

National Information Network, Freedom of Expression and Privacy: A Comparative Analysis of National Communication Infrastructures and Proposing a Policy Model within the Legal Framework of the Islamic Republic of Iran

By: Seyyed Mohammad Ali Mortazavi Shahroudi, M.A.✉

Abstract:

The present study analyzes the complex and multilayered relationship between the development of the "National Information Network" as a digital governance strategy and the fundamental rights of "freedom of expression," "free flow of information," and "privacy" within the legal system of the Islamic Republic of Iran. The main research problem is the theoretical and practical gap in aligning the technical, security, economic, and infrastructural objectives of the National Information Network with the guaranteed rights of citizens enshrined in the Constitution (particularly Articles 3, 9, 24, 25, and 175) and ordinary laws (such as the Law on Dissemination and Free Access to Information). Employing a comparative-analytical research method and drawing upon the theoretical frameworks of "Cyber Sovereignty" and "Layers of Internet Control," this article exclusively examines the experiences of leading countries in establishing "national/independent information networks" (China, Russia, the European Union, and the United States) and their specific challenges in balancing freedom of expression and data protection. Focusing on a critical analysis of the "Document on the Elaboration of National Information Network Requirements" approved by the Supreme Council of Cyberspace, the findings indicate that the success of this national megaproject lies not merely in technical advancement and infrastructure coverage, but in transitioning from a security-restrictive approach to a rights-based developmental one. This requires legal transparency, the establishment of multifaceted oversight institutions, and the urgent enactment of the long-stalled "Personal Data Protection Bill." By presenting an analytical framework and offering structural, legislative, and legal recommendations, this study argues that the National Information Network can only serve as a platform for sustainable development if it is underpinned by a new "Digital Social Contract" between the state and citizens, based on trust, transparency, and mutual respect for rights and responsibilities.

Keywords: *National Information Network, Freedom of Expression, Privacy, Cyber Sovereignty, Communication Law*

✉ PhD student in Culture and Communication, Baqir al-Olum University, Qom, Iran
Email:

Received: 2025/10/12

Accepted: 2026/05/18

DOI: 10.22082/CR.2026.2074492.2863

شبکه ملی اطلاعات، آزادی بیان و حریم خصوصی: تحلیل تطبیقی زیرساخت‌های ملی ارتباطات و ارائه الگوی سیاستی در چارچوب حقوقی جمهوری اسلامی ایران

سید محمدعلی مرتضوی شاهرودی ✉

چکیده

پژوهش حاضر به تحلیل رابطه پیچیده و چندلایه میان توسعه «شبکه ملی اطلاعات» به عنوان یک راهبرد حاکمیت دیجیتال و حقوق بنیادین «آزادی بیان»، «جریان آزاد اطلاعات» و «حریم خصوصی» در نظام حقوقی جمهوری اسلامی ایران می‌پردازد. مسئله اصلی تحقیق، شکاف نظری و عملی در چگونگی هم‌راستاسازی اهداف فنی، امنیتی، اقتصادی و زیرساختی شبکه ملی اطلاعات با تضمین حقوق آشکار شهروندان در قانون اساسی (به‌ویژه اصول ۳، ۹، ۲۴، ۲۵ و ۱۷۵) و قوانین عادی (نظیر قانون انتشار و دسترسی آزاد به اطلاعات) است. مقاله با بهره‌گیری از روش تحقیق تطبیقی-تحلیلی و با تکیه بر چارچوب نظری «حاکمیت سایبری» و «لایه‌های کنترل اینترنت»، منحصر به بررسی تجارب کشورهای پیشرو در ایجاد «شبکه‌های ملی/مستقل اطلاعاتی» (چین، روسیه، اتحادیه اروپا و ایالات متحده) و چالش‌های مشخص آنها در موازنه با مقوله آزادی بیان و حفاظت از داده‌ها می‌پردازد. یافته‌ها با تمرکز بر تحلیل انتقادی «سند تبیین الزامات شبکه ملی اطلاعات» مصوب شورای عالی فضای مجازی، نشان می‌دهد که موفقیت این ابرپروژه ملی نه فقط در گرو پیشرفت فنی و پوشش زیرساختی، بلکه مستلزم گذار از رویکرد امنیتی-محدودیت‌محور به رویکرد حقوقی-توسعه‌ای، شفافیت قانونی، ایجاد نهادهای نظارتی چندوجهی و تصویب معطل‌مانده «لایحه حفاظت از داده‌های شخصی» است. این پژوهش با ارائه یک چارچوب تحلیلی و پیشنهاداتی ساختاری، تقنینی و حقوقی، استدلال می‌کند که شبکه ملی اطلاعات تنها در صورتی می‌تواند به بستری برای توسعه پایدار تبدیل شود که پشتوانه آن یک «قرارداد اجتماعی دیجیتال» جدید میان حاکمیت و شهروندان بر پایه اعتماد، شفافیت و احترام متقابل به حقوق و مسئولیت‌ها باشد.

واژه‌های کلیدی: شبکه ملی اطلاعات، آزادی بیان، حریم خصوصی، حاکمیت سایبری، حقوق ارتباطات

✉ دانشجوی دکترای فرهنگ و ارتباطات، دانشگاه باقرالعلوم، قم، ایران

پذیرش نهایی: ۱۴۰۵/۰۲/۲۸

تاریخ دریافت: ۱۴۰۴/۰۷/۲۰

مقدمه

در دهه‌های اخیر، رشد تصاعدی فناوری‌های اطلاعات و ارتباطات، مرزهای سنتی حاکمیت ملی را درنور دیده و مفهوم قدرت و امنیت را در عرصه بین‌الملل با تحولات بنیادین مواجه ساخته است (معتدنی‌زاد، ۱۳۸۸: ۴۵). جریان فرامرزی و لحظه‌ای داده‌ها، ظهور پلتفرم‌های جهانی فراملی و وابستگی روزافزون زیرساخت‌های حیاتی کشورها به اینترنت جهانی، دولت‌ها را به اتخاذ راهبردهایی نوین برای حفظ «استقلال دیجیتال»، تاب‌آوری زیرساختی در برابر تهدیدات سایبری و صیانت از امنیت ملی واداشته است. یکی از مهم‌ترین و بحث‌برانگیزترین این راهبردها، طراحی و اجرای «شبکه‌های ملی اطلاعات»^۱ است؛ زیرساخت‌های ارتباطی بومی که با هدف مدیریت ترافیک داده‌های داخلی، کاهش وابستگی به شبکه جهانی اینترنت، ارائه خدمات پایدار و پرسرعت و توسعه اقتصاد دیجیتال بومی ایجاد می‌شوند.

جمهوری اسلامی ایران نیز از سال ۱۳۸۴ ایده اولیه شبکه ملی اطلاعات را مطرح و پس از شکل‌گیری شورای عالی فضای مجازی، در جلسه پانزدهم این شورا در تاریخ ۳ دی‌ماه ۱۳۹۲، تعریف رسمی و قانونی آن را به تصویب رساند. بر اساس «طرح کلان و معماری شبکه ملی اطلاعات»، این شبکه «زیرساخت ارتباطی مبتنی بر پروتکل اینترنت^۲ با بهره‌گیری از سوئیچ‌ها، مسیریاب‌ها و مراکز داده داخلی» تعریف شده که هدف اصلی آن «کاهش وابستگی به اینترنت جهانی و مدیریت ترافیک داخلی» عنوان گردیده است (مرکز ملی فضای مجازی، ۱۳۹۲: ۳). متعاقباً «سند تبیین الزامات شبکه ملی اطلاعات» در سال ۱۳۹۵ به تصویب رسید تا ابعاد مختلف خدمات و کارکردهای این شبکه را روشن‌تر سازد. با این حال، این پروژه عظیم ملی از همان ابتدا با پرسشی بنیادین و چالش‌برانگیز در حوزه حقوق عمومی، حقوق بشر و حقوق ارتباطات مواجه بوده است: چگونه می‌توان اهداف راهبردی حاکمیتی، امنیتی و اقتصادی شبکه ملی اطلاعات را با حقوق بنیادین شهروندان، به‌ویژه «آزادی بیان» و «حق دسترسی آزاد به اطلاعات» جمع نمود آن‌گونه که در اسناد بین‌المللی (نظیر ماده ۱۹ اعلامیه جهانی حقوق بشر) و قوانین داخلی ایران (به‌ویژه اصول قانون اساسی) تضمین شده است، بتوان به یک موازنه حقوقی پایدار دست یافت؟ این تعارض بالقوه از آنجا ناشی می‌شود که ابزارهای فنی و مدیریتی به‌کار

1. National Information Networks

2. IP

شبکه ملی اطلاعات،
آزادی بیان و حریم
خصوصی: تحلیل تطبیقی
زیرساخت‌های ملی
ارتباطات و ارائه الگوی
سیاستی در چارچوب حقوقی
جمهوری اسلامی ایران

رفته در یک شبکه ملی اطلاعات (نظیر دروازه‌های کنترل ترافیک، تجهیزات بازرسی عمیق بسته‌ها، سیستم نام دامنه بومی و پلتفرم‌های انحصاری داخلی)، ذاتاً این قابلیت را دارند که به اهرم‌هایی قدرتمند تبدیل شوند، به‌طوری که برای سانسور محتوا، محدودسازی دسترسی به منابع اطلاعاتی بین‌المللی، نقض گسترده حریم خصوصی شهروندان و ایجاد فضای خودسانسوری مؤثر واقع شوند (دناردیس^۱، ۲۰۱۴: ۳۲). در حالی که ادبیات پژوهشی موجود در ایران عمدتاً بر ابعاد فنی، امنیتی و اقتصادی شبکه ملی اطلاعات متمرکز بوده (رضایی و همکاران، ۱۳۹۶: ۱۲۴) و پژوهش‌های انتقادی بین‌المللی نیز کمتر به ارائه راهکارهای عملی و بومی‌سازی شده برای نظام‌های حقوقی خاص مانند ایران پرداخته‌اند (مک‌کینون^۲، ۲۰۱۲: ۴۵)، خلأ جدی و محسوسی در زمینه تحلیل تطبیقی تجارب سایر کشورها در ساخت و راه‌اندازی «زیرساخت‌های مشابه» و انطباق نتایج آن با چارچوب حقوقی منحصربه‌فرد جمهوری اسلامی ایران وجود دارد. این پژوهش درصدد پر کردن این شکاف علمی و ارائه تحلیلی چندبعدی از این چالش است.

پیشینه پژوهش

بررسی نظام‌مند و انتقادی ادبیات موجود در حوزه شبکه ملی اطلاعات و نسبت آن با آزادی بیان، نشان‌دهنده وجود سه جریان فکری غالب است. این بخش به تفکیک به گزارش این جریان‌ها و آثار شاخص آنها پرداخته و در نهایت، شکاف پژوهشی و جایگاه تحقیق حاضر را مشخص می‌سازد.

جریان اول: رویکرد فنی-اقتصادی و امنیتی (با تأکید بر ادبیات داخلی)

بخش عمده‌ای از پژوهش‌های داخلی که به موضوع شبکه ملی اطلاعات پرداخته‌اند، عمدتاً بر مزایای راهبردی، فنی، امنیتی و اقتصادی این پروژه متمرکز بوده و نگاهی عمدتاً درون‌گفتمانی به آن داشته‌اند.

محمدی (۱۳۹۵) در مقاله «ضرورت‌های راهبردی شبکه ملی اطلاعات» این پروژه را از منظر «دفاع سایبری»، «صیانت از داده‌های ملی» و «مقابله با تهدیدات نرم» تحلیل کرده و آن را گامی ضروری برای تحقق «حاکمیت سایبری» می‌داند.

1. DeNardis

2. MacKinnon

رضایی و همکاران (۱۳۹۶) در پژوهش خود با عنوان «تحلیل هزینه-فایده توسعه ترافیک داخلی در شبکه ملی اطلاعات»، با ارائه یک مدل اقتصادی، مزایای کاهش هزینه‌های پهنای باند بین‌الملل، افزایش سرعت دسترسی برای کاربران نهایی و رونق کسب‌وکارهای بومی را به عنوان دستاوردهای اصلی این پروژه برجسته کرده‌اند.

کهنوند (۱۳۹۶) نیز در مقاله «شبکه ملی اطلاعات» با رویکردی فرهنگی-امنیتی، این پروژه را پاسخی به «جنگ نرم» و «تهاجم فرهنگی» دشمنان دانسته و ضرورت آن را برای «حفظ سلامت فرهنگی و امنیتی جامعه» خاطرنشان ساخته است.

در سطحی کلان‌تر، همایون و هاشمی (۱۳۹۶) در مطالعه خود با عنوان «بازنمایی شبکه ملی اطلاعات در رسانه‌های برون‌مرزی»، این پروژه را از منظر «استقلال رسانه‌ای» و «مقابله با هژمونی (سلطه) خبری غرب» تحلیل کرده‌اند. نقد جریان اول: نقطه ضعف مشترک و اساسی این دسته از آثار، غفلت نسبی یا کم‌توجهی آشکار به ابعاد حقوقی-اجتماعی و پیامدهای بالقوه این پروژه بر حقوق شهروندی، به‌ویژه آزادی بیان و حق بر حریم خصوصی است. در این پژوهش‌ها، حقوق بنیادین شهروندان یا به کلی نادیده گرفته می‌شود و یا به عنوان یک متغیر وابسته و چالش فرعی در نظر گرفته می‌شود که باید در خدمت اهداف کلان‌تر امنیتی، اقتصادی و فنی مدیریت شود. این نگاه تک‌بعدی، مانع از شکل‌گیری یک گفتمان جامع و متوازن در سیاست‌گذاری این حوزه شده است.

جریان دوم: رویکرد انتقادی و حقوق‌بنیاد (بیشتر در ادبیات بین‌المللی)

در نقطه مقابل، جریان انتقادی و حقوق‌بنیادی قرار دارد که با نگاهی بدبینانه و از منظر حقوق بشر، پروژه‌های حاکمیت دیجیتال ملی را به عنوان ابزاری برای گسترش «سرمایه‌داری نظارتی»^۱ و تقویت «اقتدارگرایی دیجیتال» تحلیل می‌کند.

شوشانا زوبوف^۲ (۲۰۱۹) در اثر کارساز خود به نام «عصر سرمایه‌داری نظارتی»، استدلال می‌کند که مدل کسب‌وکار پلتفرم‌های بزرگ جهانی بر پایه جمع‌آوری و تحلیل کلان‌داده‌های رفتاری شهروندان برای پیش‌بینی و در نهایت کنترل و شکل‌دهی به رفتار آنها استوار است. از این منظر، شبکه‌های

1. Surveillance Capitalism

2. Zuboff

شبکه ملی اطلاعات،
آزادی بیان و حریم
خصوصی: تحلیل تطبیقی
زیرساخت‌های ملی
ارتباطات و ارائه الگوی
سیاستی در چارچوب حقوقی
جمهوری اسلامی ایران

ملی اطلاعات می‌توانند این نظارت را از سطح شرکتی و تجاری به سطح دولتی تسری داده و آن را به شکلی بی‌سابقه متمرکز، تشدید و نهادینه سازند.

ریکا مک‌کینون^۱ (۲۰۱۲) در کتاب «رضایت شبکه‌ای شده: مبارزه جهانی برای آزادی اینترنت»، با بررسی دقیق تجربه چین، نشان می‌دهد که چگونه دولت‌ها می‌توانند با در اختیار گرفتن کنترل کامل بر زیرساخت فیزیکی و لایه منطقی اینترنت، فضایی از «رضایت شبکه‌ای شده»^۲ ایجاد کنند که در آن، آزادی بیان به شدت محدود شده و شهروندان از ترس پیامدهای نظارتی، به طور داوطلبانه و پیشگیرانه دست به خودسانسوری گسترده می‌زنند.

در ادبیات داخلی نیز برخی پژوهش‌ها با رویکردی حقوقی، به ابعاد چالش‌برانگیز شبکه ملی پرداخته‌اند. انصاری (۱۳۹۹) در مقاله «حق دسترسی به اینترنت؛ مبانی و محتوا» با بررسی ابعاد حقوقی «قطع اینترنت» و «محدودسازی پلتفرم‌ها»، این اقدامات را از منظر نقض حق دسترسی به اطلاعات و آزادی ارتباطات مورد نقد قرار داده است. جلالی و رضایی (۱۴۰۰) نیز در مطالعه تطبیقی خود، به طور خاص به «کاستی‌های قانونی حفاظت از داده‌های شخصی در زیرساخت‌های ملی» پرداخته و هشدار داده‌اند که توسعه شبکه ملی بدون وجود یک قانون جامع، می‌تواند به نقض نظام‌مند حریم خصوصی منجر شود. نقد جریان دوم: این جریان فکری، به درستی خطرات بالقوه تحدید حقوق اساسی و تهدیدات نظارتی را برجسته می‌کند و زنگ هشدار را به صدا درمی‌آورد. با این حال، ضعف اصلی آن در این است که غالباً به ارائه راهکارهای عملی، بومی و اجرایی برای کشورهای که به دلایل راهبردی به دنبال ایجاد توازن میان حاکمیت ملی و حقوق شهروندی هستند، نمی‌پردازد و تحلیل آن غالباً به یک دوگانه ساده‌انگارانه «آزادی مطلق در برابر کنترل مطلق» فروکاسته می‌شود.

1. MacKinnon

2. Networked Consent

چارچوب نظری

برای تحلیل دقیق و چندبعدی موضوع شبکه ملی اطلاعات و اجتناب از تقلیل‌گرایی، این پژوهش از دو چارچوب نظری مکمل و قدرتمند بهره می‌گیرد:

نظریه حاکمیت سایبری^۱

میلتون مولر^۲ (۲۰۱۰) در کتاب مهم خود «شبکه‌ها و دولت‌ها: سیاست جهانی حکمرانی اینترنت»، این ایده رمانتیک که اینترنت ذاتاً یک فضای بدون دولت و رها از حاکمیت ملی است را به چالش می‌کشد. او استدلال می‌کند که اینترنت در واقع به عرصه‌ای برای رقابت شدید مدل‌های مختلف حکمرانی ملی و فراملی تبدیل شده است. مولر نشان می‌دهد که چگونه دولت‌ها با بازتعریف مفهوم کلاسیک «حاکمیت» و بسط آن به «قلمرو سایبری»، به دنبال اعمال کنترل و اعمال صلاحیت بر زیرساخت‌ها، جریان داده‌ها و رفتار کاربران در داخل مرزهای جغرافیایی خود هستند (مولر، ۲۰۱۰: ۵۵). شبکه ملی اطلاعات را می‌توان تجلی عملی و زیرساختی این نظریه در سطح «لایه فیزیکی» دانست؛ اقدامی حاکمیتی برای بازپس‌گیری کنترل بر مسیر داده‌ها، کاهش وابستگی به نقاط تبادل اینترنت خارجی و ایجاد یک «اینترنت ملی» یا «اینترانت» قدرتمند و پایدار.

نظریه لایه‌های کنترل اینترنت^۳

لارا دناردیس (۲۰۱۴) در کتاب «جنگ جهانی برای حکمرانی اینترنت»، مدلی تحلیلی و بسیار کاربردی ارائه می‌دهد که بر اساس آن، کنترل و اعمال قدرت بر اینترنت نه به صورت یکپارچه، بلکه در سه لایه مجزا اما به شدت درهم‌تنیده اعمال می‌شود (دناردیس، ۲۰۱۴: ۹):

۱. لایه فیزیکی: شامل زیرساخت‌های ملموس و عینی مانند کابل‌های فیبر نوری (خشکی و دریا)، مراکز داده، سوئیچ‌ها، مسیریاب‌ها و نقاط تبادل ترافیک. کنترل این لایه به معنای تعیین مسیرهای فیزیکی جریان داده‌هاست.
۲. لایه منطقی: شامل پروتکل‌های نرم‌افزاری که هدایت ترافیک را ممکن می‌سازند، نظیر پروتکل اینترنت، سیستم نام دامنه، آدرس‌دهی و مسیریابی. کنترل این لایه به معنای توانایی هدایت، اولویت‌بندی یا مسدودسازی ترافیک است.
۳. لایه محتوایی: شامل اطلاعات، داده‌ها، تصاویر، ویدئوها و ارتباطاتی که کاربران در بستر شبکه مبادله می‌کنند. این لایه، همان جایی است که آزادی بیان و دسترسی به اطلاعات معنا می‌یابد.

1. Cyber Sovereignty

2. Mueller

3. Layers of Internet Control

شبکه ملی اطلاعات،
آزادی بیان و حریم
خصوصی: تحلیل تطبیقی
زیرساخت‌های ملی
ارتباطات و ارائه الگوی
سیاستی در چارچوب حقوقی
جمهوری اسلامی ایران

نکته کلیدی و حیاتی این نظریه برای پژوهش حاضر آن است که تغییرات و سیاست‌گذاری‌ها در لایه‌های فیزیکی و منطقی (مانند ایجاد یک شبکه ملی اطلاعات با مراکز داده داخلی و DNS بومی)، مستقیماً و به طور اجتناب‌ناپذیری بر لایه محتوایی تأثیر می‌گذارند. به عبارت دیگر، معماری فنی شبکه، خود نوعی سیاست است و تعیین می‌کند که چه نوع ارتباطی و با چه کیفیتی ممکن یا ناممکن است. بنابراین، تحلیل حقوقی شبکه ملی اطلاعات و تأثیر آن بر آزادی بیان، بدون درک این پیوند لایه‌ای و پویایی‌های کنترل در لایه‌های زیرین، ناقص و سطحی خواهد بود.

• مبانی حقوقی آزادی بیان، جریان اطلاعات و حریم خصوصی در نظام حقوقی جمهوری اسلامی ایران

تحلیل شبکه ملی اطلاعات در ایران، ناگزیر از شناخت دقیق و چندلایه مبانی حقوقی ذیل است. برخلاف تصور رایج و تقلیل‌گرایانه که آزادی بیان در ایران را صرفاً محدود به اصل ۲۴ می‌داند، مجموعه‌ای غنی از اصول قانون اساسی و قوانین عادی وجود دارند که چارچوبی جامع، پویا و توأم با حقوق و تکالیف را برای تضمین این حق و تعیین حدود و ثغور آن ترسیم می‌کنند. این بخش به تفصیل به این مبانی می‌پردازد.

۱) اصول مرتبط در قانون اساسی جمهوری اسلامی ایران

اصل سوم (بند ۲ و ۷): بند ۲ این اصل، دولت جمهوری اسلامی ایران را موظف به «بالا بردن سطح آگاهی‌های عمومی در همه زمینه‌ها با استفاده صحیح از مطبوعات و رسانه‌های گروهی و وسایل دیگر» کرده است. این بند یک تکلیف ایجابی و فعال برای دولت ایجاد می‌کند تا بسترهای لازم برای جریان آزاد اطلاعات و ارتقای آگاهی را فراهم آورد. بنابراین، شبکه ملی اطلاعات به عنوان یک پروژه عظیم ملی و دولتی، باید به گونه‌ای طراحی، اجرا و سیاست‌گذاری شود که به تأمین این تکلیف قانونی کمک کند و به بستری برای «استفاده صحیح» از رسانه‌ها تبدیل شود، نه آنکه به مانعی در برابر آن بدل گردد. بند ۷ نیز دولت را موظف به «تأمین آزادی‌های سیاسی و اجتماعی در حدود قانون» کرده است.

اصل نهم: این اصل با عبارتی قاطع و صریح بیان می‌دارد: «در جمهوری اسلامی ایران، آزادی و استقلال و وحدت و تمامیت ارضی کشور از یکدیگر

تفکیک‌ناپذیرند و حفظ آنها وظیفه دولت و آحاد ملت است. هیچ مقامی حق ندارد به نام حفظ استقلال و تمامیت ارضی کشور آزادی‌های مشروع را، هر چند با وضع قوانین و مقررات، سلب کند. این اصل یک پادزهر حقوقی قدرتمند در برابر رویکردهای افراطی امنیتی است. این اصل مبین آن است که حفظ حاکمیت، استقلال و امنیت کشور (که هدف غایی شبکه ملی اطلاعات است) نه تنها با آزادی‌های مشروع (مانند آزادی بیان) در تضاد نیست، بلکه به هیچ‌وجه نمی‌تواند بهانه‌ای برای سلب یا تحدید فراقانونی این آزادی‌ها باشد. این اصل بر توازن، هم‌زیستی و تفکیک‌ناپذیری حاکمیت و آزادی تأکید دارد و هرگونه سیاستی که یکی را فدای دیگری کند، مغایر با روح و نص این اصل خواهد بود. اصل بیست‌و‌چهارم: «نشریات و مطبوعات در بیان مطالب آزادند مگر آنکه مخل به مبانی اسلام یا حقوق عمومی باشد. تفصیل آن را قانون معین می‌کند.» این اصل، چارچوب اصلی و اساسی تحدید آزادی بیان در فضای حقیقی و به تبع آن، فضای مجازی را مشخص می‌کند. دو نکته کلیدی و راهبردی در این اصل وجود دارد که برای تحلیل شبکه ملی اطلاعات حیاتی است:

۱. محدودیت‌ها منحصر و مضیق هستند: قیود آزادی بیان صرفاً به دو مورد «اخلال در مبانی اسلام» و «اخلال در حقوق عمومی» منحصر شده است. این امر به معنای آن است که سایر بهانه‌ها (مانند سلیقه سیاسی، مصلحت‌اندیشی‌های اداری یا رقابت‌های اقتصادی) نمی‌توانند مبنای قانونی برای محدودسازی بیان باشند.

۲. تفصیل محدودیت‌ها صرفاً با «قانون» است: تعیین مصادیق دقیق این دو قید و شیوه‌های برخورد با آنها، صرفاً به «قانون عادی» (مصوب مجلس شورای اسلامی) واگذار شده است. این بدان معناست که هرگونه محدودسازی دسترسی به محتوا، فیلترینگ و بسایت‌ها یا مسدودسازی پلتفرم‌ها در بستر شبکه ملی اطلاعات، باید مستند به قانون مصوب مجلس باشد و از اعمال سلیقه‌ای، بخشنامه‌های غیرشفاف و اقدامات فراقانونی نهادهای اجرایی یا شبه‌قضایی به شدت جلوگیری شود. این اصل، بزرگترین ضمانت اجرایی حقوقی برای آزادی بیان در ایران است.

اصل بیست‌وپنجم: «بازرسی و نرساندن نامه‌ها، ضبط و فاش کردن مکالمات تلفنی، افشای مخابرات تلگرافی و تلکس، سانسور، مخابره نکردن و نرساندن آنها، استراق سمع و هرگونه تجسس ممنوع است مگر به حکم قانون.» این اصل

شبکه ملی اطلاعات،
آزادی بیان و حریم
خصوصی: تحلیل تطبیقی
زیرساخت‌های ملی
ارتباطات و ارائه الگوی
سیاستی در چارچوب حقوقی
جمهوری اسلامی ایران

ارتباط مستقیم و غیرقابل انکاری با «حریم خصوصی» و «حفاظت از داده‌های شخصی» در بستر شبکه ملی اطلاعات دارد. از آنجا که شبکه ملی اطلاعات مستلزم تجمیع، ذخیره‌سازی و مسیریابی داخلی حجم عظیمی از داده‌های ارتباطی و شخصی شهروندان است، رعایت دقیق اصل ۲۵ و جلوگیری از هرگونه دسترسی، نظارت، شنود یا تجسس بدون «حکم قانون» (که آن هم باید از مسیر قضایی و با رعایت تشریفات دادرسی عادلانه باشد)، یک الزام اساسی و غیرقابل چشم‌پوشی است. نبود قانون جامع در این زمینه، به معنای خلأ جدی در صیانت از این اصل است.

اصل یکصد و هفتاد و پنجم: این اصل با تأکید بر «آزادی بیان و نشر افکار در صدا و سیمای جمهوری اسلامی ایران» و پیش‌بینی سازوکار نظارتی مرکب از نمایندگان قوای سه‌گانه (مجریه، مقننه و قضائیه)، مدلی نظارتی چندوجهی، متوازن و غیرمتمرکز را معرفی می‌کند. این مدل می‌تواند و باید به عنوان یک الگوی حقوقی الهام‌بخش برای حکمرانی شبکه ملی اطلاعات نیز مورد توجه قرار گیرد؛ به نحوی که به جای تمرکز مطلق قدرت نظارت و تنظیم‌گری در یک نهاد دولتی خاص، سازوکاری برای نظارت متقابل، چندقابله و پاسخگو پیش‌بینی شود.

۲) قوانین عادی و کاستی‌های قانونی موجود

قانون انتشار و دسترسی آزاد به اطلاعات (مصوب ۱۳۸۸): این قانون مقرر می‌کند که در راستای تحقق اصل ۳ قانون اساسی و با الهام از جنبش جهانی «آزادی اطلاعات» به تصویب رسیده است، حق دسترسی شهروندان به اطلاعات مؤسسات عمومی و دولتی را به رسمیت شناخته و استثنائات آن را صرفاً به موارد محدود و مشخصی مانند «امنیت ملی» و «حقوق خصوصی» منحصر کرده است (انصاری، ۱۳۹۹: ۵۶). شبکه ملی اطلاعات به عنوان بستر اصلی ارائه خدمات دولت الکترونیک، آموزش مجازی، سلامت دیجیتال و دسترسی به اطلاعات عمومی، باید در خدمت تحقق کامل اهداف این قانون باشد. هرگونه سیاستی که به کاهش شفافیت، ایجاد انحصار اطلاعاتی یا محدودیت دسترسی به اطلاعات عمومی بینجامد، ناقض آشکار این قانون خواهد بود.

خلأ قانونی حفاظت از داده‌های شخصی: «لایحه حفاظت از داده‌های شخصی» سال‌هاست که در رفت‌وآمد میان دولت و مجلس شورای اسلامی معطل مانده و به سرانجام نرسیده است. این نقص حقوقی عمیق و خطرناک در شرایطی که شبکه ملی اطلاعات با هدف تجمیع ترافیک داخلی، ارائه

خدمات بومی (پیام‌رسان‌ها، ایمیل، موتور جست‌وجو) و ذخیره‌سازی داده‌های شهروندان بر روی سرورهای داخلی در حال توسعه و پیاده‌سازی است، به مثابه یک تهدید جدی و در حال حاضر بالفعل برای «حریم خصوصی» و «آزادی بیان» شهروندان (موضوع اصول ۲۴ و ۲۵ قانون اساسی) محسوب می‌شود. نبود یک قانون جامع و بازدارنده که حقوق کاربران در قبال داده‌های شخصی‌شان، تعهدات و مسئولیت‌های ارائه‌دهندگان خدمات (اعم از دولتی و خصوصی) و ضمانت‌های اجرایی کیفری و مدنی در صورت نقض حریم خصوصی را به طور شفاف مشخص کند، می‌تواند به ایجاد «فضای ترس» و خودسانسوری گسترده در میان کاربران منجر شده و در نتیجه، آزادی بیان را به طور غیرمستقیم اما عمیقاً تضعیف نماید (کمالی، ۱۳۹۸: ۷۲). تصویب و ابلاغ فوری این لایحه، نه یک انتخاب، بلکه یک پیش‌نیاز ضروری حقوقی و اخلاقی برای راه‌اندازی کامل و ایمن شبکه ملی اطلاعات و جلب اعتماد عمومی است.

• تحلیل تطبیقی شبکه‌های ملی اطلاعات و چالش آزادی بیان

در این بخش، برخلاف تحلیل‌های کلی و انتزاعی از حکمرانی اینترنت، صرفاً به تحلیل شبکه‌های ملی اطلاعات به عنوان زیرساخت‌های فنی و مشخص و تأثیر مستقیم و انضمامی آنها بر جریان اطلاعات، آزادی بیان و حریم خصوصی پرداخته می‌شود. هدف، استخراج درس‌های عینی و مقایسه‌پذیر برای ایران است.

۱) چین: شبکه ملی اطلاعات (سپر تلایی) به مثابه اینترنت بسته و

تحدید کامل آزادی بیان

چین کامل‌ترین، پیشرفته‌ترین و در عین حال بسته‌ترین نمونه از یک شبکه ملی اطلاعات بومی را با نام پروژه «سپر تلایی»^۱ که در سطح جهان به «فایروال بزرگ چین»^۲ معروف است، طراحی و اجرا کرده است. این پروژه که از سال ۱۹۹۸ توسط وزارت امنیت عمومی چین آغاز شد، امروزه یک زیرساخت پیچیده، چندلایه و یکپارچه نظارتی و کنترلی است که بر تمامی دروازه‌های ورود و خروج ترافیک اینترنت بین‌المللی چین تسلط کامل دارد.

ویژگی‌های فنی و حقوقی شبکه ملی چین: ترافیک اینترنت داخلی چین به طور کامل و انحصاری بر روی سرورهای بومی (متعلق به شرکت‌های بزرگ فناوری چینی مانند علی‌بابا، تنسنت، بایدو و وی‌چت) هدایت و پردازش می‌شود. چین با ایجاد یک اینترنت عظیم ملی و خودکفا، وابستگی فنی و راهبردی

1. Golden Shield

2. Great Firewall of China

شبکه ملی اطلاعات،
آزادی بیان و حریم
خصوصی: تحلیل تطبیقی
زیرساخت‌های ملی
ارتباطات و ارائه الگوی
سیاستی در چارچوب حقوقی
جمهوری اسلامی ایران

خود به نقاط تبادل اینترنت بین‌المللی و شبکه‌های توزیع محتوا خارجی را به حداقل مطلق رسانده است (محمدی، ۱۳۹۹: ۸). از منظر حقوقی، قوانینی مانند «مقررات مدیریت سرویس‌های برنامه‌های صوتی و تصویری اینترنت» (که به دولت اختیار کامل برای نظارت و سانسور محتوای ویدئویی را می‌دهد)، الزام به «احراز هویت با نام واقعی» برای ثبت‌نام و فعالیت در تمامی سرویس‌های آنلاین (از شبکه‌های اجتماعی گرفته تا بازی‌های رایانه‌ای)، و «قانون امنیت سایبری» مصوب ۲۰۱۷، چارچوب حقوقی مستحکم و فراگیری را برای این کنترل متمرکز فراهم می‌کنند (سعیدی، ۱۴۰۱: ۳۹).

تأثیر مستقیم بر آزادی بیان: این شبکه صرفاً یک ابزار فنی برای افزایش سرعت یا کاهش هزینه‌های ترافیک نیست، بلکه یک مکانیسم سانسور و نظارت پیشگیرانه و فراگیر است. با قطع ارتباط انتخابی با اینترنت جهانی و مسدودسازی کامل و دائمی پلتفرم‌های اصلی خارجی (مانند گوگل، فیس‌بوک، توئیتر، یوتیوب، واتس‌اپ، اینستاگرام و تلگرام)، تنوع منابع اطلاعاتی و امکان دسترسی به رسانه‌های آزاد و بین‌المللی برای شهروندان چینی به صفر مطلق رسیده است. در این مدل، «آزادی بیان» در چارچوب شبکه ملی، به آزادی مصرف محتوای تولیدشده و تأییدشده در داخل اکوسیستم بسته و به شدت کنترل‌شده چین تقلیل یافته است. اگرچه کاربران چینی می‌توانند در پلتفرم‌های داخلی مانند ویبو^۱ یا وی‌چت^۲ اظهار نظر کنند، اما این فضا تحت نظارت شدید و لحظه‌ای الگوریتم‌های هوش مصنوعی و ارتش عظیمی از سانسورچیان انسانی قرار دارد و هرگونه محتوای منتقدانه نسبت به حزب حاکم، سیاست‌های دولت، نقض حقوق بشر یا مسائل حساس تاریخی و قومی به سرعت حذف و حساب کاربر مسدود می‌شود. (مک‌کینون، ۲۰۱۲: ۱۰۳)

درس سیاستی برای ایران: تجربه چین به وضوح و بدون هیچ ابهامی نشان می‌دهد که تبدیل شبکه ملی اطلاعات به یک اینترنت بسته و تحت کنترل مطلق حاکمیت، به قیمت از دست رفتن کامل تبادل آزاد اطلاعات با جهان خارج تمام می‌شود و تحدید شدید و نظام‌مند آزادی بیان، و شکل‌گیری یک جامعه بسته اطلاعاتی در پی دارد. برای جمهوری اسلامی ایران که در قانون اساسی خود بر آزادی مطبوعات، آزادی بیان و جریان آزاد اطلاعات (با قیود قانونی مشخص) تأکید دارد، این مدل نه تنها مطلوب نیست، بلکه با اصول

1. Weibo

2. WeChat

آشکار قانون اساسی در تضاد آشکار است. شبکه ملی اطلاعات ایران باید به عنوان مکمل و تقویت‌کننده دسترسی به اینترنت جهانی عمل کند، نه جایگزین مسدودکننده و حذف‌کننده آن.

۲) روسیه: شبکه ملی اینترنت^۱ و تهدید قطع کامل ارتباط با جهان

روسیه با تصویب «قانون حاکمیت اینترنت روسیه»^۲ که به «قانون اینترنت مستقل» نیز معروف است، در سال ۲۰۱۹، گام بلند و جسورانه‌ای در راستای ایجاد یک شبکه ملی اطلاعات مستقل و مقاوم در برابر فشارهای خارجی برداشت. این مدل از بسیاری جهات به اهداف اعلام‌شده برای شبکه ملی اطلاعات ایران شباهت دارد.

ویژگی‌های فنی و حقوقی شبکه ملی روسیه: هدف اصلی این قانون، ایجاد زیرساخت فنی و حقوقی لازم است تا در صورت وقوع تهدیدات خارجی، حملات سایبری گسترده، یا اعمال تحریم‌های ارتباطی از سوی غرب، اینترنت روسیه بتواند به‌طور کامل از شبکه جهانی جدا شده و به صورت خودگردان و پایدار به کار خود ادامه دهد. برای این منظور، روسیه ملزم به ایجاد «سیستم نام دامنه ملی» توسعه «مراکز تبادل ترافیک داخلی» و نصب اجباری تجهیزات «بازرسی عمیق بسته‌ها» بر روی شبکه تمامی ارائه‌دهندگان خدمات اینترنت شده است. قانونگذار روسی استدلال می‌کند که این اقدام برای حفاظت از شهروندان در برابر نفوذ اطلاعاتی خارجی، تضمین پایداری شبکه در برابر حملات سایبری و حفظ امنیت ملی ضروری است. (سولداتوف^۳ و بوروگان^۴، ۲۰۲۰: ۹۰)

تأثیر مستقیم بر آزادی بیان: آزمایش‌های موفقیت‌آمیز و دوره‌ای «قطع ارتباط» که توسط نهادهای نظارتی روسیه در سال‌های اخیر انجام شده، نشان داد که زیرساخت فنی ایجادشده کاملاً قابلیت خاموشی کامل و کنترل‌شده اینترنت بین‌الملل در این کشور پهناور را دارد. چنین اقدامی، نه تنها دسترسی شهروندان روس به رسانه‌های مستقل داخلی و بین‌المللی را قطع می‌کند، بلکه ارتباطات علمی، دانشگاهی، تجاری و اقتصادی با جهان خارج را نیز به طور کامل متوقف می‌سازد. این امر، نقض آشکار و فاحش اصل آزادی دریافت و انتشار اطلاعات (مندرج در ماده ۱۹ اعلامیه جهانی حقوق بشر) است. حتی در حالت عادی (بدون قطع کامل)، الزام شرکت‌های فناوری خارجی به ذخیره داده‌های کاربران در داخل خاک روسیه و همکاری اجباری با سرویس‌های امنیتی (که

1. Runet
2. Sovereign Internet Law

3. Soldatov
4. Borogan

شبکه ملی اطلاعات،
آزادی بیان و حریم
خصوصی: تحلیل تطبیقی
زیرساخت‌های ملی
ارتباطات و ارائه الگوی
سیاستی در چارچوب حقوقی
جمهوری اسلامی ایران

منجر به مسدودسازی گسترده و ناموفق پیام‌رسان تلگرام در سال ۲۰۱۸ شد)، فضای آزادی بیان را به شدت محدود کرده و محیط کسب‌وکار دیجیتال را با نبود قطعیت و ریسک بالا مواجه ساخته است. (سولدتوف و بوروگان، ۲۰۲۰: ۹۲)

درس سیاستی برای ایران: تجربه روسیه نشان می‌دهد که وجود اختیار قانونی و توانمندی فنی برای قطع کامل اینترنت بین‌الملل، حتی اگر به ندرت مورد استفاده قرار گیرد، خود به عنوان یک تهدید بالقوه دائمی علیه آزادی بیان و حق دسترسی به اطلاعات عمل کرده و فضای روانی کسب‌وکارهای دیجیتال، سرمایه‌گذاران و کاربران عادی را با ترس و بی‌اعتمادی عمیق مواجه می‌سازد. برای ایران، شفافیت کامل در پروتکل‌های مدیریت بحران شبکه، تضمین قضایی مستقل برای جلوگیری از قطع خودسرانه یا فراقانونی دسترسی به اینترنت جهانی (مستند به اصل ۹ قانون اساسی) و اطلاع‌رسانی پیشینی و شفاف به مردم در مواقع ضروری، یک ضرورت اجتناب‌ناپذیر برای حفظ حداقلی از اعتماد عمومی است.

۳) اتحادیه اروپا و فرانسه: حاکمیت داده‌محور و صیانت از حقوق دیجیتال

رویکرد اتحادیه اروپا به طور عام، و فرانسه به طور خاص، نسبت به چین و روسیه تفاوت‌های بنیادینی دارد. اروپا به دنبال ایجاد یک اینترنت موازی یا مسدودسازی کامل پلتفرم‌های خارجی نیست، بلکه هدف اصلی آن «حاکمیت دیجیتال» از طریق «صیانت از داده‌های شهروندان» و «تضمین رقابت عادلانه» در برابر غول‌های فناوری آمریکایی و چینی است.

ویژگی‌های فنی و حقوقی: در سطح کلان، اتحادیه اروپا پروژه «گایا-ایکس»^۱ را برای ایجاد یک زیرساخت ابری و شبکه‌ای امن، مستقل و مبتنی بر ارزش‌های اروپایی (شفافیت، قابلیت حمل داده‌ها و حفاظت از حریم خصوصی) راه‌اندازی کرده است. این پروژه به دنبال کاهش وابستگی فنی به سرویس‌های ابری آمریکایی (مانند آمازون، مایکروسافت و گوگل) است، اما بدون قطع ارتباط با اینترنت جهانی. همزمان، «مقررات عمومی حفاظت از داده‌ها»^۲ که از سال ۲۰۱۸ لازم‌الاجرا شده، یک چارچوب حقوقی بسیار سخت‌گیرانه و قدرتمند برای حفاظت از داده‌های شخصی شهروندان اروپایی ایجاد کرده و هرگونه پردازش و انتقال داده‌ها بدون رضایت صریح کاربران را با جرایم سنگین (تا ۴ درصد از گردش مالی سالانه شرکت) مواجه می‌سازد. در فرانسه نیز قوانینی مانند قانون

1. Gaia-X

2. GDPR

بهبود امنیت داخلی (که به دولت اجازه فیلترینگ وبسایت‌ها بدون حکم قضایی را می‌دهد) با انتقادات گسترده فعالان حقوق دیجیتال مواجه شده، اما همزمان قوانین قدرتمندی برای حمایت از «بی‌طرفی شبکه» و جلوگیری از تبعیض در ترافیک اینترنت وجود دارد. (سعیدی، ۱۴۰۱: ۱۱۱)

تأثیر مستقیم بر آزادی بیان: مدل اروپایی نشان می‌دهد که می‌توان زیرساخت‌های بومی و ملی را نه برای «مسدودسازی محتوا»، بلکه برای «اجرای مؤثرتر قوانین صیانت از حقوق شهروندی» توسعه داد. گایا-ایکس و مقررات عمومی حفاظت از داده‌ها به دنبال توانمندسازی کاربران و کنترل آنها بر داده‌های شخصی‌شان هستند، نه محدودسازی دسترسی آنها به اطلاعات. این مدل، آزادی بیان را از طریق افزایش امنیت روانی کاربران (با تضمین اینکه داده‌هایشان در بستری امن و تحت قوانین سخت‌گیرانه حریم خصوصی نگهداری می‌شود) تقویت می‌کند، نه از طریق تحدید دسترسی.

درس سیاستی برای ایران: مهم‌ترین درس مدل اروپایی برای ایران، اولویت‌بندی تصویب و اجرای یک قانون جامع حفاظت از داده‌های شخصی هم‌تراز با استانداردهای جهانی است؛ پیش از آنکه هرگونه اقدام برای تشویق یا اجبار شهروندان به مهاجرت به پلتفرم‌های بومی پدید آید. همچنین ایجاد یک نهاد رگولاتوری مستقل و قدرتمند برای نظارت بر اجرای این قانون و تضمین رقابت منصفانه در لایه خدمات شبکه ملی، یک الزام حیاتی است.

۴) ایالات متحده: چرخش از بی‌طرفی شبکه به ملی‌گرایی زیرساختی و امنیتی

ایالات متحده که به طور سنتی خود را پرچمدار «جریان آزاد اطلاعات» و مدافع اصل «بی‌طرفی شبکه» معرفی می‌کرد (لسیگ^۱، ۲۰۰۶: ۱۵۲)، در سال‌های اخیر شاهد یک چرخش راهبردی قابل توجه به سمت «ملی‌گرایی زیرساختی» و اعمال محدودیت‌های امنیت‌محور بر پلتفرم‌ها و تجهیزات خارجی بوده است. (کار^۲، ۲۰۱۶: ۵۸)

ویژگی‌های فنی و حقوقی: ابتکار «شبکه پاک» که در دوران ریاست‌جمهوری ترامپ مطرح شد، به دنبال حذف تجهیزات و نرم‌افزارهای شرکت‌های چینی (به‌ویژه هواوی و زدتی‌ای^۳) از زیرساخت‌های ارتباطی حیاتی آمریکا و متحدانش

1. Lessig
2. Carr
3. ZTE

شبکه ملی اطلاعات،
آزادی بیان و حریم
خصوصی: تحلیل تطبیقی
زیرساخت‌های ملی
ارتباطات و ارائه الگوی
سیاستی در چارچوب حقوقی
جمهوری اسلامی ایران

بود. همچنین، تلاش‌های قانونی و اجرایی برای محدودسازی یا ممنوعیت کامل پلتفرم‌های چینی مانند تیک‌تاک^۱ و وی‌چت به بهانه «تهدید امنیت ملی» و «جاسوسی سایبری»، نمونه‌های بارز این چرخش سیاستی هستند. این اقدامات نشان داد که حتی در نظام‌های لیبرال دموکراسی غربی نیز، دغدغه‌های امنیت ملی و حفظ سلطه فناورانه می‌تواند بر اصول بنیادین بازار آزاد و بی‌طرفی شبکه غلبه کند.

تأثیر مستقیم بر آزادی بیان: اگرچه این محدودیت‌ها در آمریکا بر مبنای امنیت ملی توجیه می‌شوند و با چالش‌های قضایی جدی (بر اساس متمم اول قانون اساسی) مواجه هستند، اما در عمل به محدود شدن حق انتخاب کاربران آمریکایی و تحدید دسترسی آنها به طیف متنوعی از پلتفرم‌های ارتباطی منجر شده است. این چرخش، درسی مهم به همراه دارد؛ که هیچ کشوری، حتی لیبرال‌ترین دموکراسی‌ها، از حق خود برای اعمال حاکمیت بر زیرساخت‌های حیاتی و جریان داده‌ها در مواقع ضروری چشم‌پوشی نمی‌کنند. با این حال، تفاوت کلیدی در شفافیت فرآیندها، وجود نهادهای نظارتی مستقل (مانند کنگره و دادگاه‌های فدرال) و امکان به چالش کشیدن قضایی تصمیمات اجرایی است.

1. TikTok

پژوهش‌های ارتباطی،
سال سی و دوم،
شماره ۴ (پیاپی ۱۲۴)،
زمستان ۱۴۰۴

جدول ۱: مقایسه تطبیقی زیرساخت‌های ملی اطلاعات در کشورهای منتخب و تأثیر آن
بر آزادی بیان و حریم خصوصی

ایالات متحده (مدل امنیت ملی گزینشی)	اتحادیه اروپا / فرانسه (مدل حاکمیت داده‌محور)	مدل روسیه (RuNet)	چین (مدل سپر طلایی)	معیار مقایسه
مقابله با تهدیدات سخت‌افزاری و نرم‌افزاری خارجی	صیانت از داده‌های شخصی و تقویت حاکمیت دیجیتال	استقلال زیرساختی و امکان مدیریت ارتباطات در شرایط بحران	کنترل متمرکز جریان اطلاعات و ایجاد ساختار شبکه داخلی	هدف اصلی زیرساخت ملی
ابتکار Clean Network، مقررات محدودسازی برخی پلتفرم‌ها	مقررات عمومی حفاظت از داده‌ها، پروژه GaiaX	قانون اینترنت حاکمیتی (۲۰۱۹)، DNS ملی، سامانه‌های پایش ترافیک	سامانه فیلترینگ متمرکز، DNS بومی، الزامات احراز هویت	ابزار کلیدی فنی-حقوقی
اتصال کامل همراه با محدودیت‌های مبتنی بر ملاحظات امنیتی	اتصال کامل با استانداردهای سخت‌گیرانه امنیت و حفاظت داده	اتصال به اینترنت جهانی همراه با امکان مدیریت یا قطع ارتباط در شرایط خاص	ساختار شبکه داخلی با محدودیت گسترده بر پلتفرم‌های خارجی	نسبت با اینترنت جهانی
اعمال محدودیت‌های موردی با امکان بررسی قضایی	تمرکز بر تنظیم‌گری داده بدون مسدودسازی فراگیر محتوا	ایجاد چارچوب‌های کنترلی در بستر ملی	اعمال محدودیت‌های گسترده بر جریان محتوا	تأثیر بر آزادی بیان
تنظیم‌گری ترکیبی بازار و امنیت ملی	حفاظت سخت‌گیرانه از داده‌های شخصی به‌عنوان حق بنیادین	الزام به نگهداری داده در داخل کشور	دسترسی گسترده حاکمیتی به داده‌ها	رویکرد به حریم خصوصی
تعریف چارچوب شفاف برای تهدیدات امنیتی	تقدم قانون حفاظت از داده بر توسعه خدمات	تأکید بر استقلال زیرساختی	تمرکز بر مدیریت متمرکز زیرساخت	ملاحظات سیاستی

شبکه ملی اطلاعات،
آزادی بیان و حریم
خصوصی: تحلیل تطبیقی
زیرساخت‌های ملی
ارتباطات و ارائه الگوی
سیاستی در چارچوب حقوقی
جمهوری اسلامی ایران

• تحلیل انتقادی شبکه ملی اطلاعات ایران بر اساس اسناد بالادستی (با تمرکز بر سند تبیین الزامات ۱۳۹۵)

شبکه ملی اطلاعات در ایران نه صرفاً یک پروژه فنی و عمرانی، بلکه یک راهبرد حاکمیتی کلان است که چارچوب حقوقی و سیاستی آن در دو سند اصلی مصوب شورای عالی فضای مجازی تعریف شده است. تحلیل انتقادی این اسناد از منظر حقوق شهروندی، آزادی بیان و حریم خصوصی، نقاط قوت و ضعف جدی را آشکار می‌سازد.

۱) تحلیل سند «طرح کلان و معماری شبکه ملی اطلاعات» (مصوب ۱۳۹۲)

این سند که نخستین سند راهبردی و نقشه راه فنی پروژه است، عمدتاً و تقریباً به طور انحصاری بر اهداف فنی، زیرساختی، معماری شبکه و الزامات امنیتی متمرکز است. تأکید اصلی سند بر مفاهیمی چون «کاهش وابستگی به اینترنت جهانی»، «مدیریت ترافیک داخلی»، «افزایش پایداری و تاب‌آوری شبکه» و «ارائه خدمات الکترونیک پایدار» است (مرکز ملی فضای مجازی، ۱۳۹۲: ۲). هرچند این اهداف به خودی خود ضروری، مشروع و از الزامات یک کشور مستقل هستند، اما غیبت کامل و مطلق هرگونه اشاره به حقوق شهروندی، آزادی بیان، حق دسترسی به اطلاعات و الزامات قانونی مرتبط با حریم خصوصی در این سند، نقطه ضعف اساسی و بنیادین آن است. این سکوت معنادار، زمینه را برای تفاسیر امنیتی و محدودیت‌محور از شبکه ملی اطلاعات در مراحل اجرایی فراهم کرده و به طور طبیعی نگرانی‌های گسترده فعالان حقوق دیجیتال، جامعه مدنی و کاربران را دامن زده است.

۲) تحلیل تفصیلی و انتقادی «سند تبیین الزامات شبکه ملی اطلاعات»

(مصوب ۱۳۹۵)

این سند که برای رفع ابهامات سند اول به تصویب رسید، جزئیات بیشتری در مورد خدمات، کارکردها و لایه‌های مختلف شبکه ملی اطلاعات (شامل زیرساخت، خدمات پایه کاربردی و محتوا) ارائه می‌دهد. با این حال، این سند نیز از چند خلأ و ابهام حقوقی مهم و سرنوشت‌ساز رنج می‌برد:

الف) ابهام راهبردی در نسبت شبکه با اینترنت جهانی (چالش اصلی آزادی بیان): «سند تبیین الزامات» به صراحت و با زبانی حقوقی مشخص نمی‌کند که مرز دقیق میان «مدیریت و بهینه‌سازی ترافیک داخلی» (که یک اقدام

فنی و مشروع است) و «مسدودسازی، فیلترینگ و یا قطع کامل دسترسی به اینترنت بین‌الملل» (که یک اقدام سیاسی-امنیتی با پیامدهای سنگین حقوق بشری است) کجاست (شورای عالی فضای مجازی، ۱۳۹۵: ۵). این ابهام عمدی یا سهوی، منشأ اصلی نگرانی از تبدیل تدریجی شبکه ملی اطلاعات به یک اینترنت بسته و محدود به سبک چین یا روسیه است. برای رفع این نگرانی بنیادین، لازم است در بازنگری اسناد بالادستی یا در قالب یک قانون مصوب مجلس، به طور شفاف و غیرقابل تفسیر تصریح شود که «شبکه ملی اطلاعات به عنوان یک زیرساخت ملی، به معنای قطع یا محدودسازی غیرقانونی دسترسی شهروندان به شبکه جهانی اینترنت نیست و کاربران همواره از حق انتخاب آگاهانه میان خدمات باکیفیت داخلی و بین‌المللی برخوردار خواهند بود. هرگونه تحدید دسترسی صرفاً بر اساس حکم قضایی و در چارچوب قوانین مصوب مجلس امکان‌پذیر است.»

ب) وضعیت خطرناک نبود حفاظت کامل از داده‌های شخصی و حریم خصوصی: با وجود آنکه یکی از اهداف و نتایج مستقیم راه‌اندازی شبکه ملی اطلاعات، جمع‌گسترده داده‌ها، ترافیک و ارتباطات شهروندان بر روی سرورها و زیرساخت‌های داخلی است، این سند به طرز شگفت‌آوری فاقد هرگونه الزام، استاندارد یا چارچوب حقوقی مشخص برای تضمین امنیت داده‌های شخصی، صیانت از حریم خصوصی کاربران و تعیین تکالیف نهادهای متولی در قبال این داده‌هاست. همانطور که پیشتر اشاره شد، توقف چندین‌ساله لایحه حفاظت از داده‌های شخصی در پیچ‌وخم‌های بوروکراتیک، این خلأ حقوقی را به یک بحران اعتماد تمام‌عیار تبدیل کرده است (کمالی، ۱۳۹۸: ۷۳). ادامه روند توسعه و تکمیل شبکه ملی اطلاعات و تشویق یا اجبار کاربران به استفاده از خدمات پایه بومی (پیام‌رسان‌ها و ایمیل داخلی) بدون وجود یک قانون جامع، شفاف و ضمانت‌دار در این حوزه، به منزله نقض بالقوه و نظام‌مند اصل ۲۵ قانون اساسی و به خطر انداختن امنیت روانی و اطلاعاتی شهروندان است.

ج) خطر ذاتی ایجاد انحصار و تضعیف رقابت سالم در اقتصاد دیجیتال: سند تبیین الزامات به درستی بر ضرورت حمایت از «پیام‌رسان‌های داخلی»، «موتورهای جست‌وجوی بومی» و «شبکه‌های اجتماعی ملی» تأکید دارد. اما در این حمایت، سازوکار شفاف، عادلانه و رقابتی برای تضمین «رقابت آزاد و منصفانه» و جلوگیری از شکل‌گیری «انحصارهای دولتی یا شبه‌دولتی» (که به رانت‌های اطلاعاتی و

شبکه ملی اطلاعات، آزادی بیان و حریم خصوصی: تحلیل تطبیقی زیرساخت‌های ملی ارتباطات و ارائه الگوی سیاستی در چارچوب حقوقی جمهوری اسلامی ایران

اقتصادی منجر می‌شود) پیش‌بینی نکرده است (شورای عالی فضای مجازی، ۱۳۹۵: ۱۲). این رویکرد می‌تواند در عمل به حذف تدریجی بازیگران کوچک و مستقل، کاهش تنوع و تکثر محتوایی، و محدودسازی شدید «حق انتخاب» شهروندان منجر شود و در نتیجه، آزادی بیان را از طریق کنترل انحصاری بر بسترهای اصلی انتشار محتوا و شکل‌دهی به افکار عمومی تحدید کند.

جدول ۲: خلأها و چالش‌های حقوقی در اسناد مصوب شورای عالی فضای مجازی (سند تعریف ۱۳۹۲ و سند تبیین الزامات ۱۳۹۵)

پیامدهای احتمالی اجرایی	چالش‌ها و ابهامات حقوقی	مفاد و اهداف مطرح در اسناد	حوزه کارکردی شبکه ملی
امکان محدودسازی گسترده دسترسی در شرایط خاص	ابهام در حدود مدیریت ترافیک و شرایط مدیریت بحران	کاهش وابستگی به اینترنت جهانی و مدیریت ترافیک داخلی	زیرساخت و پایداری شبکه
کاهش اعتماد عمومی در صورت نبود تضمین حقوق کاربران	نبود قانون جامع حفاظت از داده و شفافیت الگوریتمی	حمایت از پیام‌رسان‌ها و خدمات بومی	خدمات پایه کاربردی
احتمال تمرکز بازار و کاهش تنوع خدمات	نبود سازوکار شفاف رقابت و ضدانحصار	توسعه کسب‌وکارهای داخلی و تقویت محتوای بومی	اقتصاد دیجیتال و محتوا
چالش در شفافیت تصمیم‌گیری و پاسخگویی	فقدان نهاد رگولاتوری مستقل و چندذی‌نفعی	واگذاری تنظیم‌گری به نهادهای ملی ذی‌ربط	نظارت و تنظیم‌گری

۳) تحلیل حقوقی تبدیل شبکه ملی اطلاعات به اینترنت ملی در شرایط جنگی (حکم ثانویه و وضعیت اضطراری)

یکی از سناریوهای محتمل و راهبردی در طراحی شبکه ملی اطلاعات، تبدیل این شبکه به یک «اینترنت ملی» در شرایط جنگی و بحران‌های حاد امنیتی است. این اقدام که در ادبیات حقوقی زیر مفهوم «وضعیت اضطراری ۱» تحلیل می‌شود، به معنای قطع موقت ارتباط با شبکه جهانی اینترنت و اتکای کامل به زیرساخت بومی برای حفظ امنیت ملی است. در رهنمودهای نوین نظامی و نظریه‌های روابط بین‌الملل، فضای سایبری به عنوان «پنجمین عرصه نبرد» شناخته می‌شود و زیرساخت‌های ارتباطی به ابزاری دوگانه در منازعات

1. State of Emergency

ژئوپلیتیک تبدیل شده‌اند (کار، ۲۰۱۶: ۵۸). در چنین شرایطی، قطع هدفمند اینترنت بین‌الملل اقدامی ناگزیر برای خنثی‌سازی عملیات روانی دشمن، جلوگیری از نفوذ سایبری به زیرساخت‌های حیاتی و حفظ یکپارچگی فرماندهی و کنترل محسوب می‌شود. (دناردیس، ۲۰۱۴: ۴۱)

از منظر حقوق اساسی جمهوری اسلامی ایران، اصل ۷۹ قانون اساسی تصریح می‌کند که «در حالت جنگ و شرایط اضطراری نظیر آن، دولت حق دارد با تصویب مجلس شورای اسلامی به‌طور موقت محدودیت‌های ضروری را برقرار نماید». این محدودیت موقت و منوط به نظارت پارلمانی، ماهیتاً با محدودیت دائمی، سلیقه‌ای و فراقانونی تفاوت بنیادین دارد (زاهدی، ۱۴۰۰: ۱۰۱). در فقه اسلامی نیز این اقدام تحت قاعده «حکم ثانویه» توجیه می‌شود؛ بدین معنا که در شرایط عادی، آزادی بیان و دسترسی آزاد به اطلاعات «حکم اولیه» است، اما در شرایط جنگ و تهدید موجودیت کشور، «حفظ نظام» و «امنیت ملی» به عنوان احکام ثانویه، مقدم بر آن می‌شوند. در حقوق بین‌الملل نیز ماده ۴ میثاق بین‌المللی حقوق مدنی و سیاسی^۱ به دولت‌های عضو اجازه می‌دهد در شرایط اضطراری فوق‌العاده که «حیات ملت را تهدید می‌کند»، برخی از تعهدات حقوق بشری خود از جمله آزادی بیان (ماده ۱۹) را به‌طور موقت تعلیق کنند، مشروط بر آنکه این تعلیق «به میزانی که ضرورت آن ایجاب می‌کند» محدود بوده و با سایر تعهدات بین‌المللی مغایرت نداشته باشد. (دفتر کمیساری عالی حقوق بشر، ۲۰۲۰: ۱۲)

تجربه کشورهای دیگر نیز مؤید این رویکرد است. روسیه با تصویب «قانون اینترنت حاکمیتی» در سال ۲۰۱۹، زیرساخت فنی و حقوقی لازم را برای قطع ارتباط اینترنت ملی خود از شبکه جهانی در مواقع تهدید ایجاد کرده و این اقدام را در راستای حفظ «حاکمیت دیجیتال» خود توجیه نموده است (سولداتوف و بوروگان، ۲۰۲۰: ۹۰). بنابراین، تبدیل شبکه ملی اطلاعات به اینترنت ملی در زمان جنگ، نه یک ناقض فراقانونی آزادی بیان، بلکه اعمال مشروع «حق حاکمیت» در شرایط استثنایی و اضطراری است. آنچه این اقدام را از تحدید خودسرانه و دائمی آزادی بیان متمایز می‌سازد، چهار ویژگی اساسی آن است: (۱) موقتی و محدود بودن به دوره بحران؛ (۲) مشروط به تصویب مرجع قانون‌گذار (مجلس شورای اسلامی)؛ (۳) تناسب با تهدید؛ و (۴) بازگشت فوری و بدون قید و

1. ICCPR

شبکه ملی اطلاعات،
آزادی بیان و حریم
خصوصی: تحلیل تطبیقی
زیرساخت‌های ملی
ارتباطات و ارائه الگوی
سیاستی در چارچوب حقوقی
جمهوری اسلامی ایران

شرط به وضعیت عادی (باز بودن اینترنت جهانی) پس از رفع شرایط اضطراری. به عبارت دیگر، این اقدام مصداق «استثنای ضروری» در چارچوب قانون اساسی است، نه «قاعده دائمی» که به رویه عادی حکمرانی تبدیل شود.

بحث و نتیجه‌گیری

پژوهش حاضر با هدف تحلیل رابطه پیچیده و چندبعدی میان شبکه ملی اطلاعات و حقوق بنیادین آزادی بیان، جریان اطلاعات و حریم خصوصی در نظام حقوقی جمهوری اسلامی ایران و با بهره‌گیری از یک چارچوب تحلیلی تطبیقی-حقوقی انجام شد. یافته‌های تحقیق به روشنی نشان می‌دهد که موفقیت و مقبولیت شبکه ملی اطلاعات به عنوان یک «پروژه ملی»، نه صرفاً در گرو پیشرفت فنی، توسعه فیبر نوری و پوشش زیرساختی، بلکه در گرو توانایی آن برای جلب اعتماد عمومی و ایجاد یک «قرارداد اجتماعی دیجیتال» جدید میان حاکمیت و شهروندان است.

تحلیل تطبیقی تجارب چین و روسیه به عنوان یک هشدار جدی عمل می‌کند: شبکه‌های ملی اطلاعات، اگر در خلأ حقوقی و بدون نظارت مستقل توسعه یابند، به سرعت به ابزاری برای انزوای دیجیتال، سانسور نظام‌مند، نقض گسترده حریم خصوصی و تحدید کامل آزادی بیان تبدیل می‌شوند. تجربه چین نشان داد که تبدیل شبکه ملی به یک اینترنت بسته، به قیمت از دست رفتن کامل تنوع منابع اطلاعاتی و تحدید مطلق آزادی بیان تمام می‌شود. تجربه روسیه نیز ثابت کرد که وجود اختیار فنی برای قطع اینترنت بین‌الملل، حتی اگر به ندرت استفاده شود، خود به عنوان یک تهدید بالقوه دائمی علیه آزادی بیان عمل کرده و فضای روانی کسب‌وکارها و کاربران را با ترس و بی‌اعتمادی عمیق مواجه می‌سازد.

در مقابل، تجربه اتحادیه اروپا نشان می‌دهد که می‌توان زیرساخت‌های بومی را به گونه‌ای طراحی و قانون‌گذاری کرد که در خدمت «توانمندسازی حقوقی شهروندان» و «صیانت از داده‌های شخصی» باشد و از این رهگذر، به تقویت آزادی بیان و شکوفایی اقتصاد دیجیتال یاری رساند. مدل اروپایی مبتنی بر مقررات عمومی حفاظت از داده‌ها و پروژه گایا-یکس، اثبات می‌کند که «حاکمیت دیجیتال» لزوماً به معنای «انسداد و سانسور» نیست، بلکه می‌تواند از مسیر «شفافیت، قانون‌مداری و صیانت از حقوق کاربران» محقق شود.

در خصوص سناریوی تبدیل شبکه ملی اطلاعات به اینترنت ملی در شرایط جنگی و بحران‌های حاد امنیتی، این پژوهش با استناد به اصل ۷۹ قانون اساسی و قاعده فقهی «حکم ثانویه»، این اقدام را اعمال مشروع «حق حاکمیت» در شرایط استثنایی و اضطراری ارزیابی می‌کند، نه یک نقض‌کننده فراقانونی آزادی بیان. آنچه این اقدام را از تحدید خودسرانه و دائمی آزادی بیان متمایز می‌سازد، چهار ویژگی اساسی آن است: ۱) موقتی و محدود بودن به دوره بحران؛ ۲) منوط بودن به تصویب مرجع قانون‌گذار (مجلس شورای اسلامی)؛ ۳) رعایت اصل تناسب با تهدید و ۴) بازگشت فوری و بدون قید و شرط به وضعیت عادی پس از رفع شرایط اضطراری. به عبارت دیگر، این اقدام مصداق «استثنای ضروری» در چارچوب قانون اساسی است، نه «قاعده دائمی» که به رویه عادی حکمرانی تبدیل شود. آنچه در این میان حیاتی است، شفافیت در اعلام شرایط اضطراری و تضمین بازگشت به وضعیت عادی است تا از سوءاستفاده از این اختیار استثنایی برای تحدید دائمی حقوق شهروندی جلوگیری شود.

برای جمهوری اسلامی ایران که یک نظام حقوقی غنی و متوازن با تأکید همزمان بر حاکمیت ملی و حقوق ملت دارد (به‌ویژه در اصول ۳، ۹، ۲۴، ۲۵ و ۱۷۵ قانون اساسی)، مسیر پیش رو باید هوشمندانه و متفاوت از دوگانه‌های رایج «آزادی مطلق در برابر کنترل مطلق» ترسیم شود. گذار از «مدیریت سلبی» (مبتنی بر فیلترینگ، مسدودسازی و تحدید دسترسی) به «مدیریت ایجابی و حقوق‌محور» (مبتنی بر تسهیل دسترسی آزاد به اطلاعات، حمایت رقابتی از تولید محتوای متنوع و بومی، صیانت از حریم خصوصی و شفافیت کامل)، تنها راهکاری است که می‌تواند هم اهداف راهبردی کشور در زمینه استقلال دیجیتال و امنیت ملی را تأمین کند و هم حقوق بنیادین شهروندان را پاس بدارد و اعتماد از دست رفته را بازسازی نماید.

در نهایت، موفقیت شبکه ملی اطلاعات نه در تعداد کیلومترهای فیبر نوری کشیده‌شده، که در عمق اعتماد و مشارکت آگاهانه شهروندانی سنجیده می‌شود که آن را بستری امن، آزاد، شفاف و عادلانه برای زیست دیجیتال خود می‌یابند. این موضوع مهم جز از طریق امضای یک «قرارداد اجتماعی دیجیتال» جدید میان حاکمیت و ملت، که در آن حاکمیت متعهد به صیانت از حقوق دیجیتال شهروندان در ازای مشارکت آنان در توسعه زیرساخت ملی باشد، محقق نخواهد شد.

شبکه ملی اطلاعات،
آزادی بیان و حریم
خصوصی: تحلیل تطبیقی
زیرساخت‌های ملی
ارتباطات و ارائه الگوی
سیاستی در چارچوب حقوقی
جمهوری اسلامی ایران

نوآوری و محدودیت پژوهش

با کنار هم قرار دادن این دو جریان فکری، شکاف پژوهشی به وضوح نمایان می‌شود: از یک سو، ادبیات داخلی بیشتر در جریان اول (فنی-اقتصادی-امنیتی) در انحصار مانده و فاقد تحلیل عمیق حقوقی و تطبیقی با تمرکز بر چالش آزادی بیان است. از سوی دیگر، ادبیات انتقادی بین‌المللی اگرچه هشداردهنده و از نظر نظری غنی است، اما کمتر به مختصات منحصربه‌فرد و چندلایه نظام حقوقی جمهوری اسلامی ایران (از جمله ظرفیت‌های اصول ۳، ۹، ۱۷۵ و قوانین عادی در کنار قیود اصل ۲۴) توجه کرده و از ارائه راهکارهای سیاستی متناسب با این بوم حقوقی و فرهنگی ناتوان است.

نوآوری و ضرورت این پژوهش دقیقاً در پر کردن همین شکاف نهفته است. این مقاله تلاش دارد تا با بهره‌گیری از غنای تحلیلی نظریه‌های «حاکمیت سایبری» و «لایه‌های کنترل اینترنت» (به عنوان چارچوب نظری)، ضمن توجه به دغدغه‌های مشروع حاکمیتی (جریان اول) و توجه به هشدارهای جدی حقوق بشری (جریان دوم)، به این پرسش پاسخ دهد که چگونه می‌توان بر اساس مبانی استوار حقوقی جمهوری اسلامی ایران و با الهام از درس‌های عینی تجارب تطبیقی، مدلی از سیاست‌گذاری را برای شبکه ملی اطلاعات طراحی و اجرا کرد که هم اهداف راهبردی کشور در زمینه استقلال دیجیتال، امنیت ملی و توسعه اقتصادی را تأمین کند و هم در محافظت از حقوق بنیادین شهروندان، به‌ویژه آزادی بیان و حریم خصوصی به عنوان یک فرصت و مزیت راهبردی، نه یک مانع و تهدید، مؤثر باشد. به طور مشخص، تحلیل تطبیقی و همزمان اسناد مصوب شورای عالی فضای مجازی (سند تعریف ۱۳۹۲ و سند تبیین الزامات ۱۳۹۵) با اصول قانون اساسی و قوانین عادی، اقدامی است که برای نخستین بار در این پژوهش به طور نظام‌مند و با تمرکز بر پیامدهای آن برای آزادی بیان انجام می‌شود.

منابع

- انصاری، باقر. (۱۳۹۹). حق دسترسی به اینترنت؛ مبانی و محتوا. مجله حقوقی دادگستری، ۸۴(۲)، ۴۵-۶۸.
- جلالی، محمود، و رضایی، حسن. (۱۴۰۰). حمایت از داده‌های شخصی در فضای سایبر: بررسی تطبیقی نظام حقوقی ایران و اتحادیه اروپا. فصلنامه پژوهش‌های حقوق تطبیقی، ۲۵(۱)، ۵۵-۸۰.
- رضایی، علی، محمدی، حافظ. (۱۳۹۶). تحلیل هزینه-فایده توسعه ترافیک داخلی در شبکه ملی اطلاعات. مجله مهندسی برق دانشگاه تبریز، ۴۷(۲)، ۱۳۵-۱۲۱.
- زاهدی، مهدی. (۱۴۰۰). آزادی بیان و اصل دوگانگی ایده و بیان. فصلنامه علمی پژوهش حقوق عمومی، ۲۲(۳)، ۸۹-۱۱۲.
- سعیدی، رحمان. (۱۴۰۱). حقوق بین‌المللی تطبیقی ارتباطات (جلد دوم). تهران: انتشارات سیمای شرق.
- شورای عالی فضای مجازی. (۱۳۹۲). طرح کلان و معماری شبکه ملی اطلاعات. تهران: مرکز ملی فضای مجازی.
- شورای عالی فضای مجازی. (۱۳۹۵). سندتیین الزامات شبکه ملی اطلاعات. تهران: مرکز ملی فضای مجازی.
- قانون انتشار و دسترسی آزاد به اطلاعات، مصوب ۱۳۸۸ مجلس شورای اسلامی. قانون اساسی جمهوری اسلامی ایران.
- کمالی، تقی. (۱۳۹۸). امنیت سایبری و حفاظت داده‌ها. تهران: انتشارات پشتیبان.
- کهوند، محمد. (۱۳۹۶). شبکه ملی اطلاعات. نشریه مبلغان، ۱۷(۴)، ۳۳-۵۰.
- محمدی، حافظ. (۱۳۹۵). ضرورت‌های راهبردی شبکه ملی اطلاعات. فصلنامه امنیت ملی، ۶(۲۱)، ۴۵-۶۸.
- محمدی، حافظ. (۱۳۹۹). شبکه ملی اطلاعات و تحقق حکمرانی سایبری در جمهوری اسلامی ایران با رویکرد تجربه کشورها. در دومین همایش ملی حکمرانی اسلامی، تهران، ایران، ۱۵-۱.
- معمندنژاد، کاظم. (۱۳۸۸). حقوق ارتباطات. تهران: دفتر مطالعات و توسعه رسانه‌ها.
- همایون، محمدهادی، و هاشمی، محمدساجد. (۱۳۹۶). بازنمایی شبکه ملی اطلاعات در رسانه‌های برون‌مرزی. فصلنامه مطالعات رسانه‌های نوین، ۸(۲)، ۱۴۴-۱۲۱.

شبکه ملی اطلاعات،
آزادی بیان و حریم
خصوصی: تحلیل تطبیقی
زیرساخت‌های ملی
ارتباطات و ارائه الگوی
سیاستی در چارچوب حقوقی
جمهوری اسلامی ایران

Carr, M. (2016). *US Power and the Internet in International Relations: The Irony of the Information Age*. London: Palgrave Macmillan.

DeNardis, L. (2014). *The Global War for Internet Governance*. New Haven: Yale University Press.

Lessig, L. (2006). *Code: Version 2.0*. New York: Basic Books.

MacKinnon, R. (2012). *Consent of the Networked: The Worldwide Struggle for Internet Freedom*. New York: Basic Books.

Mueller, M. L. (2010). *Networks and States: The Global Politics of Internet Governance*. Cambridge: MIT Press.

·Office of the United Nations High Commissioner for Human Rights (OHCHR). (2020). *Human Rights and States of Emergency: Procedural and Substantive Safeguards*. Geneva: United Nations.

Soldatov, A., & Borogan, I. (2020). Russia's sovereign internet: A new era of control. *Foreign Affairs*, 99(4), 88-97.

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs.