت اجرایی نیست.

اداره امنیت سایبری عربستان سعودی (*NCA*) مسئولیت رسیدگی به نیازهای استراتژیک و نظارتی پادشاهی را تا آنجا که به امنیت سایبری مربوط می شود ، بر عهده دارد. این شامل جنبه هایی مانند تدوین سیاست ها ، سازوکارهای حاکمیت ، چارچوب ها ، استانداردها ، کنترل ها و دستورالعمل ها است).(*Connell, n.d*.) این اداره از طریق حکم: *National Information Security Strategy(Alsowailm et al., n.d.)* و الهیئة الوطنیة للأمن

السیبرانی *(National Cybersecurity Authority, 2020)* سلطنتی صادر شده توسط پادشاه در تاریخ ۳۱ اکتبر ۲۰۱۷ تأسیس و مورد حمایت قرار گرفته است..

نهادها و اقدامات حاکمیتی همچنین شرکت های دولتی و خصوصی درگیر آن در ابعاد ششگاه فضای مجازی در کشور عربستان که شامل حاکمیت فرهنگی؛ امنیتی؛ فنی؛ اقتصادی؛ مدیریتی و حقوقی را می‌توان در جدول ذیل مشاهده نمود.

حاکمیت	نهادهای حاکمیتی	اقدامات حاکمیتی	برخی از شرکت های دولتی و خصوصی
حاکمیت فرهنگی	وزارت فرهنگ، وزارت رسانه، صندوق فرهنگی *Nomow*، کمیتی امر به معروف و نهی از منکر، کمیسیون ارتباطات و فناوری اطلاعات(*CITC*)، مرکز گفتگو ملی	مقررات برای کاهش هرزنامه(*SPAN*)، دستور العمل ملی(*NG*) برای محافظت از انسان در برابر میدان های الکترومغناطیسی رادیویی	دارالاسلام،المدینة، الریاضیة، *Jarir Bookstore*
حاکمیت امنیتی	شورای امنیت ملی(*SNSC*)، وزارت دفاع، فدراسیون امنیت سایبری(*SAFCSP*)، اداره امنیت سایبری(*NCA*)، وزارت ارتباطات و فناوری اطلاعات(*MCIT*)، مرکز امنیت اطلاعات(*NIC*)(*Almarhabi, 2016*)	قانون جرایم ضد سایبری، انتشار سند سیاست های امنیت اطلاعات و فرایند توسعه چارچوب برای سازماندهی دولتی، استراتژی امنیت اطلاعات ملی(*NISS*)	*Mic-Elm-AEC Al Tamimi & Company*
حاکمیت فنی و	کمیسیون ارتباطات و فناوری اطلاعات(*CITC*)، اداره کل	تصویب سند«شرایط و ضوابط خدمات	*Abulla Found Group-A., A. Turki Group-*

اقتصادی	سرمایه گذاری(*SAGIA*)، اداره بازار سرمایه(*CMA*)، اداره کل زکات و مالیت(*GAZT*)، اداره کل حمل و نقل هوایی، وزارت اقتصاد و برنامه ریزی، وزارت مالیه، وزارت کار و توسعه اجتماعی، وزارت انرژی صنعت و معدن	*MVNO* و ارائه خدمات *IoT-VNO*، خدمات مبتنی بر موقعیت مکانی الجوال، قانون مخابرات، قانون ماملات الکترونیک، سرویس اینترنتی مبتنی بر فیبر با سرعت بالا(*FTTH-100MB/s*)	*Danubeco-A Faris- Savola - Panda- Dallah Avcp-SACO-Naseej-Arabast-Mibily STC ZAin ITC-DUSSUR Maaden-Sami=Tsa jeddah--www.se.com.sa-Saudia.com-SAEI-Weqaya*
حاکمیت مدیریتی و حقوقی	مرکز گفتگو ملی شاه عبدالعزیز، کمیسیون ارتباطات و فناوری اطلاعات(*CITC*)،مجلس شورا(*Shura Council*)، قوه قضاییه، اداره تحقیقات عمومی(*Mabahith*)	تصویب شاخص های *ICT* برای بخض ارتباطات و فناوری اطلاعات، برنامه دولت التکترونیک(*Yesser*)، برنامه ملی تحول ۲۰۲۰	

جدول ۱ – حاکمیت عربستان در ابعاد گوناگون

ب. اسناد بالا دستی حاکمیتی در فضای مجازی

چهار سند از اسناد و قوانین سیاستی مهم حاکمیتی عربستان در حوزه فضای مجازی به شرح زیر است:

- سند استراتژی امنیت ملی اطلاعات[15] *NISS*، در سال ۲۰۱۱، وزارت ارتباطات و فناوری اطلاعات (*MCIT*) که یکی از آژانسهای دولتی مسئول سایبر است در پی امنیت و دیجیتالی

[15] National Information Security Strategy (NISS)

کردن خدمات دولتی در عربستان سعودی با همکاری کمیسیون *CITC* شروع به توسعه اولین استراتژی امنیت اطلاعات ملی (*NISS*) نمود و پیشنویسی از سندی در این ارتباط با همکاری یک گروه بین المللی، مشاوران ارشد و کارشناسان ملی تهیه نمود. در ویرایش هفتم این سند، هدف را این چنین بیان نموده است *1*) امکان استفاده و اشتراک گذاری آزادانه و ایمن اطلاعات را فراهم کنید. ۲) ضمن ترویج افزایش استفاده از فناوری اطلاعات ، امنیت ، ایمنی و یکپارچگی اطلاعات آنلاین را افزایش دهید. ۳) ایجاد انعطاف پذیری در سیستم های اطلاعاتی. *(Developing National Information Security Strategy for the Kingdom of Saudi Arabia, n.d.)*

- سند کنترل ضروری امنیت سایبری[۱۶] (*ECC*) : *NCA* با همکاری کمیسیون *CITC* این سند را به عنوان حداقل الزامات امنیت سایبری برای نهادهای ملی برای رعایت آن توسعه داده است .*ECC* بر مبنای بهترین شیوه‌ها بوده و با هدف کاهش خطر ناشی از تهدیدهای داخلی و خارجی سایبری متفاوت است. کنترلهای امنیت سایبری شامل پنج دامنه اصلی امنیت سایبری و ۲۹ زیر مجموعه سیستم امنیتی، ۱۱۴ کنترل امنیتی سایبری که الزامات این کنترلهای امنیتی سایبری به قوانین ملی و بین المللی مربوط است.(

- چارچوب امنیت سایبری سازمان پول *SAMA*[۱۷]، این چارچوب با همکاری *CITC*، برای مدیران ارشد و اجرایی، صاحبان کسب و کار، صاحبان دارایی‌های اطلاعاتی، *CISOs* و کسانی که مسئولیت تعریف، اجرا و بررسی کنترلهای امنیتی سایبری در سازمانهای عضو را دارند، در نظر گرفته شده است. این چارچوب در چهار حوزه اصلی تشکیل شده است: الف. رهبری و نظارت بر امنیت سایبری. ب.مدیریت ریسک امنیت سایبر و رعایت آن. ج. عملیات و تکنولوژی امنیت سایبر. د. سوم شخص امنیت سایبری.

- قانون مخابرات به موجب قطعنامه شماره ۷۴ شورای وزیران

---

[16] Essential Cybersecurity Controls
[17] Saudi Arabian Monetary Agency (SAMA)

- چارچوب تنظیم مقررات امنیت سایبری ***CRF***[۱۸] : این چهارچوب برای بخش ارتباطات و فناوری اطلاعات که هدف اصلی آن صنعت مخابرات است.(***Land-Pejoska & Rehman, n.d***).

ج. نظارت و فیلترینگ در فضای مجازی

عربستان سعودی تمام ترافیک اینترنت بین المللی را از طریق یک مزرعه پروکسی واقع در شهر علم و فناوری پادشاه عبدالعزیز هدایت میکند .یک فیلتر محتوا بر اساس نرم‌افزار محاسبه امن بر روی آن وجود دارد. از اکتبر سال ۲۰۰۶، کمیسیون ارتباطات و فناوری اطلاعات(***CITC***) به جای ***KACST***، ساختار ***DNS*** و فیلتر کردن را در عربستان سعودی بر عهده دارد.

پایه قانونی اولیه برای فیلترکردن محتوای قطعنامه شورای وزیران در تاریخ ۱۲ فوریه ۲۰۰۱ است .طبق گزارش وبسایت این کمیسیون، در سال ۲۰۱۷ حدود یک میلیون و دویست هزار وب‌سایت فیلتر شده است. دلیل فیلترینگ محتواهای غیراخلاقی) تبلیغ مخدر، قمار، پورنوگرافی و ...(، نفرت پراکنی و ترویج خشونت بوده است. علاوه بر سایتهای غیراخلاقی و سایت‌هایی که حق تألیف را رعایت نمی‌کنند، سایتهای منتسب به شیعیان، ایران، حزب الله و اخوان المسلمین فیلتر میشوند. همچنین، در دورههای مختلفی 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 توئیتر شهروندان را به تجمعات ضددولتی 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 وب سایتها را براساس مواد خاصی فیلتر کند.

بر اساس دستورالعملهای کمیته امنیتی تحت نظارت وزارت اطلاعات از جمله سایتهایی که انتقاد از دولت عربستان سعودی دارند نیز مسدود می‌شوند. دو لیست از سایت ها توسط واحد

[18] Cybersecurity Regulatory Framework (CRF)

خدمات اینترنت عربستان (*ISU*) مسدود می‌گردد یکی سایتهایی حاوی محتوای غیر اخلاق که اغلب به صورت پورنوگرافی و یا حمایت از حقوق *LGBT*، مخدر، قمار و.. هستند و دیگر سایتهایی که ایدئولوژی شیعه را تبلیغ می‌کند.

سیستم فیلترینگ عربستان از طریق یک فرم آنلاین که از طریق وب قابل دسترس است، شهروندان را تشویق می‌کند که وب سایت هایی که به صورت غیر قانونی از نظر حاکمیت عربستان فعالیت می‌کنند را معرفی نمایند تا پس از بررسی مسدود کردند. از این رو حاکمیت عربستان قوانین و مقرارت خود را در فضای مجازی در سال ۲۰۰۱ به تصویب رساند (*NCDC Signing Platform, n.d.*) تا تمامی‌نشریات اعم از روزنامه نگران و حتی وبلاگ نویسان مجوز از وزارت اطلاعات دریافت نمایند. این تصمیم حاکمیتی سازماندهی فضای مجازی و مدیریت نسبی را برای دولت میسر گرداند. در یازدهم ژانویه ۲۰۰۶ ترجمه گوگل را که باعث می‌شد سایت ها مسدود نشوند را مسدود نمود.

دولت عربستان سعودی برنامه‌های آنلاین مانند اسکایپ و واتساپ را به دلیل ترس از اینکه فعالان ضد حکومتی ممکن است از این سیستم عامل استفاده کنند در سال ۲۰۱۳ مسدود نمود 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. با این حال ،*CITC* تأیید کرد که تماسها هنوز هم در سطح جهانی و محلی تحت نظارت و سانسور قرار می‌گیرند. سیستمهای رسانههای اجتماعی مانند توییتر و فیسبوک به طور گستردهای در عربستان سعودی مورد استفاده قرار میگیرند، در حالیکه نزدیک به ۳۰ درصد کاربران منطقه عرب از عربستان سعودی هستند .توییتر تبدیل به یک پلتفرم مهم برای بیان مخالفت شده است. با این حال ،شهروندان لیبرال و اخیرا محافظه‌کاران دستگیر شده‌اند و گاهی مجازات‌هایی مانند زندان و جریمه برای انتقاد از دولت در رسانه‌های اجتماعی برای آنها وضع شده است.

کمیسیون فناوری ارتباطات و اطلاعات به عنوان در عرصه بین الملل نیز مشارکت هایی را با سازمان های مربوطه داشت است که از دست آوردهای آن می‌توان به مشارکت با انگلیس (*Al-Maliki, 2013*) مشارکت با چین برای ایجاد بزرگترین اقتصاد دیجیتال خاورمیانه و شمال آفریقا *MENA*. به ویژه در حوزه سلامت، شهرهای هوشمند، بخشهای تجارت الکترونیک، آموزش و پرورش و گردشگری دیجیتال، همچنین راه اندازی نسل پنجم نسل پنجم (*G۵*) شبکه مخابراتی به عنوان یکی از پیشتازان کشورهای جهان با ایجاد بازاری با ارزش بیش از ۱۲ میلیارد دلار تا سال ۲۰۳۰ ، با کشور مصر با عنوان اتحاد دیجیتالی از طریق مبادله دانش فنی، تخصص و تجارب و آموزش برای توسعه سرمایه انسانی در بهره‌وری فنی و دیجیتالی، از طریق برنامه های مشترک و آموزش کادرهای عربستان در زمینه مهارتهای فنی و برنامه نویسی، و همچنین تبادل کمک هزینه تحصیلی و تحصیلی برای دانش آموزان. دو طرف همچنین در مورد چگونگی تشویق کارآفرینان در هر دو کشور و خدمات مشاورهای برای ایجاد مشارکت های امیدوار کننده در صنایع دیجیتال اظهار داشتند.

گزارش اوپن‌نت اینیشیتیو در جدول دو به وضوح ابعاد مختلف فیلترینگ توسط این کشور را نشان می‌دهد. در پایان این گزارش که حاوی چهل منبع است چنین نوشته شده است که به طور کلی فیلتر کردن اینترنت در عربستان سعودی منعکس کننده اقدامات گسترده دولت برای سرکوب مخالفت ها و ترویج عقاید مذهبی واحد است.

وضعیت فیلتر / ابعاد	مدرکی بر فیلتر وجود ندارد	مشکوک به فیلترینگ	انتخابی	قابل ملاحظه	فراگیر
سیاسی				●	
اجتماعی					●
امنیتی			●		
ابزارهای اینترنتی					●

جدول دو: در یک نگاه نتایج تحقیق فیلترینگ اینترنت در کشور عربستان[19]

[19] (*Saudi Arabia | OpenNet Initiative*, n.d.)

محققان دانشگاه هاروارد از طریق سرورهای پراکسی در عربستان به اینترنت متصل شده و دسترسی به حدود شصت هزار صفحه وب را به عنوان ابزاری برای تعیین تجربی دامنه و فراگیری اینترنت مورد بررسی قرار داده اند، این صفحات حاوی اطلاعاتی در مورد دین ، بهداشت ، آموزش ، مرجع ، شوخ طبعی و سرگرمی بود. یافته ها نشان داد که ۲۰۳۸ صفحه مسدود شده است. حال آنکه بیشتر این مطالب از سایتهایی تشکیل شده است که در سایر نقاط جهان محبوب هستند. در گزارش به صراحت بیان می شود که «دولت سعودی علاقه مندی فعالانه در فیلتر کردن محتوای وب غیر صریح جنسی برای کاربران درون پادشاهی دارد.» (*Zittrain & Edelman, n.d*.) عربستان سعودی ، یمن و امارات متحده عربی همه از فیلترهای مذهبی که بر روی موضوعات اجتماعی و سیاسی متمرکز استفاده کرده اند تا جلوی محتوای مذهبی را بگیرند که البته با اعتقادات مذهبی تحریم شده توسط دولت چندان منطبق نیست.(*Rahimi & Gupta, 2020*) عربستان سعودی در میان رژیم های عربی که سانسور اینترنتی را اعمال می کنند، پیشتاز است (*Black & editor, 2009*).

نتیجه گیری

فضای مجازی به شدت مورد مناقشه قرار گرفته است. چالش نه تنها بازی سنتی سیاست قدرت بین دولت ها ، بلکه از دست دادن قدرت در داخل کشورها است. کشورها در تلاش برای ایجاد هنجارها و نهادهایی که آینده حکمرانی را شکل می‌دهند، با یکدیگر رقابت می‌کنند، اما در عین حال، آنها باید شکاف حاکمیت را پر کنند و با بخش خصوصی رقابت کنند. در نتیجه، حاکمیت فضای مجازی هنوز در دست ساخت است. ایجاد یک قرارداد اجتماعی برای فضای مجازی که شامل دولت ها، شرکت ها و بازیگران جامعه مدنی باشد ، برای آینده نزدیک غیرواقعی به نظر می‌رسد. نهادهای موجود و مجموعه حقوق بین الملل موجود ابزارهای مناسبی را برای تنظیم طیف وسیعی از فعالیت های دولت در فضای مجازی فراهم می‌کنند. فضای مجازی فاقد یک انجمن یا سازمان بین المللی است که وظیفه تنظیم فعالیت های خود را داشته باشد. بنابراین، حاکمیت در مجامع تنظیم استاندارد فنی، سازمانهای خصوصی، گروههای جامعه مدنی، کشورها

و سازمانهای بین المللی گسترش می‌یابد. حکومت داری از تدوین هنجارها و آیین نامه های رفتاری، تا امضای معاهدات منطقه ای و مقررات تحمیلی را در بر می‌گیرد. آینده حاکمیت فضای مجازی در تعادل بین رقابت قدرت بزرگ و عدم تقارن قدرت بین کشورها و درون آنها است. با این مقدمه می‌توان مهمترین شاخصه های حکمرانی فضای مجازی کشور عربستان را این چنین بر شمرد که این حاکمیت در فقدان نهادهای دموکراتیک است، فیلترینگ و مسدود کردن که همراه با تعقیب قضایی است این مسدود کردن سایت های شامل سایت های منتسب به شیعیان و ایران و حزب الله حتی اخوان المسلمین است همچنین دعوت کنندگان به اعتراضات به ویژه مناطق شیعه نشین البته مسدود نمودن سایت های غیر اخلاقی نیز در دستور کار ایشان است. همانطور که در مقدمه اشاره رفت عربستان همچون اکثر کشورها، موضع گیری خاصی در قبال ایالات متحده آمریکا در حوزه فضای مجازی بلکه با ایشان همراه است تا از طریق بتواند حضور در مجامع بین المللی داشته و تلاش نماید تا بر ارتقاء موقعیت کشورش در رتبه بندیهای جهان را رقم زند. با توجه به مولفه هایی که برای حکومت خوب بر شمرده شده و یافته های تحقیق به وضوح نمایان می شود که نظام حکومتی در عربستان سعودی این امکان را فراهم نمی کند تا موارد هشتگانه حکومت خود در این سرزمین جاری و ساری گردد. همچنان که جریان های معارض نیازمند شفافیت و جریان اطلاعات هستند تا بتوانند از طریق فضای مجازی و ابزارهای نوین، بیداری اسلامی را در این کشور رقم بزنند. این حوزه همچنان نیاز به تحقیقات بیشتری دارد و روش های متفاوت برای آن متصور است. برای نمونه بررسی سانسور و فیلترینگ در دو کشور کشور خاص مثل آمریکا و عربستان (*Malki, 2015*)

منابع و مآخذ

Alassim, M., Alfayad, M., & Abbott-Halpin, E. F. (2017). Understanding Factors Influencing E-Government Implementation in Saudi Arabia from an Organizational Perspective. *International Journal of Information and Communication Engineering*, *11*(7). http://eprints.leedsbeckett.ac.uk/id/eprint/4323/

AlBar, A. M., & Hoque, Md. R. (2019). Factors affecting the adoption of information and communication technology in small and medium enterprises: A perspective from rural Saudi Arabia. *Information Technology for Development*, *25*(4), 715–738. https://doi.org/10.1080/02681102.2017.1390437

Albugami, S., & Ahmed, V. (2015). Success Factors for ICT Implementation in Saudi Secondary Schools: From the Perspective of ICT Directors, Head Teachers, Teachers and Students. *International Journal of Education and Development Using Information and Communication Technology*, *11*(1), 36–54.

Al-Maliki, S. (2013). *Information and Communication Technology (ICT) Investment in the Kingdom of Saudi Arabia: Assessing Strengths and Weaknesses*.

Almarhabi, K. (2016). Adherence to ICT Security and Privacy Policies in Saudi Arabia. *International Journal of Computer Applications*, *147*(4), 13–18.

Alsowailm, F., Spidalieri, F., & Hathaway, M. (n.d.). *KINGDOM OF SAUDI ARABIA CYBER READINESS AT A GLANCE*. https://www.belfercenter.org/sites/default/files/files/publication/cri-2.0-ksa.pdf

Barlow, J. P. (2016, January 20). *A Declaration of the Independence of Cyberspace*. Electronic Frontier Foundation. https://www.eff.org/cyberspace-independence

Betz, D., & Stevens, T. (2011). *Cyberspace and the state*.

Black, I., & editor, M. E. (2009, June 30). Saudia Arabia leads Arab regimes in internet censorship. *The Guardian*. https://www.theguardian.com/world/2009/jun/30/internet-censorship-arab-regimes

Boothby, W. H. (2014). *Conflict law: The influence of new weapons technology, human rights and emerging actors*. Springer.

Chertoff, M., Simon, T., & Innovation, C. for I. G. (2015). *The Impact of the Dark Web on Internet Governance and Cyber Security*. Centre for International Governance Innovation.

Choucri, N. (2012). *Cyberpolitics in international relations*. MIT Press.

Connell, N. (n.d.). *Saudi Arabia's draft Cloud Cybersecurity Controls—Al Tamimi & Company—Lexology*. Retrieved January 15, 2021, from https://www.lexology.com/library/detail.aspx?g=7e35491b-6ab0-40c6-8d10-26351fb2bc37

Cornish, P. (2015). Governing Cyberspace through Constructive Ambiguity. *Survival*, *57*. https://doi.org/10.1080/00396338.2015.1046230

Cukier, K. N., & Mayer-Schönberger, V. (2013). *The rise of big data*. *92*.

Deibert, Ron. (2015). The Geopolitics of Cyberspace After Snowden. *Current History (New York, N.Y.: 1941)*, *114*, 9–15. https://doi.org/10.1525/curh.2015.114.768.9

Deibert, Ronald, & Crete-Nishihata, M. (2012). Global Governance and the Spread of Cyberspace Controls. *Global Governance: A Review of Multilateralism and International Organizations*, *18*, 339–361. https://doi.org/10.1163/19426720-01803006

Demchak, C. C., & Dombrowski, P. J. (2014). Rise of a Cybered Westphalian Age: The Coming Decades. In M. Mayer, M. Carpes, & R. Knoblich (Eds.), *The Global Politics of Science and Technology—Vol. 1: Concepts from International Relations and Other Disciplines* (pp. 91–113). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-55007-2_5

Demidov, O. (2014). ICT in the Brics Agenda Before The 2015 Summit: Installing the Missing Pillar? *Security Index: A Russian Journal on International Security*, *20*, 127–132. https://doi.org/10.1080/19934270.2014.965968

DeNardis, L. (2014). The global war for internet governance. *Proceedings of the 2014 ACM Conference on Web Science - WebSci '14*, 3–3. https://doi.org/10.1145/2615569.2618146

Developing National Information Security Strategy for the Kingdom of Saudi Arabia. (n.d.). https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/SaudiArabia_NISS_Draft_7_EN.pdf

Dilipraj, E. (2014). *NTERNET GOVERNANCE : THE SHIFT FROMMONOPOLY TO MULTI-PARTY*. Centre for Air Power Studies. http://capsindia.org/files/documents/CAPS_IB_15-MAY-2014.pdf

Dunn Cavelty, M. (2014). Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. Science and Engineering Ethics, 20(3), 701–715. https://doi.org/10.1007/s11948-014-9551-y

Ebert, H., & Maurer, T. (2013). Contested Cyberspace and Rising Powers. *Third World Quarterly*, *34*(6), 1054–1074. https://doi.org/10.1080/01436597.2013.802502

Emerson, R. G. (2016). Limits to a cyber-threat. *Contemporary Politics*, *22*(2), 178–196. https://doi.org/10.1080/13569775.2016.1153284

Finkelstein, L. (1995). What Is Global Governance? *GLOBAL GOVERNANCE*,*1*,367–37 https://doi.org/10.1163/19426720-001-03-90000007

ITU: Committed to connecting the world. (n.d.). Retrieved January 5, 2021, from https://www.itu.int/en/Pages/default.aspx

Jayawardane, S., Larik, E., & Jackson, E. (2015). Cyber Governance: Challenges, Solutions, and Lessons for Effective Global Governance. *The Hague Institute for Global Justice Policy Brief*.

Kremer, J.-F., & Müller, B. (Eds.). (2014). *Cyberspace and International Relations: Theory, Prospects and Challenges*. Springer-Verlag. https://doi.org/10.1007/978-3-642-37481-4

Land-Pejoska, A., & Rehman, Z. U. (n.d.). *Cyberabia*. Retrieved January 15, 2021, from https://www.tamimi.com/law-update-articles/cyberabia-developments-in-the-cybersecurity-regulatory-landscape-in-saudi-arabia/

Lewis, J. (2010). *Cybersecurity: Next steps to protect critical infrastructure, testimony to the US Senate Committee on commerce, science and transportation*. https://www.govinfo.gov/content/pkg/CHRG-111shrg57888/html/CHRG-111shrg57888.htm

Liaropoulos, A. (2015). A Human-Centric Approach to Cybersecurity: Securing the Human in the Era of Cyberphobia, Journal of Information Warfare, 14, 4 (2015). *Journal of Information Warfare*, *14*.

Liaropoulos, A. N. (2016). Reconceptualising Cyber Security: Safeguarding Human Rights in the Era of Cyber Surveillance. *International Journal of Cyber Warfare and Terrorism*, *6*(2), 32–40. https://doi.org/10.4018/IJCWT.2016040103

Malki, Z. (2015). Analyzing the Internet Filtering Policies in KSA and USA. *International Journal of Science, Technology and Society*, *3*(3), 83. https://doi.org/10.11648/j.ijsts.20150303.13

Middle East Internet Stats and Telecommunications Reports. (n.d.). Retrieved December 30, 2020, from https://www.internetworldstats.com/middle.htm

Mihr, A. (2014). Good Cyber Governance: The Human Rights and Multi-Stakeholder Approach. *Georgetown Journal of International Affairs*, 24–34.

Ministry of Communications and Information Technology. (n.d.). https://www.mcit.gov.sa/

National Cybersecurity Authority. (2020, October 31). National Cybersecurity Authority (Saudi Arabia). https://nca.gov.sa/

NCDC Signing Platform. (n.d.). Retrieved January 5, 2021, from https://www.ncdc.gov.sa/

Nocetti, J. (2015). Contest and conquest: Russia and global internet governance. *International Affairs*, *91*(1), 111–130. https://doi.org/10.1111/1468-2346.12189

Nye, J. S., & Donahue, J. D. (Eds.). (2000). *Governance in a globalizing world*. Visions of Governance for the 21st Century ; Brookings Institution Press.

Paterson, M., Rosenau, J., & Czempiel, E.-O. (1992). Governance without Government: Order and Change in World Politics. *International Affairs (Royal Institute of International Affairs 1944-)*, *68*, 733. https://doi.org/10.2307/2622748

Patrick, S. (2014). The Unruled World The Case for Good Enough Global Governance. *Foreign Affairs (Council on Foreign Relations)*, *93*, 58-+.

Pohle, J. (n.d.). *Multistakeholderism unmasked: How the netmundial initiative shifts battle-grounds in internet governance. Global Policy*. Retrieved January 5, 2015, from Multistakeholderism unmasked: How the NetMundial Initiative shifts battlegrounds in internet governance

Rahimi, N., & Gupta, B. (2020). A Study of the Landscape of Internet Censorship and Anti-Censorship in Middle East. *EPiC Series*, *69*, 60–68. https://easychair.org/publications/open/6hvn

Rosenau, J. (1995). Governance in the Twenty-first Century. *Global Governance*, *1*, 13–43. https://doi.org/10.1163/19426720-001-01-90000004

Saudi Arabia | OpenNet Initiative. (n.d.). Retrieved December 30, 2020, from https://opennet.net/research/profiles/saudi-arabia

Slack, C. (2016). Wired yet Disconnected: The Governance of International Cyber Relations. *Global Policy*, *7*(1), 69–78. https://doi.org/10.1111/1758-5899.12268

Vision2030. (n.d.). The Owner of This Website (Www.Vision2030.Gov.Sa) Has Banned the Country or Region Your IP Address Is in (IR) from Accessing This Website. Retrieved December 30, 2020, from http://www.vision2030.gov.sa/

Weber, R. H. (2013). Internet of things – Governance quo vadis? *Computer Law & Security Review*, *29*(4), 341–347. https://doi.org/10.1016/j.clsr.2013.05.010

Weitzenboeck, E. M. (2014). Hybrid net: The regulatory framework of ICANN and the DNS. *International Journal of Law and Information Technology*, *22*(1), 49–73. https://doi.org/10.1093/ijlit/eat016

West, S. (2014). Globalizing Internet Governance: Negotiating Cyberspace Agreements in the Post-Snowden Era. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2418762

Zittrain, J., & Edelman, B. (n.d.). *Documentation of Internet Filtering in Saudi Arabia*. Retrieved January 15, 2021, from https://cyber.harvard.edu/filtering/saudiarabia/