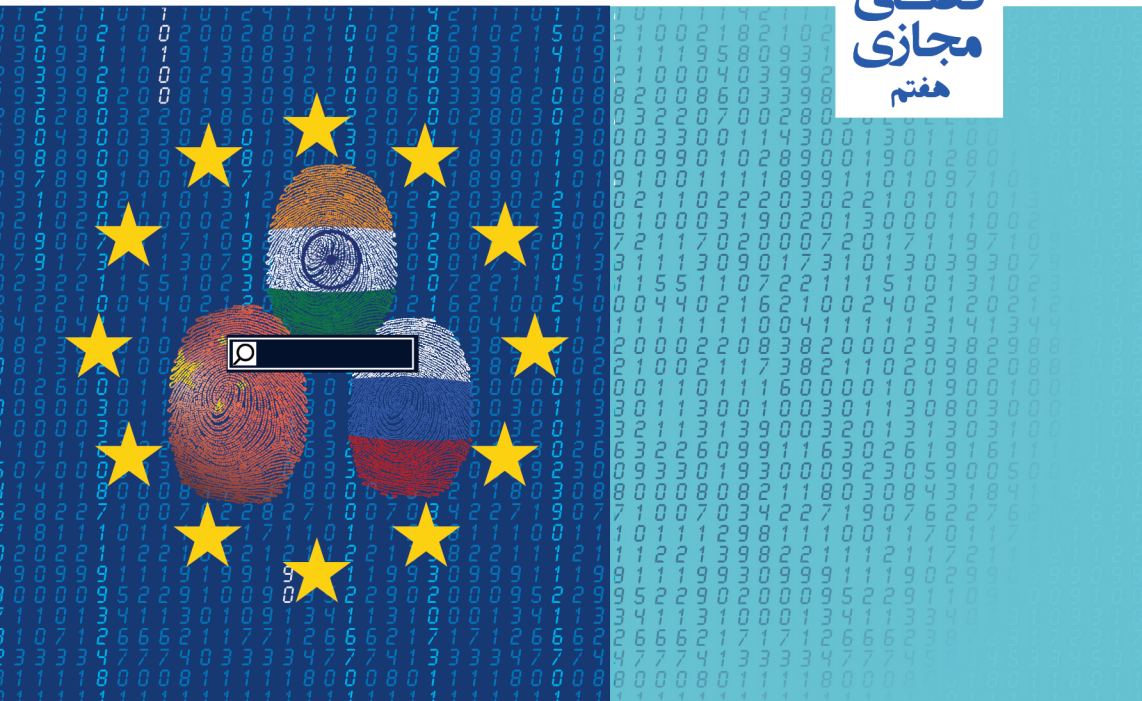




مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

عصر فضای مجازی هفتم



محله سازی داده ها

Data localization



محلی سازی داده‌ها

گزارش شماره ۷

تیرماه ۱۳۹۸

تهیه شده در: پژوهشگاه مرکز ملی فضای مجازی - گروه علوم و فناوری‌های پیشرفته فضای مجازی
تهیه کننده: حسین حسینی (عضو هیات علمی پژوهشگاه فرهنگ، هنر و ارتباطات)

ناظر علمی: محمدمهدی نصرهرندی

سر شناسه	:	حسینی، حسین، - ۱۳۶۰
عنوان و نام پدیدآور	:	محلی سازی داده ها/ تهیه کننده حسین حسینی ؛ ناظر علمی محمدمهدی نصرهرندی؛ تهیه شده در پژوهشگاه مرکز ملی فضای مجازی - گروه علوم و فناوری‌های پیشرفته فضای مجازی.
مشخصات نشر	:	تهران: پژوهشگاه فضای مجازی، ۱۴۰۰
مشخصات ظاهری	:	۲۲ص.؛ ۱۴/۵×۲۱/۵ س م
شابک	:	۹۷۸-۶۲۲-۹۷۲۳۰-۸-۱
وضعیت فهرست نویسی	:	فیفا
یادداشت	:	بالای عنوان: عصر فضای مجازی.
موضوع	:	مراکز داده پردازشی -- تدابیر ایمنی Electronic data processing departments -- Security measures حفاظت داده ها -- سیاست دولت Data protection -- Government policy حفاظت داده ها Data protection رایانش ابری Cloud computing رایانش ابری -- قوانین و مقررات -- ایران Cloud computing -- Law and legislation -- Iran حفاظت داده ها -- قوانین و مقررات -- ایران Data protection -- Law and legislation -- Iran
شناسه افزوده	:	نصر هرندی، محمدمهدی، ۱۳۶۱
رده بندی کنگره	:	QA۷۶/۹
رده بندی دیویی	:	۰۰۵/۸
شماره کتابشناسی ملی	:	۸۴۰۴۳۶۲
اطلاعات رکورد کتابشناسی	:	فیفا

نشانی: تهران، میدان آرژانتین، خیابان بیهقی، نش خیابان ۱۶ غربی، پلاک ۲۰، کدپستی ۱۵۱۵۶۷۴۳۱۱

شماره تماس: ۸۶۱۲۱۰۶۱ <http://www.majazi.ir>

حقوق مادی و معنوی این اثر متعلق به مرکز ملی فضای مجازی است و استفاده از مطالب آن صرفاً با ذکر مأخذ
بلامانع است.

محتوای انتشار یافته در این گزارش الزاماً بیانگر دیدگاه مرکز ملی فضای مجازی نیست

سخن نخست

فضای مجازی با شتاب شگرف و روبه‌ترایدی که در حال بطن و گسترش است تمام ساحات اجتماعی، اقتصادی، سیاسی و فرهنگی زندگی بشر را در نور دیده و هر روز بخش بزرگی از زندگی واقعی را در خود فرو برده و حیات متفاوت و جدیدی به آن می‌دهد. لذا به نظرمی رسد دو نگاه کلان به فضای مجازی وجود دارد: نگاه اول که بالانص در ابتدای رشد و تکوین فضای مجازی مسلط شده بود، آن را همچون ابزاری کنار سایر ابزارهای بشری تصویر می‌کرد که تنها طریقت داشت. اما نگاه دوم، در نتیجه رشد تحولات خیره‌کننده فضای مجازی و سایه‌گستری آن در حوزه‌ها و شئون بشر در یک دهه اخیر آن را چون سکویی می‌داند که بسیار فراتر از شأن ابزاری حیات انسان‌ها را سامان جدیدی داده و ادعای تمدن‌نویسی را دارد. رویکردی که از قضا از چشمان بصیر رهبر انقلاب نیز دور نمانده و انتظاری تمدنی از فضای مجازی در ایران را مطالبه داشته‌اند.

در همین راستا گزارش‌های عصر فضای مجازی تلاش می‌کند تا فهم سازمان‌ها و دستگاه‌های مرتبط با حوزه‌ی فضای مجازی را ارتقاء بخشد و آن‌ها را برای مواجهه فعال و خردمندانه با تحولات این عرصه مهیا سازد.

سید ابوالحسن فیروزآبادی
دبیر شورای عالی و رئیس مرکز ملی فضای مجازی

چکیده

هدف این گزارش معرفی مفهوم محلی‌سازی داده‌ها است. محلی‌سازی داده که به طور مختصر به معنای ذخیره داده‌های تولید شده در داخل هر کشور بر روی سرورهای همان کشور است، ملی‌گرایی داده نیز نامیده می‌شود. در این گزارش ضمن مرور تعاریف مختلف محلی‌سازی داده‌ها، فرصت‌های و چالش‌هایی که اتخاذ این رویکرد برای هر کشور دارد تحلیل می‌شود. در پایان نیز گزارشی از سیاست‌های محلی‌سازی داده در کشورهای چین، روسیه، هند و همچنین اتحادیه اروپا ارائه می‌شود.

واژگان کلیدی

فضای سایبر، حکمرانی، محلی‌سازی داده، مقررات حفاظت از داده‌ها (اتحادیه اروپا)، روسیه، چین، هند

فهرست مطالب

۱- مقدمه	۱
۲- محلی سازی داده‌ها در جهان امروز	۱
۳- دلایل محلی سازی داده‌ها	۳
۴- تعریف محلی سازی داده‌ها	۴
۵- نویدها و چالش‌های محلی سازی داده‌ها	۵
۶- محلی سازی داده در هند	۸
۷- محلی سازی داده‌ها در روسیه	۱۳
۸- اتحادیه اروپا (مقررات عمومی حفاظت از داده‌ها)	۱۵
۹- محلی سازی داده در چین	۱۵
۱۰- نتیجه‌گیری	۱۶
۱۱- منابع	۱۷

۱- مقدمه

یکی از ابعاد مهم حکمرانی فضای سایبر نحوه مواجهه با داده‌ها است. امروزه داده‌ها که محصول انواع تعاملات آنلاین هستند ارزشمندترین محصول و مبنای سرمایه‌داری آینده به شمار می‌روند. با توجه به اهمیت تولید، انتشار و پردازش داده‌ها در آینده اجتماعی و اقتصادی کشورهای مختلف و روابط بین‌الملل، ضرورت دارد که نوع سیاستگذاری در مواجهه با انبوه داده‌های کلانی که هر روزه و هر لحظه در حال تولید و انتشار هستند مبتنی بر صیانت از منافع ملی باشد. پس از افشاگری‌های ادوارد اسنودن در سال ۲۰۱۳ مبنی بر همکاری پنهانی پلتفرم‌های بزرگ آنلاین با نهادهای امنیتی آمریکا، بسیاری از کشورها از جمله کشورهایی که به ادعای دولتهای غربی کمتر دموکراتیک هستند همانند چین و روسیه گرفته تا کشورهای غربی همانند آلمان و استرالیا و نیز هند و نیجریه سیاست‌هایی را برای ذخیره‌سازی داده‌های شخصی و حساس در داخل مرزهای ملی کشورهای خود در پیش گرفتند که اصطلاحاً محلی‌سازی داده‌ها^۱ نامیده می‌شود و به آن ملی‌گرایی داده^۲ نیز گفته می‌شود.

در این گزارش تلاش می‌شود ضمن مفهوم‌سازی محلی‌سازی داده‌ها، ابعاد مختلف و مزیتها و معایب آن مورد توجه قرار گیرد. بخش دوم این گزارش بررسی وضعیت و قوانین محلی‌سازی داده‌ها در برخی از مناطق و کشورهای جهان شامل هند، روسیه، چین و اتحادیه اروپا است.

۲- محلی‌سازی داده‌ها در جهان امروز

برخلاف تصور اولیه مبنی بر این که به اصطلاح کشورهای غیردموکراتیک در پی محصورسازی داده‌های تولیدی درون کشور خود هستند، بسیاری از کشورهای گوناگون، چه دموکراتیک و چه غیردموکراتیک-به تعبیر غربی‌ها- در پی وضع قوانینی برای محلی‌سازی داده‌ها هستند. برای مثال، دولت نیجریه به عنوان یک کشور آفریقایی همه مشترکان و مشتریان داده‌های شرکتهای فناوری اطلاعات و نیز شرکتهای تولیدکننده داده‌های دولتی را از تاریخ دسامبر ۲۰۱۳ ملزم کرده است تا داده‌ها را داخل این کشور ذخیره‌سازی کنند. کشور اروپایی آلمان، شرکتهای مخابراتی و ارائه‌کنندگان خدمات اینترنتی (آی.اس.پی.ها) را ملزم کرده است تا داده‌ها را درون قلمرو این کشور ذخیره نمایند. بر اساس قانون شماره ۲۴۲-اف.زد فدراسیون روسیه (در ادامه گزارش تحلیل خواهد شد)، که از سپتامبر ۲۰۱۶ اجرایی شده است، همه پایگاه‌های داده‌ای که داده‌های شخصی شهروندان این کشور را نگهداری می‌کنند باید داخل قلمرو

^۱ .Data Localization

^۲ .data nationalism

روسیه قرار گرفته باشند. کشورهای دیگر نظیر استرالیا و به خصوص هند نیز قوانینی دارند که انتقال داده‌ها در حوزه‌های خاص همانند سلامت و دولت را محدود و مشروط می‌کنند (وی، ۲۰۱۸).

یکی از ویژگی‌های فضای سایبر در عصر حاضر این است که شرکت‌های اطلاعاتی واسطه^۱ عمده و یا پلتفرم‌های بزرگ همانند گوگل که کاربران در سطح جهان به آنها اعتماد می‌کنند و داده‌های اطلاعات خصوصی خود را در اختیارشان قرار می‌دهند در آمریکا واقع شده‌اند. در بیشتر موارد، این شرکت‌ها در راستای سیاست‌های نهادهای اطلاعاتی مختلف دولت آمریکا و نیز در جهت اجرای قانون دست به افشای اطلاعات کاربران می‌زنند. تحت فشارهای مختلف هم امکان دارد که این شرکت‌ها از استانداردهای رمزگذاری عدول کنند و امکان دسترسی مخفیانه به داده‌ها را فراهم نمایند؛ این موضوع سبب می‌شود که حریم خصوصی کاربران جهانی آنها در معرض نظارت ناخواسته قرار گیرد. برای مثال در سال ۲۰۱۳ ادوارد اسنودن مشاور آژانس امنیت ملی آمریکا (ان.اس.ای)^۲ دست به افشاگری درباره برخی برنامه‌های نظارتی زد که این نهاد با همکاری واسطه‌های اطلاعاتی یا پلتفرم‌های بزرگ همانند مایکروسافت، گوگل و اپل انجام داده بود. اجرای این برنامه‌ها سبب شده بود تا امکان دسترسی مستقیم نهادهای امنیتی و اطلاعاتی ایالات متحده به داده‌های ارتباطی کلیه کاربران، سیاستمداران و شرکت‌های مختلف در سرتاسر جهان فراهم شود. در واقع دولت آمریکا تلاش می‌کند به کمک این زیرساخت‌های ارتباطی واسطه یا پلتفرم‌های بزرگ منافع سیاسی خود را به پیش ببرد (سارگسیان، ۲۰۱۶).

بنابراین، به دلیل تمرکز پلتفرم‌های بزرگ در داخل مرزهای ایالات متحده موقعیت و فرصت مناسبی برای اهداف مختلف دولت آمریکا از منظر ذخیره‌سازی و تحلیل داده‌ها در جهت کاربردهای گوناگون از جمله نظارتی و تجاری پدید آمده است.

افشاگری‌های اسنودن و پوشش رسانه‌های وسیع متعاقب آن سبب شد تا بسیاری از دولت‌ها با ارائه برنامه‌های ابتکاری محلی‌سازی داده‌ها برنامه‌هایی را در جهت توسعه زیرساخت‌های داخلی در جهت منافع سیاسی خود در پیش بگیرند (سارگسیان، ۲۰۱۶).

اما می‌توان مدعی شد که حرکت در جهت محلی‌سازی داده‌ها به سال‌ها پیش از افشاگری‌های اسنودن برمی‌گردد. برای مثال، در ابتدای سال ۲۰۰۵ دولت قزاقستان قانونی را تصویب کرد که طبق آن همه داده‌هایی که در دامنه "دات.کاز" تولید می‌شوند باید در داخل این کشور ذخیره شوند؛ گرچه بعدها برای برخی شرکت‌های اطلاعاتی همانند گوگل استثنائاتی قائل شدند (میشرا، ۲۰۱۶).

الزام برای محلی‌سازی داده‌ها یا محدودیت بر سر جریان آزاد اطلاعات در سال‌های اخیر در کشورهای نظیر ویتنام، اندونزی، برونئی، ایران، چین، برزیل، هند، استرالیا، کره، نیجریه و اخیراً روسیه صورت گرفته است. گرچه انواع آن مختلف است؛ برای مثال، برخی از کشورها نوعی ممنوعیت کلی را برای انتقال همه

^۱ .intermediary

^۲ .National Security Agency

^۳ . .kz

مقوله‌های داده‌های شخصی به خارج از کشور خود اعمال می‌کنند اما کشورهای دیگر نظیر کره جنوبی و استرالیا در مواردی خاص همانند سلامت و امور مالی محدودیت‌هایی را برای حفاظت از داده‌های حساس شهروندان خود تعیین کرده‌اند (میشرا، ۲۰۱۶).

۳- دلایل محلی‌سازی داده‌ها

دولتها به دلایل گوناگونی مانع از جریان آزاد داده‌ها فراتر از مرزهای ملی یا یک منطقه خاص می‌شوند که از جمله این دلایل می‌توان به تأثیر این موضوع بر عملکرد دولت و یا حفاظت و مسائل امنیتی اشاره کرد (وب سایت تکنوپدیدا، تاریخ مراجعه ۲۲ خرداد ۱۳۹۸) - که در ادامه گزارش به آن توجه خواهد شد. دولتها به دلایل مختلفی اقدام به محلی‌سازی داده‌ها می‌کنند که از جمله آنها می‌توان به حفاظت از حق حاکمیت بر داده تا توسعه رشد اقتصاد دیجیتال داخلی اشاره کرد. همه دولتهای جهان به اهمیت زیرساختهای واسطه یا میانجی اطلاعات برای امنیت ملی، ایمنی عمومی و منافع سیاسی دیگر پی‌برده‌اند. نهادهای دولتی و اطلاعاتی با چالشهای مختلفی از قبیل حملات سایبری، فریبکاری و در برخی جوامع با جنبش‌های اجتماعی و اپوزسیون سیاسی روبرو هستند. برای مقابله با این تهدیدات، نهادهای دولتی اغلب نیازمند دسترسی به داده‌های اطلاعاتی هستند که در اغلب موارد تولید و انتشار آنها به واسطه برخی پلتفرم‌های میانجی صورت می‌گیرد که دولت‌های ملی کنترلی بر عملکرد آنها ندارند؛ زیرا سیاستگذاری و زیرساختهای فنی این میانجی‌ها ورای مرزهای جغرافیایی کشورهای قرار دارد. این موضوع قدرت دولتها را به چالش کشیده است و به همین دلیل دولتها نمی‌توانند بدون تکیه بر زیرساخت شرکتی واسطه به سادگی به اعمال قانون بپردازند، یا این که داده‌ها و جریان اطلاعات را دستکاری کنند و حریم خصوصی و امنیت تمام کاربران و شهروندان را تضمین کنند (سارگسیان، ۲۰۱۶).

به عبارت دیگر، با وجود این که کاربران از سرتاسر جهان اطلاعات خود را در اختیار واسطه‌هایی همانند گوگل، آمازون، یاهو و مایکروسافت قرار می‌دهند، اما داده‌های آنها در مراکز داده جغرافیایی محدودی نگهداری می‌شود که تنها برخی از کشورها امکان طرح ادعای صلاحیت قضایی در مورد داده‌ها و دسترسی به آنها به منظور اعمال قوانین نظارتی مختلف را دارند (سارگسیان، ۲۰۱۶).

برخی کشورها سیاستهای محلی‌سازی داده‌ها را برای مقابله با تهدید علیه حریم خصوصی شهروندان و مخاطرات امنیتی که از جانب سازمان‌های اطلاعاتی کشورهای دیگر وجود دارد در پیش گرفته‌اند. برخی از کشورهای دیگر نیز نگرانی‌های عمومی ناشی از جاسوسی آژانس امنیت ملی آمریکا - پس از افشاگری‌های اسنودن - را به عنوان دستاویزی برای گسترش کنترل خود بر داده‌ها و نظارت بر آنها توسط رویکرد محلی‌سازی داده‌ها مورد استفاده قرار داده‌اند.

عمده‌ترین هدف محلی‌سازی داده‌ها حفاظت از حقوق اساسی افراد در فضای آنلاین در مواجهه با نظارت خارجی و تخطی گسترده از حریم خصوصی و نیز ارائه یک مزیتی رقابتی برای شرکتهای محلی در مواجهه با جهانی شدن اقتصاد دیجیتال است (فریزر، ۲۰۱۶).

۴- تعریف محلی‌سازی داده‌ها

محلی‌سازی داده‌ها گرچه از منظر حفاظت از حریم خصوصی، امنیت کشورها و نیز مباحث تجاری اهمیت فوق‌العاده‌ای برای کشورهای مختلف دارد اما تعریف آن ساده است. محلی‌سازی داده‌ها به معنای فرایند ذخیره داده‌ها درون مرزهای یک کشور خاص و در واقع در محل تولید داده‌ها است که به آن ملی‌گرایی داده نیز گفته می‌شود و شامل تنظیم برخی مقررات ویژه برای کنترل مستقیم دولت بر داده‌های تولید شده توسط شهروندان واقع در یک محدوده جغرافیایی است.

محلی‌سازی داده‌ها عموماً شامل الزاماتی است که طبق آن داده‌ها باید در درون حوزه قضایی هر کشور ذخیره شود و/یا این که به خارج از مرزها انتقال نیابند. در عمل برنامه‌های محلی‌سازی داده‌ها شرکتها را وادار می‌کند تا با تغییر مکان یا ساختن مراکز داده جدید در مکانهای مشخص، زیرساخت‌های خود را تغییر دهند (سارگسیان، ۲۰۱۶).

اصطلاح محلی‌سازی به طور کلی به معنای الزام برای ذخیره‌سازی فیزیکی داده‌ها درون مرزهای یک کشور تعریف شده است اما گاهی در معنای وسیعتر برای تعریف هر نوع محدودیت نسبت به عبور جریان داده‌ها از مرزها نیز به کار می‌رود (بیلی و پارشیرا، ۲۰۱۸).

به گفته چندلر و لی (۲۰۱۵) محلی‌سازی به معنای همه اقداماتی است که «مانع از انتقال داده» از مرزهای ملی می‌شود و می‌تواند به شکلهای مختلفی باشد؛ همانند جلوگیری از ارسال اطلاعات به خارج از کشور، الزام به کسب رضایت مشتری قبل از انتقال، ذخیره یک نسخه محلی از داده و اعمال مالیات نسبت به صادرات داده.

به گفته (کیم، ۲۰۱۶) برخی کشورها قوانینی را وضع کرده‌اند که داده‌های شهروندان یا داده‌ها درباره شهروندانشان باید درون مرزهای ملی آن کشورها باقی بماند که به آن محلی‌سازی داده‌ها یا ملی‌گرایی داده گفته می‌شود.

محلی‌سازی باید در یک زمینه کلی‌تر رو به رشد اقتصادی، راهبردی و سیاسی، اقتصاد دیجیتال و تقاضا برای کنترل دولتی و حق حاکمیت مورد توجه قرار گیرد. در حوزه‌هایی همانند امنیت سایبری، حفاظت از داده‌ها، نظارت، مالیات‌بندی دیجیتال و تنظیم مقررات برای پلتفرمها، محلی‌سازی اغلب به منزله ابزاری برای تأکید و تصریح کنترل در این نواحی دیگر قلمداد شده است (چندر و لی، ۲۰۱۵).

فراکین (۲۰۱۷) انتقال داده ورای مرزها را به دو دسته اساسی سختگیرانه و مشروط^۱ تقسیم کرده است. انتقال داده به شکل سختگیرانه به معنای الزام به ذخیره‌سازی یا پردازش داده‌ها در یک محل جغرافیایی خاص، و در موارد شدیدتر شامل ممنوعیت کامل انتقال داده به خارج از کشور است. در دسته دوم، انتقال داده مشروط به برآورده کردن برخی شرایط معین است که این شرایط ممکن است به افراد انتقال دهنده داده و یا کشوری که داده‌ها را دریافت می‌کند اعمال شود. برای مثال، مقررات عمومی حفاظت از داده اروپا تعیین کرده است که کشور ثالث باید از «سطح قابل قبول حفاظت» برخوردار باشد.

به گفته بیلی و پارشیلا (۲۰۱۸) محلی‌سازی یا محلی‌سازی داده به معنای الزام اجباری ذخیره‌سازی داده‌ها به شکل محلی است که می‌تواند به شکل هنجارهای نگهداری اجباری باشد و طبق آن داده‌ها باید فقط در سرورهای داخلی نگهداری شوند و یا این که در نسخه کمتر سختگیرانه آن به شکل نظارت بر داده^۲ است. طبق این نگرش، دست‌کم یک نسخه از داده‌ها باید به شکل محلی ذخیره و نگهداری شوند. بیلی و پارشیلا (۲۰۱۸) بحث‌های کنونی درباره محلی‌سازی داده را به سه دسته اصلی تقسیم کرده‌اند. رویکرد نخست آزادی‌های مدنی^۳ نام دارد و به تأثیر محلی‌سازی داده‌ها برای پیامدهای بهتر برای افراد از منظر ایمنی داده‌های شخصی آنها، حفاظت در برابر نظارت داخلی یا خارجی و اعمال حق آزادی بیان مربوط می‌شود. رویکرد دوم کارکردهای دولت^۴ است؛ که ناشی از چالش‌های پیش روی مقامات دولت برای دسترسی به داده‌ها برای انجام کارکردهای اعمال قانون و تنظیم مقررات نشأت می‌گیرد و شامل مواردی همچون حفاظت از منافع امنیت ملی است. رویکرد سوم توسعه اقتصادی^۵ است که طی آن از محلی‌سازی به منزله اهرمی برای توسعه اقتصاد ملی و به‌ویژه پیشرفت زیرساخت‌های فناوری اطلاعات استفاده می‌شود.

۵- نویدها و چالش‌های محلی‌سازی داده‌ها

محلی‌سازی داده‌ها دارای ابعاد مثبت و ابعاد منفی است و طیفی از تأثیرات مختلف از آزادی‌های فردی گرفته تا فعالیت‌های تجاری بین‌الملل را دربرمی‌گیرد. محلی‌سازی داده‌ها هم برای شهروندان و شرکتها و هم برای دولتها پیامدهای مثبت و منفی مختلفی در پی دارد. قطعاً پلتفرم‌های آنلاین بزرگ به دلیل این که محدودیت‌هایی بر سر راه تولید محتوا و داده در آنها توسط دولتهای مختلف ایجاد می‌شود، مخالف محلی‌سازی داده‌ها هستند. از طرف دیگر، شرکتهای فناوری و پایگاه داده محلی ممکن است از سیاست ذخیره‌سازی داده‌ها در بسترهای داخلی بهره‌مند شده و در ابعاد گوناگون پیشرفت کنند.

^۱. strict and conditional

^۲. data monitoring

^۳. civil liberties

^۴. government functions

^۵. economic development

گسترش تولید داده‌ها توسعه اقتصاد دیجیتال و نوآوری‌های فنی انقلابی را امکان‌پذیر کرده است. ماهیت بدون مرز اینترنت سبب توسعه حقوق افراد می‌شود، به این دلیل که به آنها امکان می‌دهد تا بدون محدودیت‌های جغرافیایی به مبادله اطلاعات، ایده‌ها، گفتار سیاسی و سایر شکل‌های بیان نظرات اقدام کنند (فریزر، ۲۰۱۶).

از طرف دیگر، سیاست‌هایی که مانع از جریان آزاد داده‌ها در میان مرزها می‌شود یکی از حساس‌ترین موانع تجارت در قرن بیست و یکم است. برخی کارشناسان این محدودیت‌ها را جزو سیاست‌های غیرقابل تحمل بر سر راه جریان آزاد داده‌ها و تراکنش‌های جهانی می‌دانند. به علاوه منتقدان محلی‌سازی داده‌ها نسبت به این که آیا این عمل می‌تواند موجب ایجاد ارزش افزوده برای اقتصاد داخلی شود هشدار داده‌اند (میشرا، ۲۰۱۶).

سیاست‌های محلی‌سازی داده‌ها هم در کشورهای دموکراتیک و لیبرال همانند استرالیا، کانادا و هند و هم در کشورهای دیگر همانند چین، ویتنام، ایران و روسیه دنبال شده است. منتقدان اعتقاد دارند که محلی‌سازی داده‌ها ابزاری برای سرکوب هر نوع ناراضی‌های سیاسی از طریق پلتفرم‌های آنلاین و جلوگیری از جریان آزاد اطلاعات است (میشرا، ۲۰۱۶).

یکی از مشکلات اساسی تبعیت شرکت‌ها از قانون محلی‌سازی داده‌ها دشواری تصمیم‌گیری برای این موضوع است که کدام یک از داده‌ها باید به شکل محلی ذخیره شوند و کدامیک از آنها باید به خارج از کشور ارسال شوند. ایجاد تمایز بین داده‌های شخصی و غیرشخصی با هدف محلی‌سازی داده‌ها یک مسئله پیچیده است (میشرا، ۲۰۱۶).

از طرف دیگر، الزامات محلی‌سازی داده‌ها به این دلیل که سبب ایجاد وقفه و تداخل در جریان جهانی داده و کجایی و چگونگی ذخیره‌سازی، پردازش و انتقال آنها می‌شود مورد انتقاد قرار گرفته است. دولت‌ها به شکل فزاینده این محدودیت‌ها را با هدف حفاظت از حقوق شهروندان اعمال می‌کنند. گرچه در عمل محلی‌سازی داده‌ها ممکن است به «بالکانیزه شدن» اینترنت منجر شود و بر حقوق و اقتصاد دیجیتال تأثیر بگذارد. قوانین محلی‌سازی داده‌ها می‌تواند مانع از حرکت داده‌ها خارج از مرزهای ملی شود؛ همچنین می‌تواند سبب محدودیت این مسئله شود که داده‌ها در کجا و توسط چه کسانی ذخیره‌سازی و پردازش شوند (فریزر، ۲۰۱۶).

اینترنت عمده‌تاً ذاتاً بدون ملاحظه مرزهای ملی توسعه یافت تا داده‌ها درون شبکه به طور خودکار و خودمختار با سرعت جریان پیدا کنند. داده‌ها از مکانی به مکان دیگر به سرعت و ظاهراً به شکل تصادفی و غیرقابل پیش‌بینی و بدون آگاهی یا رضایت کاربر انتقال می‌یابند. این نوع جریان آزاد داده در طول مرزها کارایی و مزیت‌های اقتصادی زیادی را در ذخیره‌سازی و پردازش داده‌ها امکان‌پذیر کرده است؛ اما محلی‌سازی یکی از موانع بر سر راه تحقق این هدف است.

تقویت مرزهای ملی از طریق قوانین محلی‌سازی داده‌ها سبب تکه تکه شدن اینترنت می‌شود و این شبکه جهانی را به اینترنت‌های مختلف، مجزا و ویژه تبدیل خواهد کرد که نتیجه آن تأخیر، عدم کارآمدی

و هزینه‌های بیشتر است. به علاوه کاربران اینترنت و صاحبان کسب و کار فعال در اقتصاد جهانی دیجیتال مجبور خواهند شد تا در طیف پیچیده‌ای از حوزه‌های قضایی مختلف که دستورالعمل‌های متضاد را تحمیل می‌کنند فعالیت نمایند. (فریزر، ۲۰۱۶).

منظرهای مختلف محلی‌سازی داده‌ها

فریزر (۲۰۱۶) محلی‌سازی داده‌ها را از منظرهای مختلف بررسی کرده است:

الف) امنیت داده

محلی‌سازی داده‌ها به منزله ابزاری برای ارتقاء امنیت داده و در نتیجه حفاظت از حریم خصوصی و امنیت اطلاعات شخصی کاربران در برابر کنشگران غیردولتی تلقی شده است. اما در عمل ممکن است تأمین‌کنندگان محلی نتوانند همان میزان از دقت تأمین‌کنندگان جهانی (واسطه‌ها یا پلتفرم‌های آنلاین) را به کار برند؛ علت این موضوع منابع مالی کمتر، تخصص پایین‌تر، نیاز کمتر به جذب مشتریان و همین‌طور محدودیت از نظر سطح فناوری است.

ب) حقوق فردی

حفاظت از حقوق اساسی در انتقال و ذخیره‌سازی آنلاین داده‌ها یکی از نگرانی‌های عمده همه دولت‌ها است. فاصله فیزیکی بین محل تولید داده و کاربر تولیدکننده آن داده‌ها در یک زمان مشخص، سبب تضعیف قوانین حفاظت از حقوق افراد می‌شود؛ به‌ویژه زمانی که اعمال این قوانین به مکان وابسته باشد. وقتی تخطی از حقوق افراد توسط مقامات کشور ثالث صورت گیرد و اثر این نقض فقط در قلمرو کشور ثالث پدیدار شود، حفاظت از حقوق بنیادین افراد که مستلزم وجود عنصر کنترل توسط کنشگران دولتی است در دسترس قرار ندارد. بنابراین استفاده از الزامات محلی‌سازی برای ممانعت از انتقال داده‌ها به خارج می‌تواند به منزله ابزاری برای حفاظت از حقوق شهروندان تلقی شود.

ج) نظارت خارجی

ممانعت از نظارت دولت‌های خارجی بر داده‌های تولید شده توسط شهروندان یک کشور، یکی از توجیهات عمده برای اعمال قوانین محلی‌سازی داده‌ها و مبتنی بر این باور است که اگر داده‌ها خارج از کشور باشند امنیت و حریم خصوصی افراد به مخاطره می‌افتد. این موضوع به‌ویژه پس از افشاگری‌های اسنودن بسیار مورد توجه قرار گرفت.

د) نظارت داخلی

دولتها می‌توانند از محلی‌سازی داده‌ها به عنوان ابزاری برای اطمینان از دسترسی به داده‌ها برای اجرای قوانین داخلی در جهت تحقیق و جمع‌آوری شواهد استفاده نمایند. علت این موضوع دشواری دریافت اطلاعات از شرکتهای خارجی درگیر فعالیت گردآوری و پردازش اطلاعات است. از طرف دیگر پلتفرمهای بزرگ نیز ممکن است در برابر درخواست برای افشای اطلاعات کاربران یک کشور مقاومت کنند.

تأثیرات اقتصادی محلی سازی داده‌ها

محلی سازی داده‌ها دارای تأثیرات اقتصادی نیز هست. این رویکرد به منزله یکی از علل شکوفایی اقتصاد داخلی تلقی شده است اما همانطور که فریزر (۲۰۱۶) اشاره کرده است، باید توجه کرد که محلی سازی داده‌ها می‌تواند پیامدهای اقتصادی معکوس در پی داشته باشد. آثار اقتصادی محلی سازی داده‌ها بر بخشهای مختلف از این قرار است:

الف) اقتصاد داخلی

قوانین محلی سازی داده‌ها راهبردی در واکنش به هژمونی آمریکا بر اینترنت است که طی آن تلاش می‌شود تا شرکتهای محلی و داخلی در برابر سهم روزافزون شرکتهای فناوری آمریکایی بتوانند به مزیت رقابتی دست پیدا کنند. برای مثال، قوانینی که ذخیره سازی داده‌ها را در داخل کشور الزامی می‌کنند استقرار مراکز داده محلی را نیز ضروری می‌نمایند. این موضوع مستلزم سرمایه گذاری در زیرساختها و توسعه مشاغل داخلی است.

ب) اقتصاد بین الملل

محدودیت‌های ناشی از محلی سازی داده‌ها می‌تواند بر تجارت بین الملل اثرات منفی داشته باشد: نخست این که امکان دارد این موضوع سبب شود برخی کشورها از ارائه خدمات در داخل کشور خودداری کنند که سبب تحلیل رفتن سرمایه گذاری خارجی می‌شود.

دوم این که تدوین و اعمال قوانین محلی سازی داده‌ها ممکن است سبب تحریک حفاظت گرایی دوسویه شود، زیرا کشورهای دیگر نیز موانعی را بر سر راه تجارت با کشور ما قرار می‌دهند که این موضوع به مصرف کنندگان آسیب می‌زند و توانایی شرکتهای داخلی برای گسترش از طریق اینترنت را محدود می‌کند.

سوم این که قوانین محلی سازی داده‌ها ممکن است سبب شود تا برخی کشورها از توافقنامه‌های تجاری چندجانبه حذف شوند.

علاوه بر این محلی سازی داده‌ها ممکن است هزینه‌های اقتصادی دیگری را نیز در پی داشته باشد. مطالعه‌ای در مورد شش کشور در حال توسعه و ۲۸ کشور اتحادیه اروپا نشان می‌دهد که این قوانین سبب کاهش تولید ناخالص ملی به میزان ۱/۷ درصد، کاهش سرمایه گذاری به میزان ۴/۲ درصد و کاهش صادرات به میزان ۱/۷ درصد شده است (کیم، ۲۰۱۶).

در ادامه به سیاستهای برخی از کشورها برای محلی سازی داده‌ها اشاره می‌شود.

۶- محلی سازی داده در هند

سیاستگذاری اخیر محلی سازی داده‌های در مورد بخش‌های پرداخت و داده‌های شخصی به یکی از پربحث‌ترین موضوعات در کشور هند تبدیل شده است (بلی و پارشیرا، ۲۰۱۸).

چهار رویداد مهم طی سالهای اخیر سبب برجسته شدن بحث محلی سازی داده‌ها در هند شده است: اول انتشار نسخه پیش‌نویس قانون امنیت اطلاعات دیجیتال در مراقبت سلامت^۱ توسط دولت هند در ۲۱ مارس ۲۰۱۸ بود. هدف این قانون دادن اختیارات به اداره ملی سلامت الکترونیک^۲ برای اعمال الزامات محلی سازی در مورد داده‌های سلامت دیجیتال بود.

دوم این که بانک مرکزی هند^۳ دستورالعملی را در ۶ آوریل ۲۰۱۸ صادر کرد که به موجب آن الزامات محلی سازی شدیدی در مورد همه بازیگران عمده در اکوسیستم پرداختهای هند وضع شده است. این دستورالعمل همه تأمین‌کنندگان و درخواست‌کنندگان و واسطه‌های نظام پرداخت را ملزم کرده تا همه داده‌های مرتبط با تراکنشهای پرداخت را فقط در هند ذخیره کنند. فقط تراکنشهایی که دارای عنصر فرامرزی بودند از این دستور مستثنی شده‌اند و بعد از یک فرصت شش ماهه این دستورالعمل از ۱۵ اکتبر ۲۰۱۸ الزامی شد.

مورد سوم انتشار پیشنهادات کمیته تخصصی به رهبری یکی از قضات دیوان عالی هند به نام سریکرشنا^۴ بود. وظیفه این کمیته پیشنهاد یک چارچوب حفاظت از داده جدید برای هند بوده است. این کمیته گزارش و پیش‌نویس لایحه حفاظت از داده‌های شخصی^۵ را در ماه ژوئیه ۲۰۱۸ به دولت ارائه کرد که در آن پیشنهادات کلیدی برای محلی سازی داده‌های شخصی ارائه شده بود. این کمیته با ارائه یک مدل سه شاخه‌ای پیشنهاد کرده بود که دست کم یک نسخه از همه داده‌های شخصی باید در هند ذخیره شود. علاوه بر آن «داده‌های شخصی حساس» مشمول سختگیری بیشتری بود و باید فقط در هندوستان ذخیره سازی و پردازش می‌شد. علاوه بر این دولت این اختیار را داشت تا کشورها، بخشها یا سازمانهای بین‌المللی خاصی را از محدودیتهای ایجاد شده بر سر راه جریان آزاد داده در میان مرزها بر مبنای «ضرورت» یا «منافع راهبردی دولت» استثناء نماید (بیلی و پارشیرا، ۲۰۱۸).

به عبارت دیگر کمیته‌ای که به فرمان دولت هند و زیر نظر قاضی سابق دیوان عالی هند شری بی. ان. سریکرشنا تشکیل شد در پی مطالعه مسائل گوناگون مرتبط با حفاظت از داده‌ها در هند و ارائه برخی پیشنهادات بر پایه اصول مورد توجه برای حفاظت از داده‌ها بود و پیش‌نویس لایحه را ارائه کرد. این کمیته پیش‌نویس مد نظر خود را در تاریخ ۲۷ ژوئیه ۲۰۱۸ به وزارت فناوری اطلاعات و الکترونیک هند ارائه کرد. در این لایحه مجازاتهای مختلفی برای نقض قوانین در نظر گرفته شده است که از دو و نیم میلیون روپیه یا ۲ درصد کل گردش مالی تا هفت و نیم میلیون روپیه یا ۴ درصد از کل گردش مالی جهانی را دربرمی‌گیرد. این لایحه برداشتهای از حریم خصوصی را در هند تغییر می‌دهد. (بهات، ۲۰۱۸) تصویری کلی از لایحه حفاظت از داده‌های شخصی در هند را ارائه کرده است که در شکل ۱ مشاهده می‌شود.

^۱ Digital Information Security in Healthcare Act

^۲ National Electronic Health Authority

^۳ Reserve Bank of India

^۴ Srikrishna Committee

^۵ Personal Data Protection Bill

 رضایت همه داده‌های شخصی، داده‌های شخصی حساس و داده‌های مربوط به کودکان برای ذخیره شدن باید بر مبنای جلب رضایت باشد.	 لایحه حفاظت از داده‌های شخصی چیست؟ هدف این لایحه ایجاد اطمینان از وجود اقتصاد دیجیتال آزاد و منصفانه در هند است و به منزله گامی حیاتی در جهت ارائه چارچوب حریم خصوصی محسوب می‌شود که به شهروندان هند برای حفاظت از داده‌های شخصی خود آزادی کامل می‌دهد
 داده‌های شخصی حساس/حیاتی باید فقط در هند ذخیره شوند.	 چه کسانی از این لایحه متأثر می‌شوند؟ این لایحه بر بخشهای خصوصی و دولتی اعمال می‌شود. این لایحه بر فعالیتهای همه کسب و کارها در هند اعمال می‌شود. - کالاهای و خدماتی که به مسئولان داده در هند ارائه می‌شوند. - هر نوع فعالیتی که در آن پروفایل شهروندان هند دخیل است.  در هر نوع پردازش داده خارج یا داخل هند، یک «نسخه الگو» باید در هند نگهداری شود.
 تعریف داده‌های شخصی بر مبنای پارامتر قابلیت شناسایی^۱ تعیین می‌شود. - ویژگی‌ها - خصوصیات - خصلتها لایحه جدید حفاظت از داده ستون مهمی در اکوسیستم حریم خصوصی هند است. - سوژه‌های داده از حقوق فراموش شدن و حذف شدن از اسناد برخوردارند	 نگهداری امانتی داده‌ها باید گامی در جهت حفاظت از شفافیت با توجه به اصول کلی مرتبط با پردازش داده‌های شخصی تلقی شود. باید از اصول حفظ سند، بررسی‌های داده و ارزیابی تأثیر حفاظت از داده تبعیت شود.  انتصاب یک افسر حفاظت از داده مطابق با فعالیتهای پردازشی خود

^۱ .identifiability

- کاربران می‌توانند نسخه‌ای از داده‌های شخصی را در قالب قابل حمل درخواست کنند. - کاربران از حق تصحیح^۳ و حق تصدیق برخوردارند.	 محصولات، سیستم‌ها و فرایندها باید مفاهیم حریم خصوصی^۱ را به هنگام طراحی در طول توسعه مد نظر قرار دهند.
 مجازات سختگیرانه جریمه‌ها برابر با ۲ تا ۴ درصد کل گردش مالی جهانی یا ۲/۵ تا ۷ میلیون روپیه	

شکل (۱) نگاهی کلی به لایحه حفاظت از داده‌های شخصی هند؛ منبع: (بهات، ۲۰۱۸)

در این لایحه منظور از داده‌های شخصی، داده‌های مربوط به یک شخص معمولی است که به شکل مستقیم یا غیرمستقیم قابل شناسایی می‌باشد. شناسایی بر اساس ویژگی، خصوصیت، خصلت و هر ویژگی هویتی دیگر و یا ترکیبی از این خصیصه‌ها با اطلاعات دیگر صورت می‌گیرد. به عبارت دیگر، داده‌های شخصی شامل هر نوع داده مرتبط با افراد از قبیل واژگان عبور، داده‌های مالی، داده‌های سلامت، شناساگرهای رسمی، داده‌های جنسی، گرایش جنسی، داده‌های ژنتیکی، کاست، قبیله، باور سیاسی و مذهبی یا هر نوع وابستگی دیگر می‌شود.

این قانون فقط چند هفته پس از آنکه مقررات عمومی حفاظت از داده اتحادیه اروپا در ۲۵ مه ۲۰۱۸ اجرایی شد و کالیفرنیا قانون حریم خصوصی مصرف‌کننده^۴ را در پایان ماه ژوئن تصویب کرد، ارائه شد. بر اساس فصل یک از بخش یک این لایحه، این قانون «به کل هند تسری می‌یابد». اما در واقع بسیار گسترده‌تر است و به شرکت‌های خارج از هند در سرتاسر جهان نیز اعمال می‌شود. همه شرکت‌ها در همه جای جهان که داده‌های شخصی را در قلمرو هند پردازش می‌کنند و هر شرکت هندی که داده‌های شخصی را پردازش می‌کند باید از این قانون تبعیت کند.

قانون حفاظت از داده‌های شخصی به همه داده‌های شخصی که در درون هندوستان گردآوری، افشاء و به اشتراک گذاشته می‌شوند اعمال می‌شود. منظور از پردازش در این قانون ذخیره‌سازی است که به طور مفصل این مفهوم در این قانون مورد توجه قرار گرفته و ارتباط مستقیمی با محلّی سازی داده‌ها در کشور هند دارد.

^۱. privacy-by-design

^۳. correction

^۴. California Consumer Privacy Act

این قانون شامل یک مقدمه و ۱۵ فصل است. در بند دوم مقدمه این لایحه آمده است که این قانون در موارد زیر به کار می‌رود:

الف) پردازش اطلاعات شخصی در هر جایی که این داده‌ها گردآوری، افشاء و به اشتراک گذاشته می‌شوند یا به شکل دیگر درون قلمرو هند پردازش می‌شوند.

ب) پردازش داده‌های شخصی توسط دولت، هر شرکت هندی، هر شهروند هندی و یا هر شخص یا گروهی از اشخاص که تحت قوانین هند قرار دارند یا بر اساس آن ایجاد می‌شوند، انجام می‌گیرد. در وب‌سایت اینسایتس ماینڈمپ که به بررسی محلی‌سازی داده‌ها در هند اختصاص دارد دلایل نیاز به محلی‌سازی داده‌ها به این شکل توضیح داده شده است:

- جهت امنیت داده‌های شهروندان، حریم خصوصی داده‌ها، حق حاکمیت داده، امنیت ملی و توسعه اقتصادی کشور

- بیشتر داده‌های ناشی از فروش آنلاین در پلتفرم‌های تجاری احتمالاً توسط شرکت‌های داده آمریکایی میزبانی و ذخیره‌سازی می‌شوند.

- گردآوری گسترده داده توسط شرکت‌های فناوری به آنها امکان داده است تا خارج از مرزهای کشور هند این داده‌ها را پردازش و از آنها کسب درآمد کنند.

- کاستن از مخاطرات استفاده غیرقاعده‌مند و خودخواهانه داده‌های شخصی

- با پیشرفت رایانش ابری، داده‌های کاربران هندی خارج از مرزهای این کشور است که سبب منازعات در حوزه قضایی در مناقشات مختلف می‌شود.

- داده‌ها آثار دیجیتالی تراکنش‌ها هستند. به هنگام بروز مخاصمات امکان خاموش کردن و یا از کار انداختن مراکز داده وجود دارد. این سناریوها سبب شده است تا کشورها به سمت زیرساخت‌های داخل روی بیاورند.

مزیت‌های محلی‌سازی داده‌ها در هند

- تصور می‌شود که محلی‌سازی داده‌ها سبب ایجاد برخی مزایا برای صنایع مرتبط با مراکز داده می‌شود.

- این امر سبب افزایش سرعت تراکنش‌ها و کاهش رکود در شبکه می‌شود.

- می‌تواند به رشد افراد و شرکت‌های درگیر در زیرساخت فناوری اطلاعات کمک کند.

- فرصتی برای شرکت‌های فناوری است تا چشم‌انداز خود را از خدمات به محصولات تغییر دهند.

معایب محلی‌سازی داده‌ها برای هند

- می‌تواند سبب ایجاد نوعی سیاست دومینیویی حفاظت‌گرا شود که کشورهای دیگر نیز از آن تبعیت کنند؛ سبب بخش‌بخش شدن اینترنت می‌شود.

- شرکت‌های و نهادهای آمریکایی مخالف محلی سازی داده‌ها هستند.
- می‌تواند بر استارت‌آپ‌های تازه کاری که در پی رشد در سطح جهانی هستند تأثیر منفی داشته باشد.
- می‌تواند بر برخی شرکت‌ها که داده‌های خارجی را در درون کشور پردازش می‌کنند تأثیر منفی داشته باشد.
- حتی اگر داده‌ها درون کشور ذخیره سازی شوند، کلیدهای رمزنگاری ممکن خارج از دسترس نهادهای ملی باشد.
- می‌تواند به منزله مانعی بر سر راه گسترش خدمات قلمداد شود و علاوه بر مصرف کنندگان بر رشد بازار پرداخت نیز تأثیر منفی بگذارد.
- عدم وجود زیرساخت کافی برای مدیریت و گردآوری کارآمد داده یکی از مسائل بحث برانگیز است.

۷- محلی سازی داده‌ها در روسیه

پس از افشاگرهای اسنودن در سال ۲۰۱۳ قوانین مرتبط با داده در روسیه نیز در واکنش به نگرانی‌های داخلی و منطقه‌ای وضع شدند و به اجرا درآمدند. برخی از این نگرانی‌ها شامل تمایل دولت روسیه برای سانسور اطلاعات و کنترل نارضایتی‌ها است که هر دوی آنها نقش مهمی در توسعه سیاست‌های محلی سازی داده‌ها در این کشور داشته است. هدف از این عمل در اصل تضمین ثبات دولت روسیه بوده است. دولت روسیه از طریق پیگیری اطلاعات بیش از صد میلیون کاربر اینترنت، ایمن سازی داده‌ها در سرورهای داخلی و دادن اختیار به نهادهای قانونی برای مقابله با افراط گرایی، حقوق حاکمیت دولتی خود را بر فضای آنلاین این کشور اعمال می‌کند (نیوتون و سایمرز، ۲۰۱۸).

اولین موج از ماده‌های قانونی محلی سازی داده‌ها در روسیه در حوزه بانکداری ظاهر شد. بر اساس الحاقیه‌های اضافه شده به قانون فدرال «فعالیت بانک‌ها و بانکداری» که در سال ۲۰۱۳ تصویب شد، نهادهای مالی تحت نظارت بانک مرکزی روسیه ملزم شدند تا همه تراکنش‌های مالی خود را در پایگاه‌های داده ذخیره سازی کنند. قوانین بعدی بانک مرکزی روسیه، تمامی بانک‌ها را ملزم کرد تا نسخه‌های پایگاه داده خود را در داخل روسیه نگهداری نمایند. موج دوم قانونگذاری در حوزه محلی سازی داده‌ها در سال ۲۰۱۴ و پس از حملات تروریستی در شهر ولگوگراد ظاهر شدند که محدودیت‌های بیشتری را در برابر پرداخت‌های مالی الکترونیکی ناشناس ایجاد کرد، تعیین هویت کاربران خدمات اینترنتی در نقاط دسترسی همگانی را الزامی اعلام نمود و نکته مهمتر الحاقیه‌هایی بود که به قانون اصلی تنظیم کننده مقررات فناوری اطلاعات در روسیه، قانون فدرال شماره ۱۴۹-اف،^۱ افزوده شدند. این بخش مستقیماً به الزامات محلی سازی داده‌ها مربوط است که «سازمان دهنده انتشار اطلاعات در اینترنت»^۲ نام دارد و شامل هر

^۱ Federal Law No. 149-FZ

^۲ Organizer of dissemination of internet in internet

شخص تسهیل کننده عملکردهای سیستمهای اطلاعاتی و/یا برنامه‌های رایانه‌ای است که ممکن است برای دریافت، انتقال، توزیع و/یا پردازش پیام‌های الکترونیکی به کار رفته شده یا به کار می‌رود. بخشی از وظایف این سازماندهی ذخیره‌سازی ترافیک و داده‌های کاربران به مدت شش ماه در روسیه و همکاری با نهادهای اجرای قانون در روسیه از جمله نهاد امنیت فدرال برای دادن اجازه دسترسی به داده‌ها در صورت درخواست آن است (ساولیف، ۲۰۱۶).

علاوه بر این، دولت روسیه شرکتهای روسی را ملزم کرده است تا برای ذخیره‌سازی داده‌ها روی سرورهای روسی هزینه پرداخت کنند. قوانین محلی‌سازی داده در روسیه پلتفرمهای بزرگی نظیر توئیتر، فیس‌بوک، اپل، گوگل و مایکروسافت را ملزم کرده است تا به قوانین روسیه تن دهند. روسیه با ملزم کردن این شرکتها و شرکتهای دیگر برای ذخیره‌سازی داده‌های شهروندان روسی در سرورهای خاص واقع در روسیه، به نحوی مؤثر موانع اضافی دیگری را نیز برای ورود به بخش بازار روسیه فراروی آنها قرار داده است. دولت روسیه شرکتهایی را که با انتقال حجم عظیم داده‌های کاربران این کشور سروکار دارند ملزم کرده است تا فضای سرورهای واقع در روسیه را اجاره کنند و هزینه‌هایی را به شرکتهای خدمات داده روسیه پرداخت نمایند. در غیر این صورت باید خطر مسدود شدن کامل فعالیتهای خود درون قلمرو این کشور را پذیرا شوند.

قانون محلی‌سازی داده به طور رسمی قانون فدرال شماره ۲۴۲ ف.ز.^۱ نام دارد. الحاقیه‌های نهایی به این قانون در ۱ سپتامبر ۲۰۱۵ اجرایی شدند و همه شرکتهای داخلی و خارجی را ملزم شدند تا اطلاعات شخصی کاربران شهروندان روسیه را روی سرورهای انباشت، ذخیره‌سازی و پردازش کنند که به طور فیزیکی درون مرزهای روسیه قرار گرفته‌اند.

سرویس فدرال ارتباطات، فناوری اطلاعات و رسانه‌های جمعی روسیه^۲ که روسکومنادزور^۳ نامیده می‌شود به شدت بر اجرای این قانون در روسیه نظارت دارد. در پی تشدید فعالیتهای این نهاد و مسدودسازی فعالیت بیش از ۷۳۰۰ وب سایت در این کشور، بسیاری از شرکتهای روسی و آمریکایی داده‌های خود را به مراکز داده روسیه منتقل کردند. اپل، فیس بوک و گوگل همگی در نهایت از این قانون تبعیت کردند. اما فعالیت سایت لینکداین در سال ۲۰۱۶ در روسیه به دلیل ناتوانی در تبعیت از این قانون متوقف شد. روسکومنادزور همچنین گوگل و اپل را ملزم کرد تا لینکداین را از فروشگاه‌های آنلاین اپلیکیشن‌های خود نیز حذف کنند. روسیه از قوانین محلی‌سازی داده به عنوان بخشی از راهبرد امنیتی گسترده‌تر خود استفاده می‌کند (نیوتون و سایمرز، ۲۰۱۸).

^۱ Federal Law No. 242-FZ

^۲ Federal Service for Supervision of Communications, Information Technology and Mass Media

^۳ Roskomnadzor

۸- اتحادیه اروپا (مقررات عمومی حفاظت از داده‌ها)^۱

پس از چهار سال آماده‌سازی و بحث، مقررات عمومی حفاظت از داده‌ها در نهایت در تاریخ ۴ آوریل ۲۰۱۶ در پارلمان اروپا تصویب و در ۲۵ مه ۲۰۱۸ به اجرا گذاشته شد. هدف از این قانون هماهنگی قوانین حفظ حریم خصوصی در سرتاسر اروپا، حفاظت و توانمندسازی همه شهروندان اتحادیه اروپا از منظر حریم داده و بازنگری در نحوه رویکرد سازمانهای واقع در اتحادیه اروپا به حریم خصوصی است.^۲

این قانون قوی‌ترین قانون حریم خصوصی و امنیت در جهان است و وظایفی را برای همه سازمانها در همه جای جهان هنگام هدفگذاری یا گردآوری داده‌های مرتبط با افراد ساکن در اتحادیه اروپا تعیین کرده است. در این قانون جرایم شدیدی علیه کسانی که معیارهای حریم خصوصی و امنیت آن را نقض کنند وضع شده است و میزان جرایم تعیین شده در آن به میلیون‌ها یورو نیز بالغ می‌شود.^۳

اگر فردی یا نهادی داده‌های شخصی شهروندان یا ساکنان اتحادیه اروپا را پردازش کند یا خدمات و کالاهایی را به این افراد عرضه کند، این قانون به وی اعمال می‌شود، حتی اگر ساکن اتحادیه اروپا نباشد. داده‌های شخصی شامل هر نوع اطلاعات مرتبط با افرادی است که امکان شناسایی مستقیم یا غیرمستقیم آنها وجود داشته باشد. نام و آدرس ایمیل، اطلاعات موقعیت، قومیت، جنسیت، باورهای شخصی و دیدگاه‌های سیاسی داده‌های شخصی محسوب می‌شوند. منظور از پردازش داده در این قانون هر نوع عملی است که به شکل خودکار یا دستی روی داده‌ها انجام می‌شود و مواردی همانند گردآوری، ضبط، ساماندهی، ساختاربندی، ذخیره‌سازی، استفاده، پاک کردن و تقریباً همه چیز را دربرمی‌گیرد. در این قانون سوژه داده شخصی است که داده‌اش پردازش می‌شود و کنترل‌کننده داده فردی است که تصمیم می‌گیرد چرا و چگونه داده‌های شخصی پردازش می‌شوند.

۹- محلی سازی داده در چین

یکی از ویژگیهای محلی‌سازی داده‌ها در چین جامعیت آن است. این اصل علاوه بر جمع‌آوری داده‌های شخصی، «داده‌های مهم مرتبط با زیرساخت اطلاعاتی حساس» را نیز شامل می‌شود که این عبارت تقریباً همه جنبه‌های زندگی روزمره را در برمی‌گیرد (وی، ۲۰۱۸).

قانون امنیت سایبری چین^۴ در ۷ نوامبر ۲۰۱۶ تصویب و در ۱ ژوئن ۲۰۱۷ به اجرا گذاشته شد. این قانون به عنوان اولین مقررات جامع حریم خصوصی و امنیت برای فضای سایبر، شامل برخی تغییرجهت‌های

^۱ . General Data Protection Regulation

^۲ . <https://eugdpr.org/>

^۳ . <https://gdpr.eu/what-is-gdpr/>

^۴ . CSL

کلی از جمله محلی‌سازی داده‌ها است. قانون امنیت سایبری به «اپراتورهای شبکه» و اپراتورهای «زیرساخت اطلاعاتی حساس»^۱ اعمال شده است. منظور از زیرساخت‌های حساس این است که هر نوع اختلال در عملکرد آن به آسیب جدی علیه امنیت ملی، اقتصاد ملی و زندگی مردم و منافع عمومی منجر می‌شود. بر اساس این قانون «اطلاعات شخصی» و «داده‌های مهم» که توسط اپراتورهای اطلاعاتی حساس در چین گردآوری و یا تولید شده‌اند باید در کشور چین ذخیره‌سازی شوند. گرچه بر طبق قانون امنیت سایبری الزام محلی‌سازی داده‌ها فقط برای اپراتورهای زیرساختی حساس اعمال می‌شد اما در نسخه‌های بعد اپراتورهای شبکه نیز مشمول این محدودیت شدند. در نتیجه زمانی که یک اپراتور شبکه می‌خواهد این داده‌ها را به خارج از کشور ارسال کند باید ضرورت ارسال آن داده‌ها را اثبات کند و نوعی خود-ارزیابی امنیتی یا نوعی ارزیابی امنیتی رسمی انجام دهد. یک ارزیابی رسمی امنیتی توسط مقامات چین شامل این موارد است:

۱) کارگروهی به منظور انجام ارزیابی به‌وسیله «آزمون از راه دور» و «بازرسی در محل»^۲ و ارائه یک گزارش ارزیابی مستقر می‌شود.

۲) یک کمیته کارشناسی که توسط اداره فضای مرکزی چین^۳ یا متولیان قانونگذاری بخش مربوطه منصوب می‌شود آن گزارش را مرور و پیشنهاد می‌کند که انتقال داده پیشنهادی باید پذیرفته شود یا خیر. ۳) اداره فضای سایر یا بخش قانونگذار مربوط تصمیم نهایی را اتخاذ می‌کند (ژانگ و همکاران، ۲۰۱۸).

در قانون فضای سایبری چین تعریف جامعی از زیرساخت اطلاعاتی حساس ارائه شده اما بعدها این عبارت به «داده‌های مهم» تغییر داده شد که دامنه قانونگذاری مرتبط با آن را توسعه داده است. در این قانون مقررات مرتبط با محلی‌سازی داده با جزئیات زیادی شرح داده شده است، اما استفاده گسترده تعریف از عبارت «داده‌های مهم» راه را برای مداخله نامحدود دولت در هر صنعتی باز گذاشته است (وی، ۲۰۱۸).

۱۰- نتیجه‌گیری

با توجه به بحث‌هایی که صورت گرفت تصور می‌شود ضرورت دارد تا یک راهبرد بلندمدت برای سیاستگذاری در مورد محلی‌سازی داده در داخل ایران پیشنهاد و در مورد محلی‌سازی یا عدم محلی‌سازی و نیز سطوح مختلف آن تصمیمات لازم اتخاذ شود. همچنین باید زیرساخت‌های فناورانه و فنی و نیز دانش فنی مورد نیاز برای تحقق این اصل در کشور فراهم باشد و یا تأمین شود. محلی‌سازی داده‌ها موضوعی مجزا و منفرد نیست بلکه با سیاست‌های اساسی اجتماعی و اقتصادی کشور و نوع تعاملات بین‌المللی و

^۱ Critical Information Infrastructure

^۲ on-site inspection

^۳ Cyberspace Administration of China (CAC)

جایگاه آن در روابط بین‌المللی و جهانی کسب و کارها به‌ویژه در زمینه فناوریهای اطلاعاتی و ارتباطی ارتباط مستقیم دارد. هر نوع سیاستگذاری در جهت محلّی سازی سختگیرانه داده‌ها آثار و پیامدهای مختلفی برای فعالیت فرامرزی شرکتها و به‌ویژه شرکتهای نوپای فناوری اطلاعات دارد. از این رو هنگام سیاستگذاری برای محلّی سازی داده‌ها باید علاوه بر صیانت از داده‌های تولید کاربران و حریم شخصی آنها، تعامل مناسب با بخش‌های گوناگون و فرامرزی فضای سایبر مورد توجه قرار گیرد.

۱۱- منابع

- Bailey, Rishab and Parsheera, Smriti (2018) Data localisation in India: Questioning the means and ends, New Delhi : National Institute of Public Finance and Policy
- Bhatt, Nitin (2018) Personal Data Protection Bill-2018 An initiative to enforce privacy principles in India, New Delhi: EY; [https://www.ey.com/Publication/vwLUAssets/ey-personal-data-protection-bill-2018/\\$File/ey-personal-data-protection-bill-2018.pdf](https://www.ey.com/Publication/vwLUAssets/ey-personal-data-protection-bill-2018/$File/ey-personal-data-protection-bill-2018.pdf)
- Chander, A. & Le, U. P. (2015). Data nationalism. *Emory Law Journal*, 64(3). Retrieved from <https://ssrn.com/abstract=2577947>
- Determann, Lothar, and Gupta, Chetan (2019) Indian Personal Data Protection Act, 2018 - Draft bill and its history, compared to EU GDPR and California Privacy Law; https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3244203
- Ferracane, Martina. F. (2017) *Restrictions on cross-border data flows: A taxonomy*. European Centre for International Political Economy. <https://ecipe.org/publications/restrictions-to-cross-border-data-flows-a-taxonomy/>
- Fraser, Erica (2016) Data Localisation and the Balkanisation of the Internet; Scripted, Volume 13, Issue 3, December 2016
- Insights Mindmaps (2017) General Studies-3; Topic- Challenges to internal security through communication networks, role of media and social networking sites in internal security challenges
- Kim, Jim Yong (2016) Digital Dividends; World Development Report 2016; New York: World Bank Group.
- Mishra, Neha (2016) Data Localization Laws in a digital World; Data Protection or Data Protectionism? The Public Sphere | 2016 issue.
- Newton, Matthew & Symmers, Julia (2018) Russian Data Localization Laws: "Security" & Economy; https://jsis.washington.edu/news/russian-data-localization-enriching-security-economy/#_ftn22

حوزه فضای مجازی به اندازه انقلاب اسلامی اهمیت دارد. این فضا مثل یک رودخانه پر از آب و خروشان است که می آید و دائماً هم بر آب آن افزوده و خروشان تر می شود. اگر ما بر این رودخانه تدبیر کنیم و برنامه داشته باشیم، زهکشی کنیم و هدایت کنیم این رودخانه را تا به سد بریزد، می شود فرصت. اگر رهایش کنیم و برنامه ای برای آن نداشته باشیم می شود یک تهدید.



csri.majazi.ir