



Submit Date: 25 August 2024
Revise Date: 03 November 2024
Accept Date: 14 November 2024
Publish Date: 26 November 2024

The Encyclopedia of Comparative Jurisprudence and Law

Investigating the Impact of Internet Filtering on Users' Privacy in Cyberspace

MohammadReza Rahmat¹, Sahand Nezaminia^{*2}

1. Assistant Professor, Department of Law, Faculty of Law, Meybod University, Meybod, Iran
2. PhD student, Department of Law, Criminal and Criminology, Faculty of Law, University of Meybod, Meybod, Iran

* Corresponding Author's Email: Dr.nezaminia@gmail.com

ABSTRACT

Cyberspace, as one of the most significant phenomena of the digital era, plays a pivotal role in facilitating communication, expanding businesses, and providing access to information. Simultaneously, filtering policies and internet restrictions have introduced serious challenges to user privacy and fundamental rights. The purpose of this study is to examine the impacts of internet filtering on users' privacy and to analyze the associated legal, social, and jurisprudential dimensions. This research adopts a descriptive-analytical approach, utilizing analysis of national and international laws, jurisprudential principles such as the "no-harm" rule (La Darar), and a comparative study of filtering policies in China, Singapore, and Iran. The findings revealed that non-transparent and broad filtering policies can lead to significant violations of privacy, reduced access to reliable information, severe restrictions on freedom of expression, and disruption of the digital economy. Moreover, these policies diminish public trust and increase reliance on illegal tools such as VPNs. In contrast, the use of intelligent technologies, the development of transparent legislation, and the implementation of targeted content management tools can establish an effective balance between security and privacy, thereby restoring user trust in cyberspace governance policies.

Keywords: *Filtering, Privacy, Cyberspace, User Rights.*

How to cite: Rahmat, M. R., & Nezaminia, S. (2024). Investigating the Impact of Internet Filtering on Users' Privacy in Cyberspace. *The Encyclopedia of Comparative Jurisprudence and Law*, 2(3), 55-71.



تاریخ ارسال: ۴ شهریور ۱۴۰۳
تاریخ بازنگری: ۱۳ آبان ۱۴۰۳
تاریخ پذیرش: ۲۴ آبان ۱۴۰۳
تاریخ چاپ: ۶ آذر ۱۴۰۳

دانشنامه فقه و حقوق تطبیقه

بررسی تاثیر فیلترینگ بر حریم خصوصی کاربران در فضای مجازی

محمد رضا رحمت^۱، سهند نظامی نیا^{۲*}

۱. استادیار، گروه حقوق، دانشکده حقوق، دانشگاه میبد، میبد، ایران

۲. دانشجوی دکتری، گروه حقوق، گرایش جزا و جرم شناسی، دانشکده حقوق، دانشگاه میبد، میبد، ایران

* پست الکترونیک نویسنده مسئول: Dr.nezaminia@gmail.com

چکیده

فضای مجازی، به عنوان یکی از مهم ترین پدیده های عصر دیجیتال، نقشی کلیدی در ایجاد ارتباطات، توسعه کسب و کارها و دسترسی به اطلاعات ایفا می کند. در عین حال، سیاست های فیلترینگ و محدودیت های اینترنتی، چالش های جدی برای حریم خصوصی و حقوق بنیادین کاربران ایجاد کرده اند. هدف این پژوهش بررسی تأثیرات فیلترینگ بر حریم خصوصی کاربران و تحلیل ابعاد حقوقی، اجتماعی و فقهی مرتبط با آن است. این پژوهش با رویکرد تحلیلی-توصیفی و با بهره گیری از تحلیل قوانین ملی و بین المللی، اصول فقهی نظیر قاعده "لاضرر"، و مطالعه تطبیقی سیاست های فیلترینگ در کشورهای چین، سنگاپور و ایران انجام شده است. یافته ها نشان داد که سیاست های فیلترینگ غیرشفاف و گسترده می توانند به نقض جدی حریم خصوصی، کاهش دسترسی به اطلاعات معتبر، محدودیت شدید بر آزادی بیان و اختلال در اقتصاد دیجیتال منجر شوند. همچنین، این سیاست ها با کاهش اعتماد عمومی و افزایش وابستگی به ابزارهای غیرقانونی مانند VPN همراه است. در مقابل، بهره گیری از فناوری های هوشمند، تدوین قوانین شفاف، و استفاده از ابزارهای مدیریت هدفمند محتوا می تواند تعادل مؤثری میان امنیت و حریم خصوصی ایجاد کند و اعتماد کاربران را به سیاست های مدیریت فضای مجازی بازگرداند.

کلیدواژگان: فیلترینگ، حریم خصوصی، فضای مجازی، حقوق کاربران.

کسب و کارهای آنلاین، نقض آزادی اطلاعات و محدودیت در استفاده از شبکه‌های اجتماعی شود (Ogungbemi et al., 2024).

هدف این مطالعه، بررسی تأثیرات فیلترینگ بر حریم خصوصی کاربران با تمرکز بر ابعاد حقوقی، اجتماعی و عملی آن است. با تحلیل مبانی نظری و ارائه نمونه‌های واقعی، این مقاله تلاش می‌کند تا چشم‌اندازی جامع از این موضوع ارائه دهد و راهکارهایی برای حفظ تعادل میان امنیت فضای مجازی و رعایت حقوق شهروندی پیشنهاد کند.

۱. پیشینه پژوهش

پژوهش‌های مرتبط در زمینه تأثیر فیلترینگ بر حقوق شهروندان، یافته‌های متنوعی را ارائه می‌دهند. محمدی‌نیا (۱۴۰۳) در مقاله‌ای به بررسی مبانی فقهی و حقوقی مسئولیت مدنی دولت در قبال فیلترینگ شبکه‌های اجتماعی پرداخت. این پژوهش نشان داد که اصول فقهی مانند قاعده "لاضرر"، احترام به کرامت انسانی و قاعده تسبیب، بر لزوم حفظ حقوق کاربران تأکید دارند و هرگونه محدودیت باید با رعایت حقوق اساسی شهروندان و در چهارچوب اصول حقوقی مانند نظریه مسئولیت مبتنی بر تقصیر و خطر اعمال شود. نتایج این تحقیق بیانگر ضرورت الزام‌آور بودن مسئولیت مدنی دولت در این حوزه است (Mohammadi Nia & Karamati Moaz, 2024). همچنین بیداروند (۱۴۰۰) در مقاله‌ای تحت عنوان "فیلترینگ تلگرام از بایستگی امنیت ملی تا نقض آزادی بیان" به تحلیل فیلترینگ تلگرام پرداخت و نشان داد که این اقدام به منظور تأمین امنیت ملی ممکن است در مواردی مجاز باشد؛ اما در عین حال، با محدودیت‌هایی برای آزادی بیان مواجه است. پژوهش وی تأکید داشت که اعمال فیلترینگ باید تنها در موارد قانونی و با اولویت‌دهی به امنیت ملی در برابر تهدیدات واقعی صورت پذیرد. این تحقیقات به درک بهتر

در دنیای امروز، فضای مجازی به بخشی جدایی‌ناپذیر از زندگی اجتماعی، فرهنگی و اقتصادی انسان‌ها تبدیل شده است. این فضا امکان تبادل سریع اطلاعات، ارتباطات گسترده و دسترسی به منابع مختلف را فراهم آورده، اما در عین حال، چالش‌های مهمی را نیز به همراه داشته است (Moradi et al., 2019). یکی از این چالش‌ها مسئله فیلترینگ است که به عنوان ابزاری برای کنترل و مدیریت محتوا توسط دولت‌ها به کار می‌رود (Derikvand & Jafari, 2023). فیلترینگ، اگرچه با هدف حفظ امنیت، نظم عمومی و جلوگیری از نشر محتوای مخرب اعمال می‌شود، می‌تواند تأثیرات جدی و غیرقابل‌انکاری بر حقوق بنیادین افراد، به ویژه حریم خصوصی آنان، داشته باشد (Tashev, 2024). حریم خصوصی به معنای حفاظت از اطلاعات شخصی و حق افراد برای کنترل دسترسی دیگران به اطلاعات مربوط به زندگی خصوصی‌شان، از اصول بنیادین حقوق بشری است (Alimoradi, 2022). فضای مجازی با فراهم کردن دسترسی آسان به اطلاعات، این حق را به شدت در معرض تهدید قرار داده و فیلترینگ، در صورتی که ناموجه و غیرشفاف اعمال شود، می‌تواند نقض آشکار این حق تلقی شود (Liu et al., 2020). تحلیل و ارزیابی این مسئله از اهمیت ویژه‌ای برخوردار است؛ چرا که از یک سو، دولت‌ها موظف‌اند امنیت فضای مجازی را تأمین کنند و از سوی دیگر، باید از نقض حقوق فردی شهروندان جلوگیری نمایند (Rahimi et al., 2021). از منظر حقوقی، قاعده "لاضرر" و اصولی چون احترام به کرامت انسانی، احترام به حریم خصوصی و نظریه‌های حقوقی مانند مسئولیت مبتنی بر تقصیر و خطر، چارچوب‌های مهمی برای تحلیل این مسئله ارائه می‌دهند (Hossein Nejad & Moniri Hamzeh Kolai, 2017). در عین حال، این مباحث از بعد عملی نیز چالش‌برانگیز هستند؛ چرا که فیلترینگ می‌تواند موجب اختلال در

تعارض‌ها و توازن میان امنیت ملی و حفظ حقوق کاربران کمک شایانی می‌کند (Bidarvand et al., 2021).

۲. روش تحقیق

این پژوهش از روش توصیفی-تحلیلی برای بررسی تأثیرات فیلترینگ بر حریم خصوصی کاربران استفاده کرده است. در این راستا، با تحلیل مبانی نظری، اصول فقهی نظیر قاعده "لاضرر"، و قوانین ملی و بین‌المللی مرتبط، تلاش شده است چارچوبی برای ارزیابی حقوقی و اجتماعی این مسئله ارائه شود. همچنین، مطالعه تطبیقی سیاست‌های فیلترینگ در کشورهای چین، سنگاپور و ایران به منظور شناسایی تفاوت‌ها و شباهت‌ها در رویکردها انجام شده است. داده‌های مورد استفاده عمدتاً از طریق منابع کتابخانه‌ای، مقالات پژوهشی و مستندات قانونی جمع‌آوری شده و با رویکردی تحلیلی مورد بررسی قرار گرفته‌اند.

۳. چارچوب نظری

۳.۱. مفهوم‌شناسی و مبانی نظری

۳.۱.۱. تعریف فیلترینگ و انواع آن

فیلترینگ به معنای محدودسازی یا کنترل دسترسی کاربران به محتواها یا خدمات خاص در فضای مجازی است. این اقدام عمدتاً توسط دولت‌ها یا نهادهای نظارتی به منظور تأمین امنیت، حفظ اخلاق عمومی یا جلوگیری از انتشار محتوای غیرقانونی اعمال می‌شود. فیلترینگ از دو منظر قابل بررسی است: فیلترینگ فنی و فیلترینگ قانونی. در فیلترینگ فنی، از ابزارها و فناوری‌هایی نظیر دیوار آتش یا پروکسی برای محدودسازی دسترسی استفاده می‌شود، در حالی که فیلترینگ قانونی مبتنی بر مصوبات و دستورالعمل‌های قانونی است که اغلب توسط سیستم‌های قضایی و قانون‌گذاری تدوین می‌شود (Nasrollahi, 2023). علاوه بر این، فیلترینگ می‌تواند از لحاظ گستردگی نیز دسته‌بندی شود: محدودسازی جزئی که تنها بخشی از محتواها را مسدود می‌کند، و محدودسازی کلی که کل یک پلتفرم یا سرویس را از دسترس

خارج می‌سازد. این تنوع در ابزارها و رویکردهای فیلترینگ باعث شده تا تأثیرات آن بر کاربران نیز به‌طور گسترده‌ای متغیر باشد (Liang et al., 2021).

۳.۱.۳. حریم خصوصی: مفاهیم، مصادیق و اهمیت

حریم خصوصی یکی از مهم‌ترین حقوق بنیادین افراد است که بر حق کنترل آن‌ها بر اطلاعات شخصی و تعاملات خصوصی‌شان تأکید دارد. این مفهوم دربرگیرنده جنبه‌های مختلفی از زندگی افراد، از جمله حریم فیزیکی، حریم اطلاعاتی، و حریم ارتباطی است. در دنیای دیجیتال، حریم خصوصی به داده‌هایی مانند اطلاعات مالی، تاریخچه جستجوها، فعالیت‌های شبکه‌های اجتماعی، موقعیت جغرافیایی و تعاملات آنلاین کاربران گسترش یافته است. اهمیت حریم خصوصی در فضای مجازی از دو جنبه برجسته است. نخست، این حق به افراد اجازه می‌دهد که هویت، عقاید و رفتارهای خود را آزادانه و بدون ترس از نظارت یا سوءاستفاده ابراز کنند. دوم، حریم خصوصی به ایجاد اعتماد میان کاربران و پلتفرم‌های آنلاین کمک می‌کند و این اعتماد برای عملکرد صحیح اقتصاد دیجیتال حیاتی است. نقض این حریم می‌تواند عواقب جدی به همراه داشته باشد، از جمله سرقت هویت، کلاهبرداری‌های مالی، انتشار اطلاعات شخصی بدون رضایت، و حتی تبعیض یا سرکوب سیاسی (Hejazi Nia, 2015). در سطح جهانی، برخی کشورها قوانینی جامع برای حفاظت از حریم خصوصی تدوین کرده‌اند، نظیر "قانون حفاظت از داده‌های عمومی (GDPR)" در اتحادیه اروپا، که شرکت‌ها را ملزم می‌کند تا داده‌های کاربران را با شفافیت مدیریت کنند. با این حال، در بسیاری از نقاط جهان، نبود قوانین مناسب یا اجرای ضعیف آن‌ها، حریم خصوصی کاربران را در معرض تهدید قرار داده است. همچنین، ظهور فناوری‌هایی نظیر هوش مصنوعی و اینترنت اشیا (IoT) چالش‌های جدیدی را برای حفاظت از حریم خصوصی به وجود آورده است. این شرایط نشان می‌دهد که حریم

محدودسازی آزادی‌های مدنی استفاده می‌کنند. این شرایط نیازمند سیاست‌گذاری‌های جامع و رویکردهای مبتنی بر حقوق بشر است تا تعادل میان استفاده از فضای مجازی و حفظ حقوق کاربران حفظ شود (Beigi, 2018).

۲.۳. مبانی حقوقی فیلترینگ و حریم خصوصی

مبانی حقوقی فیلترینگ و حریم خصوصی به بررسی چهارچوب‌های قانونی و اصول حقوقی مرتبط با محدودسازی دسترسی به محتوا در فضای مجازی می‌پردازد. این موضوع شامل تحلیل قوانین ملی و بین‌المللی، ارزیابی ارتباط میان حق دسترسی به اطلاعات و حفظ حریم خصوصی، و تبیین تعارض میان سیاست‌های فیلترینگ و حقوق شهروندی است.

۱.۲.۳. تحلیل قوانین ملی و بین‌المللی در خصوص فیلترینگ

تحلیل قوانین ملی و بین‌المللی در زمینه فیلترینگ نشان‌دهنده پیچیدگی‌ها و تفاوت‌های قابل توجهی میان کشورها است. در سطح ملی، بسیاری از دولت‌ها قوانینی را تصویب کرده‌اند که هدف آن‌ها محدودسازی محتوای مضر یا غیرقانونی در فضای مجازی است. در ایران، قانون جرائم رایانه‌ای مصوب ۱۳۸۸، به همراه مصوبات شورای عالی فضای مجازی، اختیارات گسترده‌ای به نهادهای دولتی داده است تا دسترسی به محتوای اینترنتی را محدود کنند. این قوانین معمولاً به دلایل امنیت ملی، اخلاق عمومی، یا حفاظت از حقوق کودکان اعمال می‌شوند. به عنوان مثال، مسدودسازی سایت‌ها یا پلتفرم‌هایی که از دیدگاه دولت تهدیدی برای نظم عمومی تلقی می‌شوند، در چارچوب این قوانین قرار می‌گیرد (Rahmani et al., 2023). در سطح بین‌المللی، قوانین و اسناد حقوق بشری نظیر ماده ۱۹ اعلامیه جهانی حقوق بشر، آزادی بیان و دسترسی به اطلاعات را به عنوان حقوق بنیادین انسان به رسمیت شناخته‌اند. ماده ۱۰ کنوانسیون اروپایی حقوق بشر نیز تصریح می‌کند که آزادی بیان شامل دریافت و انتقال اطلاعات بدون دخالت دولت‌ها است، اما این آزادی‌ها می‌توانند تحت شرایط

خصوصی دیگر یک مسئله فردی نیست، بلکه بخشی از حقوق جمعی جامعه است که نیازمند رویکردی جامع در سیاست‌گذاری‌ها و قوانین است (Ghanad & Aliqoli, 2020).

۳.۱.۳. نقش فضای مجازی در حفظ یا نقض حقوق کاربران

فضای مجازی یک ابزار دوگانه است که می‌تواند به‌طور همزمان به حفظ یا نقض حقوق کاربران منجر شود. از یک سو، اینترنت به عنوان یک بستر گسترده، امکان دسترسی آزاد به اطلاعات، برقراری ارتباطات اجتماعی، و مشارکت در فعالیت‌های مدنی و سیاسی را فراهم می‌کند. کاربران می‌توانند عقاید خود را بدون محدودیت جغرافیایی بیان کرده و از منابع گوناگون برای یادگیری و تبادل دانش بهره‌مند شوند. این ویژگی‌ها، فضای مجازی را به ابزاری قدرتمند برای ارتقای آگاهی عمومی، تقویت آزادی بیان، و توسعه اجتماعی تبدیل کرده است. از سوی دیگر، فضای مجازی می‌تواند زمینه‌ساز نقض گسترده حقوق کاربران باشد. جمع‌آوری و تحلیل داده‌های کاربران توسط شرکت‌ها و دولت‌ها بدون رضایت یا اطلاع آنان، یکی از بزرگ‌ترین تهدیدات برای حریم خصوصی است. این نقض‌ها شامل نظارت گسترده بر ارتباطات، استفاده از اطلاعات شخصی برای اهداف تجاری یا سیاسی، و حتی سانسور محتوا و محدودسازی آزادی بیان است. علاوه بر این، فعالیت‌های غیرقانونی نظیر هک، کلاهبرداری، و انتشار اطلاعات نادرست نیز در این فضا به تهدیدی برای امنیت کاربران تبدیل شده است (Moradi et al., 2019). نقش دولت‌ها و سازمان‌ها در این میان بسیار مهم است. در برخی کشورها، قوانین شفاف و محافظت‌کننده از حقوق کاربران تدوین شده است که تعادل میان آزادی و امنیت را تضمین می‌کند. برای مثال، دولت‌هایی که شفافیت و حفاظت از داده‌ها را در اولویت قرار می‌دهند، اعتماد عمومی بیشتری ایجاد می‌کنند. با این حال، در بسیاری از کشورها، دولت‌ها از فضای مجازی به عنوان ابزاری برای نظارت گسترده و

ایجاد چارچوب‌های شفاف و مشارکت کاربران در تصمیم‌گیری می‌تواند این توازن را تسهیل کند (Elyasi et al., 2022).

۳.۲.۳. حقوق شهروندی و تعارض با سیاست‌های فیلترینگ

حقوق شهروندی، شامل آزادی بیان، حریم خصوصی، و دسترسی به اطلاعات، اساس یک جامعه دموکراتیک است. سیاست‌های فیلترینگ گسترده اغلب در تقابل با این حقوق قرار دارند و می‌تواند منجر به نقض گسترده آزادی‌های فردی شوند. برای مثال، مسدودسازی شبکه‌های اجتماعی پرکاربرد نه تنها آزادی بیان را محدود می‌کند، بلکه به‌طور مستقیم بر ارتباطات اجتماعی، تعاملات فرهنگی، و حتی فعالیت‌های اقتصادی کاربران تأثیر منفی می‌گذارد. این تعارض زمانی شدت می‌گیرد که سیاست‌های فیلترینگ فاقد شفافیت و دلایل منطقی باشند یا به‌صورت تبعیض‌آمیز اعمال شوند (Mohammadi et al., 2019). از سوی دیگر، دولت‌ها موظف‌اند امنیت ملی و نظم عمومی را تأمین کنند، اما این مسئولیت نباید بهانه‌ای برای نقض گسترده حقوق شهروندی باشد. نمونه‌های موفق در کشورهای توسعه‌یافته نشان داده است که دولت‌ها می‌توانند با ایجاد قوانین جامع و مشخص، تعارض میان امنیت و حقوق شهروندی را کاهش دهند. برای مثال، برخی کشورها از فناوری‌های پیشرفته برای محدودسازی هدفمند محتواهای مخرب استفاده می‌کنند، بدون آن‌که کل یک پلتفرم را مسدود کنند. علاوه بر این، مشارکت جامعه مدنی و سازمان‌های مستقل در نظارت بر سیاست‌های فیلترینگ، می‌تواند از سوءاستفاده‌های احتمالی جلوگیری کند. در نهایت، اعمال سیاست‌هایی که اصول عدالت، شفافیت، و تناسب را رعایت کنند، می‌تواند توازنی میان امنیت و آزادی‌های شهروندی برقرار کند و اعتماد عمومی را به سیاست‌های دولت افزایش دهد (Hashemi et al., 2021).

۳.۳. مبانی فقهی مرتبط با فیلترینگ و حریم خصوصی

خاصی محدود شوند، نظیر حفظ امنیت ملی، پیشگیری از جنایات یا محافظت از اخلاق عمومی. این استثنائات باعث ایجاد چالش‌هایی در تعیین حدود و قلمرو اعمال فیلترینگ می‌شود. در عمل، تضاد میان قوانین ملی و استانداردهای بین‌المللی، به‌ویژه در کشورهایی که چارچوب‌های حقوق بشری ضعیف‌تر دارند، منجر به نقض حقوق کاربران می‌شود. به همین دلیل، ایجاد سازوکارهای نظارتی شفاف و مستقل که بر اجرای محدودیت‌ها نظارت کند، امری ضروری به نظر می‌رسد (Ramak et al., 2019).

۲.۲.۳. ارتباط میان حق دسترسی به اطلاعات و حریم خصوصی

حق دسترسی به اطلاعات و حریم خصوصی، هرچند در نگاه اول به‌ظاهر مستقل به نظر می‌رسند، اما در فضای مجازی به‌شدت به یکدیگر وابسته‌اند. دسترسی آزاد به اطلاعات به کاربران امکان می‌دهد تا به منابع گسترده‌ای از داده‌ها و اخبار دست یابند، که برای تقویت آزادی بیان، مشارکت مدنی، و آگاهی عمومی حیاتی است. از سوی دیگر، همین دسترسی می‌تواند به نقض حریم خصوصی افراد منجر شود، به‌ویژه زمانی که داده‌های کاربران بدون رضایت آن‌ها توسط سازمان‌ها، شرکت‌ها، یا نهادهای دولتی جمع‌آوری و تحلیل می‌شود. این تعارض، نیاز به ایجاد توازن میان این دو حق اساسی را بیش از پیش برجسته می‌کند. برای مثال، قوانین حفاظت از داده‌های شخصی، نظیر GDPR در اتحادیه اروپا، تلاش می‌کنند تا از نقض حریم خصوصی جلوگیری کنند، در حالی که همچنان دسترسی به اطلاعات عمومی را تسهیل می‌کنند. اما در غیاب چنین قوانین شفاف، سیاست‌های فیلترینگ می‌توانند هر دو حق را تهدید کنند. به‌عنوان نمونه، استفاده گسترده از ابزارهای نظارتی برای فیلترینگ محتوا می‌تواند منجر به نقض حریم خصوصی کاربران شود. در عین حال، اعمال محدودیت‌های غیرشفاف بر دسترسی به اطلاعات، آزادی بیان را تضعیف می‌کند. این شرایط نیازمند سیاست‌گذاری‌هایی است که تضمین کند هیچ‌کدام از این حقوق قربانی دیگری نشوند، و راه‌حل‌هایی مانند

افزایش نارضایتی اجتماعی منجر شود (Behbood & Mobin, 2023).

۲.۳.۳. اصل احترام به کرامت انسانی و حریم مؤمن

اصل احترام به کرامت انسانی یکی از اصول اساسی در فقه اسلامی است که حفظ شأن و جایگاه افراد را در هر شرایطی واجب می‌داند. در فضای مجازی، این اصل بر لزوم حفاظت از حریم خصوصی کاربران و عدم تعرض به اطلاعات شخصی آن‌ها تأکید دارد. نقض این اصل، از طریق فیلترینگ غیرشفاف یا نظارت گسترده، می‌تواند حس بی‌اعتمادی و ناامنی را در میان کاربران ایجاد کند. حریم مؤمن، که به‌عنوان بخشی از کرامت انسانی در فقه اسلامی شناخته می‌شود، به معنای مصونیت افراد از هرگونه تعرض به اطلاعات و ارتباطات خصوصی‌شان است. این مفهوم در فضای مجازی اهمیت دوچندانی می‌یابد، زیرا اطلاعات شخصی کاربران به راحتی قابل ذخیره‌سازی و تحلیل است (Vali Asl, 2024). دولت‌ها بر اساس این اصل موظف‌اند که از ابزارهای نظارتی با احتیاط و تنها در شرایطی استفاده کنند که به‌طور قانونی و موجه ضرورت داشته باشد. انتشار یا تحلیل داده‌های کاربران بدون رضایت آنان، نقض آشکار کرامت انسانی است و می‌تواند به سوءاستفاده‌های گسترده منجر شود. این اصل دولت را ملزم می‌کند که نه تنها از ورود غیرموجه به حریم خصوصی کاربران اجتناب کند، بلکه با استفاده از فناوری‌های مدرن، امنیت و حقوق کاربران را تضمین نماید. علاوه بر این، تأکید بر شفافیت و اطلاع‌رسانی در مورد نحوه و دلایل اعمال نظارت یا محدودیت‌های خاص، بخشی از تعهد دولت به حفظ کرامت انسانی محسوب می‌شود (Khan Mohammadi & Shameli, 2016).

۳.۳.۳. قاعده تسبیب و مسئولیت دولت در قبال زیان‌های ناشی از فیلترینگ

مبانی فقهی مرتبط با فیلترینگ و حریم خصوصی شامل اصول قواعدی است که از آموزه‌های اسلامی نشأت گرفته و نقش اساسی در تبیین مسئولیت دولت و حفظ حقوق شهروندان در فضای مجازی دارند. این اصول در ارزیابی مشروعیت فیلترینگ و تأثیر آن بر حریم خصوصی افراد بسیار حائز اهمیت‌اند.

۱.۳.۳. قاعده "لاضرر" و تأثیر آن بر محدودیت‌های فضای مجازی

قاعده "لاضرر" یکی از اصول کلیدی فقه اسلامی است که بر نفع هرگونه زیان غیرموجه در تعاملات انسانی تأکید دارد. این قاعده، که از حدیث مشهور پیامبر اسلام "لا ضرر و لا ضرار فی الاسلام" استخراج شده است، به‌ویژه در فضای مجازی نقشی حیاتی ایفا می‌کند. بر اساس این قاعده، دولت‌ها موظف‌اند در اعمال محدودیت‌ها، از وارد کردن زیان‌های گسترده و غیرضروری به جامعه خودداری کنند. در حوزه فیلترینگ، مسدودسازی کامل یک پلتفرم می‌تواند پیامدهای زیان‌باری به همراه داشته باشد، از جمله از دست رفتن فرصت‌های شغلی، محدودیت در دسترسی به منابع آموزشی، و کاهش فرصت‌های تعامل اجتماعی. این زیان‌ها، به‌ویژه در شرایطی که بخش قابل توجهی از فعالیت‌های اقتصادی و فرهنگی بر بستر فضای مجازی انجام می‌شود، می‌تواند عواقب اجتماعی و اقتصادی گسترده‌ای داشته باشند. از سوی دیگر، اعمال فیلترینگ در چارچوب "لاضرر" تنها زمانی مشروع است که هدف آن جلوگیری از زیان‌های بزرگ‌تر مانند انتشار محتوای خشونت‌آمیز یا تهدیدات امنیتی باشد. این قاعده همچنین دولت را ملزم می‌کند که در صورت بروز زیان، مسئولیت جبران خسارت را بپذیرد. برای مثال، اگر فیلترینگ منجر به آسیب اقتصادی به کسب‌وکارهای آنلاین شود، دولت موظف است مکانیزم‌هایی برای جبران این زیان‌ها طراحی کند. علاوه بر این، شفافیت در تصمیم‌گیری و توجیه دلایل فیلترینگ از منظر این قاعده ضروری است، زیرا عدم شفافیت می‌تواند به کاهش اعتماد عمومی و

بررسی این پیامدها در سه حوزه اجتماعی-فرهنگی، اقتصادی و حقوقی می‌پردازد.

۱.۴.۳. پیامدهای اجتماعی و فرهنگی

فیلترینگ به‌طور گسترده بر ابعاد اجتماعی و فرهنگی زندگی کاربران تأثیر می‌گذارد. این محدودیت‌ها کاربران را از مشارکت در جوامع بین‌المللی و دسترسی به اطلاعات و فرهنگ‌های متنوع محروم می‌کند. برای مثال، محدودیت دسترسی به شبکه‌های اجتماعی پرکاربرد مانند اینستاگرام و تلگرام می‌تواند افراد را از اشتراک‌گذاری ایده‌ها، تجربیات، و تعامل با دیگران در سطوح بین‌المللی بازدارد. یکی از پیامدهای مهم این محدودیت‌ها کاهش تنوع فرهنگی است، زیرا محتواهای داخلی که اغلب توسط سیاست‌های نظارتی کنترل می‌شوند، نمی‌توانند جایگزین محتواهای جهانی شوند. از سوی دیگر، فیلترینگ می‌تواند باعث افزایش استفاده از ابزارهای غیرقانونی مانند VPN برای دسترسی به محتوای مسدود شده شود. این وضعیت خطرات امنیتی را برای کاربران افزایش داده و آن‌ها را در معرض سوءاستفاده هکرها و بدافزارها قرار می‌دهد. در سطح اجتماعی، این محدودیت‌ها می‌توانند به کاهش اعتماد عمومی نسبت به دولت منجر شوند، زیرا کاربران این سیاست‌ها را به‌عنوان ابزاری برای کنترل اجتماعی در نظر می‌گیرند. همچنین، نسل جوان که بیشترین کاربران فضای مجازی هستند، ممکن است با احساس انزوا و محدودیت مواجه شوند، که این امر بر تعاملات اجتماعی آن‌ها و حتی وضعیت روانی‌شان تأثیر منفی دارد. این پیامدها نشان می‌دهند که فیلترینگ فراتر از محدودیت دسترسی به محتوا، تأثیر عمیقی بر بافت اجتماعی و فرهنگی جامعه دارد (Zaroudi & Borzoui, 2022).

۲.۴.۳. تأثیر فیلترینگ بر کسب‌وکارهای آنلاین

اعمال فیلترینگ تأثیرات مخربی بر اقتصاد دیجیتال دارد و کسب‌وکارهای آنلاین، به‌ویژه استارت‌آپ‌ها و مشاغل کوچک، از

قاعده تسبیب در فقه اسلامی بر این اصل تأکید دارد که هرکس به طور غیرمستقیم سبب وقوع زیان برای دیگری شود، مسئول جبران خسارت است. این قاعده در زمینه سیاست‌های فیلترینگ نیز به‌طور گسترده قابل اعمال است. دولت‌ها به عنوان مجریان اصلی فیلترینگ، مسئول پیامدهای زیان‌باری هستند که ممکن است از این سیاست‌ها ناشی شود. برای مثال، اعمال فیلترینگ گسترده می‌تواند به تعطیلی کسب‌وکارهای کوچک که به پلتفرم‌های آنلاین وابسته‌اند، محدودیت در دسترسی به منابع علمی و آموزشی، و حتی افزایش تنش‌های اجتماعی منجر شود. بر اساس قاعده تسبیب، دولت‌ها موظف‌اند که پیش از اعمال فیلترینگ، پیامدهای احتمالی آن را ارزیابی کرده و از اعمال سیاست‌هایی که زیان‌های گسترده و غیرقابل جبرانی به همراه دارند، اجتناب کنند. این قاعده همچنین بر لزوم تناسب در اعمال محدودیت‌ها تأکید دارد؛ یعنی فیلترینگ باید تنها در شرایطی انجام شود که تهدید جدی برای امنیت عمومی یا منافع جامعه وجود داشته باشد. در غیر این صورت، استفاده از این ابزار می‌تواند به نقض حقوق کاربران منجر شود. علاوه بر این، قاعده تسبیب دولت را ملزم می‌کند که در صورت وارد شدن زیان به کاربران، اقدامات جبرانی مناسب انجام دهد. این اقدامات می‌تواند شامل ارائه حمایت مالی به کسب‌وکارهای آسیب‌دیده، تسهیل دسترسی به ابزارهای جایگزین، یا اصلاح سیاست‌های فیلترینگ باشد. این قاعده نقش کلیدی در تنظیم تعادل میان مسئولیت دولت و حفظ حقوق شهروندان ایفا می‌کند و به‌عنوان مبنای مهمی برای سیاست‌گذاری فضای مجازی محسوب می‌شود (Sadeghi & Ghasemi, 2022).

۴.۳. تأثیرات عملی فیلترینگ بر حریم خصوصی کاربران

فیلترینگ به‌عنوان ابزاری برای کنترل فضای مجازی، پیامدهای گسترده‌ای بر جنبه‌های مختلف زندگی کاربران، از جمله حریم خصوصی، آزادی بیان و کسب‌وکارهای آنلاین دارد. این بخش به

می‌تواند به تحریف واقعیت‌ها و ایجاد یک‌جانبه‌گرایی اطلاعاتی منجر شود. همچنین، فیلترینگ اغلب به‌عنوان ابزاری برای سرکوب صدای مخالفان سیاسی و اجتماعی استفاده می‌شود، که این امر باعث کاهش مشارکت سیاسی و اجتماعی افراد می‌شود. در مواردی، کاربران ممکن است از ترس نظارت یا مجازات‌های قانونی، از اظهار نظر یا اشتراک‌گذاری اطلاعات خودداری کنند. علاوه بر این، محدودیت‌های اعمال‌شده باعث افزایش وابستگی کاربران به منابع غیرقابل‌اعتماد و انتشار شایعات می‌شود. برای مثال، در شرایطی که دسترسی به رسانه‌های بین‌المللی مسدود است، کاربران ممکن است به منابع داخلی روی آورند که در بسیاری از موارد تحت کنترل دولت هستند. این امر می‌تواند به کاهش شفافیت و پاسخگویی در جامعه منجر شود. آزادی بیان و دسترسی به اطلاعات نه تنها حقوق اساسی کاربران هستند، بلکه برای توسعه فرهنگی، سیاسی و اجتماعی جوامع نیز ضروری‌اند، و نقض این حقوق می‌تواند پیامدهای بلندمدتی برای جامعه به همراه داشته باشد (Asadzadeh & Seyed Mousavi, 2015).

۵.۳. تحلیل تطبیقی سیاست‌های فیلترینگ در کشورها

سیاست‌های فیلترینگ در کشورهای مختلف جهان بسته به فرهنگ، اولویت‌های حکومتی و نظام حقوقی متفاوت هستند. برخی کشورها مانند چین، سیاست‌های بسیار سخت‌گیرانه‌ای در کنترل فضای مجازی اجرا می‌کنند، در حالی که کشورهایی مانند سنگاپور تلاش کرده‌اند تا تعادلی میان حفظ امنیت و آزادی بیان برقرار کنند. این تفاوت‌ها نشان‌دهنده اهمیت عوامل فرهنگی، اجتماعی و حقوقی در شکل‌دهی به سیاست‌های فیلترینگ است. در این بخش، سیاست‌های فیلترینگ در کشورهایی مانند چین و سنگاپور بررسی و با سیاست‌های ایران مقایسه می‌شود تا نقاط قوت، ضعف، و قابلیت‌های تطبیقی هر مدل مشخص شود.

جمله آسیب‌دیدگان اصلی این سیاست‌ها هستند. بسیاری از کسب‌وکارهای کوچک از پلتفرم‌های جهانی مانند اینستاگرام، واتساپ و تلگرام برای تبلیغات، فروش، و ارتباط با مشتریان استفاده می‌کنند. فیلترینگ این پلتفرم‌ها می‌تواند باعث کاهش شدید درآمد آن‌ها شود. برای مثال، فروشگاه‌های آنلاین که مخاطبان خود را از طریق شبکه‌های اجتماعی جذب می‌کنند، ممکن است با مسدودسازی این پلتفرم‌ها مشتریان خود را از دست دهند. علاوه بر این، محدودیت دسترسی به ابزارها و خدمات بین‌المللی باعث می‌شود کسب‌وکارها مجبور شوند از پلتفرم‌های داخلی استفاده کنند که معمولاً امکانات و کیفیت پایین‌تری دارند. این موضوع نوآوری را محدود کرده و رقابت‌پذیری اقتصاد دیجیتال کشور را در سطح جهانی کاهش می‌دهد. همچنین، فیلترینگ باعث افزایش هزینه‌های عملیاتی می‌شود، زیرا کسب‌وکارها مجبورند برای دور زدن محدودیت‌ها از ابزارهای جایگزین استفاده کنند. به‌عنوان مثال، راه‌اندازی زیرساخت‌های جدید یا استفاده از خدمات واسطه‌ها برای ادامه فعالیت در فضای مجازی می‌تواند هزینه‌های زیادی برای مشاغل کوچک و متوسط به همراه داشته باشد. در نهایت، اعمال فیلترینگ به‌عنوان مانعی برای سرمایه‌گذاری خارجی نیز عمل می‌کند، زیرا بسیاری از شرکت‌های بین‌المللی در شرایطی که پلتفرم‌های جهانی مسدود شده‌اند، تمایلی به فعالیت در این کشورها ندارند (Rahmani et al., 2023).

۳.۴.۳. نقض آزادی بیان و دسترسی آزاد به اطلاعات

یکی از جدی‌ترین پیامدهای فیلترینگ، نقض آزادی بیان و دسترسی آزاد به اطلاعات است. این اصول اساسی حقوق بشر، تضمین‌کننده دسترسی کاربران به دیدگاه‌های متنوع و امکان اظهار عقاید آزادانه هستند. فیلترینگ باعث می‌شود کاربران به منابع اطلاعاتی رسمی و غیررسمی محدود شوند و از دسترسی به دیدگاه‌ها و اخبار مخالف یا متنوع محروم گردند. این وضعیت

۱.۵.۳. بررسی نمونه‌هایی از سیاست‌های فیلترینگ در کشورهای مختلف

۱.۱.۵.۳. مدل چین: سخت‌گیری گسترده

چین به عنوان یکی از کشورهایی که سیاست‌های سخت‌گیرانه‌ای در زمینه فیلترینگ اعمال می‌کند، از یک سیستم پیشرفته به نام "دیوار آتش بزرگ" استفاده می‌کند. این سیستم به دولت اجازه می‌دهد تا دسترسی به اکثر پلتفرم‌های بین‌المللی مانند گوگل، یوتیوب، فیس‌بوک و توییتر را مسدود کرده و کاربران را به استفاده از پلتفرم‌های داخلی مانند بایدو و وی‌چت سوق دهد. این رویکرد بخشی از تلاش دولت چین برای کنترل کامل بر فضای مجازی و جلوگیری از نفوذ فرهنگی و سیاسی خارجی است. دولت چین از ابزارهای فناوری پیشرفته مانند هوش مصنوعی و الگوریتم‌های یادگیری ماشینی برای نظارت و مسدودسازی محتوا استفاده می‌کند. این ابزارها به‌طور خودکار محتوای حساس یا مخالف را شناسایی و حذف می‌کنند. علاوه بر این، چین قوانین سخت‌گیرانه‌ای وضع کرده که استفاده از ابزارهای دور زدن فیلتر (VPN) را جرم‌انگاری می‌کند و افراد یا شرکت‌هایی که این قوانین را نقض کنند با مجازات‌های سنگین مواجه می‌شوند (Soleimani, 2018). با وجود موفقیت‌های چین در ایجاد یک اینترنت داخلی قوی، این سیاست‌ها انتقادات گسترده‌ای را به دنبال داشته است. محدودیت‌های شدید دسترسی به اطلاعات باعث شده تا آزادی بیان به‌شدت محدود شود و کاربران از دسترسی به منابع متنوع بین‌المللی محروم شوند. این محدودیت‌ها همچنین به مشکلات اقتصادی منجر شده، زیرا شرکت‌های بین‌المللی از فعالیت در چین بازداشته می‌شوند و کسب‌وکارهای داخلی نیز از رقابت جهانی بازمی‌مانند. در عین حال، این سیاست‌ها توانسته‌اند از نظر دولت چین، امنیت و ثبات سیاسی را تضمین کنند و به کنترل اطلاعات در سطح ملی کمک کنند. سیاست‌های فیلترینگ

چین نمونه‌ای از اولویت‌دهی به کنترل اجتماعی و امنیت بر آزادی‌های فردی است (Mishra, 2021).

۲.۱.۵.۳. مدل سنگاپور: تعادل میان قانون و فناوری

سنگاپور یکی از کشورهایی است که رویکرد متعادلی به فیلترینگ اتخاذ کرده است. برخلاف چین، در سنگاپور کاربران به اکثر پلتفرم‌های بین‌المللی مانند یوتیوب، گوگل و توییتر دسترسی دارند، اما دولت به‌طور خاص محتواهایی را که تهدیدی برای نظم عمومی، اخلاقیات یا امنیت ملی محسوب می‌شوند، مسدود می‌کند. یکی از ویژگی‌های کلیدی سیاست‌های سنگاپور، شفافیت در قوانین و مقررات مربوط به فضای مجازی است. دولت سنگاپور لیستی از محتوای غیرقانونی یا نامناسب را منتشر می‌کند و کاربران را از قوانین موجود آگاه می‌سازد. این رویکرد، علاوه بر حفظ آزادی بیان، اعتماد عمومی را به سیاست‌های دولت افزایش داده است. از منظر فناوری، سنگاپور از ابزارهای هوشمند برای مدیریت محتوا استفاده می‌کند، اما این ابزارها عمدتاً به‌عنوان ابزاری حمایتی به کار می‌روند و نه نظارتی. همچنین، دولت سنگاپور برنامه‌های متعددی برای ارتقای سواد دیجیتال و افزایش آگاهی کاربران نسبت به خطرات فضای مجازی اجرا می‌کند. این برنامه‌ها شامل دوره‌های آموزشی، کارگاه‌های آگاهی‌بخشی و ارائه منابع آموزشی آنلاین است که هدف آن‌ها افزایش توانایی کاربران در تشخیص اطلاعات صحیح از نادرست و محافظت از خود در برابر تهدیدات آنلاین است. سنگاپور تلاش کرده است تا تعادل میان حقوق شهروندی و الزامات امنیتی را حفظ کند. این مدل، برخلاف سیاست‌های سخت‌گیرانه چین، بر مشارکت کاربران و ایجاد اعتماد اجتماعی استوار است و توانسته است محیطی پایدار و قابل اعتماد برای فعالیت‌های آنلاین فراهم کند (Hashemi et al., 2021).

۲.۵.۳. مقایسه با سیاست‌های فیلترینگ در ایران

سیاست‌های فیلترینگ در ایران، به‌ویژه در سال‌های اخیر، بیشتر شبیه به مدل سخت‌گیرانه چین بوده است، اما با تفاوت‌هایی از نظر

فیلترینگ را مشخص کنند، ضروری است. این قوانین باید به گونه‌ای طراحی شوند که تضمین‌کننده حقوق شهروندان در زمینه دسترسی به اطلاعات و آزادی بیان باشند و در عین حال امنیت ملی را حفظ کنند. به عنوان نمونه، قوانینی که دولت‌ها را ملزم می‌کند قبل از اعمال هرگونه محدودیت، دلایل فنی و حقوقی آن را اعلام کرده و تأیید نهادهای مستقل را دریافت کنند، می‌تواند از سوءاستفاده جلوگیری کند. همچنین، سازوکارهای مشخصی برای اعتراض کاربران به تصمیمات فیلترینگ باید پیش‌بینی شود تا افرادی که احساس می‌کنند حقوقشان نقض شده است، بتوانند درخواست بازنگری ارائه کنند. یکی از راه‌های مؤثر در این زمینه، ایجاد نهادهای نظارتی مستقل است که به صورت شفاف و بی‌طرفانه عملکرد دولت در زمینه فیلترینگ را ارزیابی کرده و از اعمال محدودیت‌های گسترده و غیرضروری جلوگیری کنند. این نهادها می‌توانند نمایندگان دولت، جامعه مدنی، و متخصصان حوزه فناوری اطلاعات را شامل شوند. علاوه بر این، قوانین باید به گونه‌ای تدوین شوند که تناسب میان میزان محدودیت و شدت تهدید را تضمین کنند. برای مثال، مسدودسازی کامل یک پلتفرم فقط در شرایطی مجاز باشد که تهدیدی جدی برای امنیت ملی وجود داشته باشد و ابزارهای دیگر ناکارآمد باشند. در نهایت، ایجاد سازوکارهایی برای ارائه گزارش‌های دوره‌ای درباره عملکرد فیلترینگ و پیامدهای آن به جامعه، می‌تواند اعتماد عمومی را تقویت کند و شفافیت بیشتری در سیاست‌گذاری‌ها به وجود آور

(Khan Mohammadi & Shameli, 2016).

۲.۶.۳. استفاده از فناوری‌های جایگزین برای کنترل محتوا

به جای استفاده از روش‌های گسترده و ناکارآمد مسدودسازی پلتفرم‌ها، بهره‌گیری از فناوری‌های پیشرفته و جایگزین می‌تواند راهکار مؤثرتری برای مدیریت محتوای نامناسب باشد. استفاده از هوش مصنوعی و یادگیری ماشینی برای شناسایی محتوای مضر یا غیرقانونی، به دولت‌ها اجازه می‌دهد تا به طور هدفمند تنها محتوای

ابزارها و نتایج. بسیاری از پلتفرم‌های بین‌المللی مانند فیس‌بوک، توئیتر و تلگرام در ایران مسدود شده‌اند و کاربران مجبور به استفاده از شبکه‌های داخلی یا ابزارهای دور زدن فیلتر مانند VPN شده‌اند. با این حال، برخلاف چین که جایگزین‌های داخلی قدرتمندی ایجاد کرده است، پلتفرم‌های داخلی ایران معمولاً از نظر قابلیت‌ها و کیفیت پایین‌تر هستند و نتوانسته‌اند اعتماد کاربران را جلب کنند. این مسئله باعث شده است که بسیاری از کاربران همچنان به استفاده از ابزارهای غیرقانونی برای دسترسی به محتوای خارجی ادامه دهند. یکی دیگر از تفاوت‌های کلیدی، شفافیت قوانین است (Mirzaei et al., 2019). در حالی که سنگاپور قوانین مشخص و شفافی برای مدیریت محتوا دارد، در ایران سیاست‌های فیلترینگ غالباً به صورت ناگهانی و بدون اطلاع‌رسانی قبلی اجرا می‌شوند. این عدم شفافیت باعث کاهش اعتماد عمومی به دولت و افزایش نارضایتی کاربران شده است. همچنین، برخلاف سنگاپور که برنامه‌های سواد دیجیتال را اجرا می‌کند، در ایران تمرکز بیشتر بر ابزارهای نظارتی و امنیتی است و به ارتقای آگاهی کاربران توجه کمتری شده است. از نظر اقتصادی، سیاست‌های فیلترینگ در ایران، مانند چین، بر کسب‌وکارهای آنلاین تأثیر منفی گذاشته و بسیاری از مشاغل کوچک و متوسط را با چالش‌های جدی مواجه کرده است. این مقایسه نشان می‌دهد که سیاست‌های ایران می‌توانند از مدل متعادل‌تر سنگاپور الهام بگیرند، تا تعادل بهتری میان امنیت و آزادی‌های شهروندی برقرار شود (Esmailpour, Moghadam, 2023).

۶.۳. راهبردهای عملی و سیاست‌گذاری برای بهبود مدیریت فضای مجازی

۱.۶.۳. راهکارهای حقوقی برای کاهش تعارض میان امنیت و حریم خصوصی

برای ایجاد تعادل میان امنیت و حریم خصوصی، تدوین قوانین شفاف و جامع که به وضوح معیارها، حدود و شرایط اعمال

مشکل ساز را حذف کنند، بدون آن که دسترسی به کل پلتفرم محدود شود. این فناوری‌ها قابلیت تجزیه و تحلیل داده‌های عظیم را دارند و می‌توانند محتوای مخرب را با دقت بالایی شناسایی کنند. برای مثال، الگوریتم‌هایی که قادر به شناسایی سخنان نفرت‌پراکن، خشونت، یا انتشار اطلاعات نادرست هستند، می‌توانند با حذف هدفمند این محتوا، به جای فیلتر کامل، تعادل بهتری ایجاد کنند. همچنین، استفاده از فناوری‌های رمزنگاری می‌تواند نقش مهمی در حفاظت از داده‌های کاربران داشته باشد. این فناوری‌ها می‌توانند به کاربران اطمینان دهند که داده‌های شخصی آن‌ها حتی در صورت نظارت دولتی، از دسترس نهادهای غیرمجاز در امان است. علاوه بر این، همکاری میان دولت‌ها و شرکت‌های بین‌المللی برای مدیریت محتوا می‌تواند جایگزینی مناسب برای فیلترینگ یک‌جانبه باشد. این همکاری‌ها به دولت اجازه می‌دهد تا درخواست حذف محتوای خاص را به شرکت‌های پلتفرمی ارائه داده و این درخواست‌ها با شفافیت بررسی شود. چنین رویکردی از مسدودسازی کل پلتفرم جلوگیری کرده و تأثیرات منفی آن بر کاربران و کسب‌وکارها را کاهش می‌دهد. در نهایت، این روش‌ها می‌توانند به کاهش نارضایتی عمومی و افزایش کارایی سیاست‌های نظارتی کمک کنند (Eftadeh, 2013).

۳.۶.۳. نقش دولت در شفاف‌سازی سیاست‌های فیلترینگ

شفافیت در سیاست‌های فیلترینگ، عامل کلیدی در ایجاد اعتماد میان دولت و شهروندان است. دولت‌ها باید به‌طور علنی اهداف و دلایل فیلترینگ را اعلام کنند تا از انتشار شایعات و سوءتفاهم‌ها جلوگیری شود. یکی از روش‌های افزایش شفافیت، انتشار لیست سایت‌ها یا پلتفرم‌هایی است که مسدود شده‌اند، همراه با توضیحات دقیق درباره دلایل مسدودسازی. این شفاف‌سازی باید به گونه‌ای انجام شود که شهروندان مطمئن باشند محدودیت‌ها تنها در شرایط ضروری و بر اساس دلایل منطقی اعمال می‌شوند. دولت‌ها می‌توانند با تشکیل نهادهای مستقل نظارتی که شامل

نمایندگان جامعه مدنی، متخصصان فناوری و دولت باشند، نظارت بر سیاست‌های فیلترینگ را تضمین کنند. این نهادها باید قادر باشند تا عملکرد دولت را در این زمینه ارزیابی کرده و در صورت مشاهده نقض حقوق کاربران، اقدامات اصلاحی را پیشنهاد دهند. علاوه بر این، شفافیت می‌تواند از طریق آموزش و اطلاع‌رسانی عمومی تقویت شود. دولت‌ها باید با برگزاری کمپین‌های آگاهی‌بخشی و ارائه اطلاعات دقیق درباره سیاست‌های فیلترینگ، به شهروندان کمک کنند تا درک بهتری از این سیاست‌ها داشته باشند. همچنین، ارائه گزارش‌های دوره‌ای درباره عملکرد فیلترینگ و پیامدهای آن می‌تواند به افزایش اعتماد عمومی کمک کند. این گزارش‌ها باید شامل اطلاعاتی درباره میزان محتوای مسدود شده، دلایل مسدودسازی، و پیامدهای آن بر کاربران و کسب‌وکارها باشد. در نهایت، شفاف‌سازی سیاست‌های فیلترینگ نه تنها به بهبود تعامل میان دولت و شهروندان کمک می‌کند، بلکه زمینه را برای اعمال سیاست‌های مؤثرتر و عادلانه‌تر فراهم می‌سازد (Rahimi et al., 2021).

نتیجه‌گیری

فضای مجازی به‌عنوان یکی از مهم‌ترین دستاوردهای فناوری در دنیای امروز، نقش کلیدی در زندگی اجتماعی، اقتصادی و فرهنگی افراد ایفا می‌کند. با این حال، چالش‌هایی نظیر فیلترینگ و تأثیر آن بر حقوق بنیادین کاربران، از جمله حریم خصوصی، آزادی بیان و دسترسی به اطلاعات، موضوعی است که نیازمند بررسی دقیق و سیاست‌گذاری هوشمندانه است. این مقاله با هدف ارزیابی تأثیرات فیلترینگ بر حریم خصوصی کاربران، به تحلیل ابعاد حقوقی، فقهی و عملی این مسئله پرداخته است. روش تحقیق بر پایه تحلیل مبانی نظری و بررسی تطبیقی سیاست‌های فیلترینگ در کشورهای مختلف بوده است. یافته‌ها نشان می‌دهند که سیاست‌های فیلترینگ، در صورت عدم شفافیت و رعایت اصول عدالت و تناسب، می‌توانند حقوق اساسی کاربران را به شدت نقض کرده و

خصوصی و آزادی‌های فردی بنا شود، به گونه‌ای که کاربران بتوانند با اطمینان از ایمنی و رعایت حقوق خود، از این بستر بهره‌مند شوند. دستیابی به این هدف نیازمند سیاست‌گذاری هوشمندانه، تعامل مستمر با کاربران و استفاده از ظرفیت‌های فناوری است. در نهایت پیشنهادات زیر ارائه می‌گردد:

- تحلیل تأثیرات روان‌شناختی فیلترینگ بر رفتار کاربران فضای مجازی
- تأثیر فیلترینگ بر نوآوری و توسعه اقتصاد دیجیتال
- نقش هوش مصنوعی در مدیریت محتوا و حفظ حریم خصوصی کاربران
- ارزیابی دیدگاه‌های عمومی نسبت به سیاست‌های فیلترینگ در کشورهای مختلف

مشارکت نویسندگان

در نگارش این مقاله تمامی نویسندگان نقش یکسانی ایفا کردند.

تعارض منافع

در انجام مطالعه حاضر، هیچ گونه تضاد منافی وجود ندارد.

EXTENDED ABSTRACT

Cyberspace has become an inseparable element of contemporary human life, interwoven with social interactions, economic systems, and political engagement. The rapid expansion of the internet has democratized access to knowledge, empowered marginalized voices, and enabled transnational connectivity. However, with this growth, states have increasingly exercised control over digital content through filtering policies—ostensibly justified by national security, public morality, or protection of minors. Yet, the exercise of filtering, when lacking transparency and grounded principles, may infringe upon fundamental human rights, most notably the right to privacy. As one of the cornerstones of individual autonomy, privacy ensures the protection of personal data and provides

پیامدهای اجتماعی، فرهنگی و اقتصادی جدی به همراه داشته باشند. برای مثال، محدودسازی گسترده محتوا بدون ارائه جایگزین‌های مؤثر، باعث کاهش اعتماد عمومی، محدودیت در کسب و کارهای آنلاین، و تضعیف مشارکت سیاسی و اجتماعی می‌شود. تحلیل مبانی فقهی نیز نشان داد که اصولی مانند قاعده "لاضرر"، کرامت انسانی و قاعده تسبیب می‌تواند راهنمایی ارزشمند برای تبیین مسئولیت دولت در قبال کاربران فضای مجازی باشند. در سطح تطبیقی، بررسی سیاست‌های فیلترینگ در کشورهایی مانند چین و سنگاپور نشان داد که تعادل میان امنیت و آزادی‌های کاربران، در صورتی که قوانین شفاف و فناوری‌های پیشرفته به کار گرفته شوند، امکان‌پذیر است. بنابراین، لازم است دولت‌ها با تدوین قوانین شفاف، نظارت مستقل و بهره‌گیری از فناوری‌های جایگزین، تعادلی میان حفظ امنیت ملی و رعایت حقوق شهروندی برقرار کنند. تقویت آموزش عمومی و ارتقای سواد دیجیتال، در کنار شفاف‌سازی سیاست‌ها، می‌تواند اعتماد کاربران به مدیریت فضای مجازی را افزایش دهد. در نهایت، چشم‌انداز فضای مجازی باید بر پایه تعادل میان امنیت، حریم

individuals with control over their personal spheres. In the digital domain, privacy encompasses a spectrum of concerns ranging from data surveillance and algorithmic profiling to state censorship. Filtering mechanisms, particularly when applied arbitrarily or discriminatorily, often erode this right by enabling intrusive monitoring, limiting informational self-determination, and disrupting access to verified data sources (Alimoradi, 2022; Liu et al., 2020). Further complicating this terrain is the dual responsibility of governments—to guarantee national cybersecurity while upholding citizen rights. From a legal-philosophical lens, Islamic jurisprudence and universal human rights frameworks converge on principles such as "La Darar" (no harm), the dignity of the individual, and accountability in policy

implementation, establishing robust theoretical anchors for assessing filtering policies (Hossein Nejad & Moniri Hamzeh Kolai, 2017; Tashev, 2024). The current study delves into the multidimensional effects of internet filtering on user privacy by combining legal interpretation, jurisprudential doctrines, and comparative analyses with China, Singapore, and Iran as case illustrations.

The jurisprudential and legal literature underscores the gravity of filtering as a tool with socio-political ramifications. Prior studies have scrutinized the role of filtering in balancing state authority and civil liberties, often spotlighting its double-edged consequences. For instance, research has shown that governments invoking filtering under the pretext of national interest often sidestep legal thresholds of necessity and proportionality, undermining public trust and generating unintended harms to digital economies (Bidarvand et al., 2021). Islamic jurisprudence—specifically the “La Darar” principle—prohibits unjustified harm, which applies poignantly to indiscriminate filtering that causes widespread socio-economic damage. Similarly, the principle of “tasbib” (causation) implies that governments are liable for damages inflicted on digital enterprises due to poor content regulation frameworks (Mohammadi Nia & Karamati Moaz, 2024). Moreover, domestic regulations like Iran’s Cybercrime Law grant sweeping authority to state entities with insufficient oversight, increasing the risk of rights violations (Rahmani et al., 2023). In contrast, normative international instruments such as the Universal Declaration of Human Rights (Article 19) and the European Convention on Human Rights (Article 10) advocate for minimal restrictions on freedom of expression and access to information, promoting only narrowly tailored interventions. Hence, filtering policies must be subjected to rigorous legality, legitimacy, and necessity standards.

Legal ambiguities and lack of procedural transparency, as found in multiple jurisdictions, often lead to the misuse of filtering tools, resulting in disproportionate harm to user privacy, democratic participation, and access to critical knowledge sources (Elyasi et al., 2022; Ramak et al., 2019). Conceptually, filtering is not monolithic but exists in both technical and legal forms. Technological filtering involves firewalls, proxy servers, and deep packet inspection, while legal filtering entails statutory frameworks and regulatory decrees. The latter carries profound implications for digital rights, especially when applied without procedural safeguards or public deliberation (Nasrollahi, 2023). The jurisprudential notion of “harim al-mu’min” (the believer’s sanctuary) reinforces the sacredness of private communication, extending it to the digital environment where mass data collection and content suppression can constitute spiritual and psychological transgressions (Vali Asl, 2024). Privacy in cyberspace is also essential for preserving identity integrity, political participation, and digital autonomy. Tools such as artificial intelligence and Internet-of-Things (IoT) technologies, while offering personalized services, also carry surveillance potential that can be exacerbated by filtering protocols (Ghanad & Aliqoli, 2020; Hejazi Nia, 2015). In examining the intersection of privacy and filtering, the study emphasizes that privacy should not be perceived solely as an individual entitlement but as a collective social good that fosters trust, innovation, and inclusive development. Filtering policies that disregard this dimension risk not only violating user rights but also stifling the growth of digital economies and the flourishing of online civil societies.

Empirical illustrations of filtering policies in practice reveal varied trajectories. China’s “Great Firewall” epitomizes a centralized and rigid system that prioritizes national cohesion

and ideological conformity over civil liberties. The Chinese model, while technologically sophisticated, criminalizes VPN use, restricts foreign platforms, and exerts granular control over digital narratives. These efforts have created a parallel internet insulated from global influence but also isolated from diverse knowledge systems (Mishra, 2021; Soleimani, 2018). Conversely, Singapore offers a more balanced model where targeted content regulation is combined with digital literacy programs and transparent guidelines. Singapore's filtering system allows access to most global platforms but intervenes selectively where content contravenes clearly defined societal norms or security interests. This model, by reinforcing procedural clarity and stakeholder engagement, has fostered greater public trust (Hashemi et al., 2021). Iran, while drawing structurally from the Chinese approach, faces challenges in policy implementation due to weaker technological alternatives and lower public compliance. Many Iranian users resort to VPNs to bypass censorship, reflecting a lack of confidence in state-sanctioned platforms (Esmailpour Moghadam, 2023; Mirzaei et al., 2019). Moreover, filtering in Iran often occurs abruptly and without public notice, intensifying user dissatisfaction and economic disruption. In contrast, policy models emphasizing transparency, legal predictability, and technological cooperation—such as Singapore's—demonstrate the feasibility of reconciling content governance with rights protection. Comparative findings thus highlight that the legitimacy and effectiveness of filtering are not solely determined by technical prowess but by the embeddedness of democratic norms, participatory mechanisms, and technological openness.

The consequences of filtering on users' privacy and broader digital ecosystems extend beyond legal abstractions to practical disruptions in

social, cultural, and economic life. On the sociocultural front, filtering reduces exposure to global perspectives, curtails youth engagement in transnational discourse, and fosters informational homogeneity, ultimately weakening cognitive diversity and innovation potential (Zaroudi & Borzoui, 2022). Psychologically, persistent filtering can induce feelings of alienation, especially among younger demographics reliant on online platforms for identity expression and community-building. Economically, filtering acts as a structural impediment to digital entrepreneurship, particularly affecting small and medium enterprises (SMEs) dependent on global platforms for outreach, customer interaction, and logistics. These businesses often lack the financial capacity to migrate to costly alternatives or build proprietary platforms, rendering them vulnerable to market exclusion and reduced competitiveness (Rahmani et al., 2023). The economic fallout includes not only revenue losses but also barriers to foreign investment, as international firms prefer predictable and open regulatory environments. Furthermore, filtering compromises the integrity of information flows by narrowing access to diverse content, undermining informed decision-making, civic engagement, and press freedom. Over time, these limitations create epistemic enclaves where users are either uninformed or misinformed, contributing to political polarization, authoritarian resilience, and social stagnation (Asadzadeh & Seyed Mousavi, 2015). The cumulative result is a digitally fragmented society marked by mistrust, inefficiency, and rights suppression—conditions that demand urgent policy recalibration.

To mitigate the adverse effects of filtering while preserving legitimate security objectives, strategic policy and technological interventions are imperative. Firstly, legal reforms should prioritize clarity, necessity,

and proportionality—codifying when, how, and by whom filtering can be applied, subject to independent judicial oversight. Laws should mandate impact assessments prior to implementation and allow user appeals for wrongful restrictions (Khan Mohammadi & Shameli, 2016). Secondly, the deployment of artificial intelligence and big data analytics can offer targeted content moderation solutions, reducing the need for blanket bans. These tools can filter harmful content with minimal infringement on lawful speech, especially when designed with algorithmic transparency and bias mitigation. Additionally, partnerships between states and global tech companies can institutionalize content review mechanisms that align with both domestic values and international rights standards (Eftadeh, 2013). Thirdly, governments must invest in digital literacy and public education programs that empower users to navigate, assess, and respond to online risks without overreliance on state intervention. Transparency in listing blocked sites, publishing annual filtering reports, and establishing ombudspersons for digital grievances can further enhance accountability and civic trust (Rahimi et al., 2021). Ultimately, a multi-stakeholder governance model—incorporating civil society, academia, private tech actors, and regulatory bodies—offers the most sustainable path toward equitable cyberspace regulation. Such a model ensures that privacy, freedom of expression, and cybersecurity are not framed in binary opposition but managed as interdependent facets of democratic digital governance. In conclusion, the intersection of internet filtering and user privacy presents a complex legal, technological, and moral challenge for modern governance systems. While national security, cultural protection, and public order are legitimate policy goals, their pursuit must not eclipse foundational human rights. Filtering, when overextended or non-

transparent, risks violating privacy, distorting public discourse, and eroding digital trust. Comparative evidence from China, Singapore, and Iran underscores that the design and implementation of filtering policies must align with jurisprudential ethics, international norms, and local contextual realities. Effective policy requires a fine balance—leveraging advanced technologies and clear legislation to protect users without silencing them. Only through such integrated and transparent approaches can states foster a cyberspace that is both secure and respectful of human dignity, thereby nurturing democratic resilience in the digital age.

References

- Alimoradi, M. (2022). Supervision of Cyberspace and User Privacy. *Raha-e-Noor*, 80, 40-49.
- Asadzadeh, A., & Seyed Mousavi, M. S. (2015). The Law on Publication and Free Access to Information and Its Role in Developing Freedom of Access and Information Dissemination. First International Conference on Humanities with a Native-Islamic Approach and Emphasis on New Research,
- Behbood, P., & Mobin, H. (2023). Protecting Property Rights of Virtual Game Users Based on the Rule of No Harm. *Journal of Contract Law and Modern Technologies*, 1, 135-148.
- Beigi, J. (2018). Strategies for Preventing Violations of Citizen Rights in Cyberspace. *Science and Advocacy*, 11, 39-57.
- Bidarvand, M., Pour Gahramani, B., & Beigi, J. (2021). Telegram Filtering: From National Security Necessity to Violation of Freedom of Expression. *Islamic Jurisprudence and Legal Foundations*, 4SP - 29, 48.
- Derikvand, Z., & Jafari, M. (2023). Examining Principles, Foundations, and Types of Filtering in Cyberspace to Prevent Crime and Immorality. *Journal of New Approaches in Islamic Studies*, 15, 199-224.
- Eftadeh, J. (2013). Alternative Solutions to Filtering Social Media. *Communication Management*, 10, 44-73.
<https://doi.org/10.1097/01.NUMA.0000427191.36468.65>
- Elyasi, B., Sadeghi, M., Dastaranj, N., Hosseinpour, M., & Mirsaeed Ghazi, T. (2022). Policy-Making for Access to Open Data in Iran from the Perspective of Privacy Protection and Personal Data Ownership. *Iranian Information and Communication Technology*, 51, 17-34.

- Esmailpour Moghadam, H. (2023). Data Mining in Iran's Stock Market Using Complex Network Filtering Modeling: MST Approach. *Financial Economics*, 62, 239-252.
- Ghanad, F., & Aliqoli, A. (2020). The Concept and Importance of Personal Data and Privacy and Types of Protection in Cyberspace. *Journal of Contract Law and Modern Technologies*, 15, 297-322.
- Hashemi, S. M., Mohseni, V., Javid, M. J., & Abbasi, B. (2021). Legal Analysis and Assessment of Citizen Rights Guarantees with Filtering. *Judicial Legal Perspectives*, 94, 94-115.
- Hejazi Nia, R. (2015). Examining the Importance of Privacy Protection in Cyberspace from the Perspective of Islam. Second International Conference on Iranian-Islamic Economy, Management, and Culture,
- Hossein Nejad, S. M., & Moniri Hamzeh Kolai, H. (2017). Jurisprudential Analysis of Filtering Implementation in Cyberspace. *Islamic Government*, 17, 27-35.
- Khan Mohammadi, K., & Shameli, A. A. (2016). Ethical Conflict Between Privacy Respect and User Security in Cyber Social Networks and Providing Solutions. *Religion and Cultural Politics*, 8, 75-94.
- Liang, W., Xie, S., Cai, J. A. U. X. J., Hu, Y., Xu, Y., & Qiu, M. (2021). Deep neural network security collaborative filtering scheme for service recommendation in intelligent cyber-physical systems. *Ieee Internet of Things Journal*, 9(22), 22123-22132.
<https://doi.org/10.1109/JIOT.2021.3086845>
- Liu, J., Wang, Y., Cao, J., Yue, D., & Xie, X. (2020). Secure adaptive-event-triggered filter design with input constraint and hybrid cyber attack. *IEEE Transactions on Cybernetics*, 51(8), 4000-4010.
<https://doi.org/10.1109/TCYB.2020.3003752>
- Mirzaei, V., Vatani, A., & Abbasi Sarmadi, M. (2019). Ethical Structure in the Limits of Information Freedom and Filtering in Iran. *Ethical Research*, 12, 265-276.
- Mishra, N. (2021). Breaking Down Digital Walls: The Interface of International Trade Law and Online Content Regulation through the Lens of the Chinese VPN Measure. *Brook. J. Int'l L.*, 47SP - 359. <https://doi.org/10.2139/ssrn.4036902>
- Mohammadi Nia, O., & Karamati Moaz, H. (2024). Jurisprudential and Legal Foundations of State Civil Liability Regarding Filtering (Censorship) of Virtual Social Networks. *Comparative Research in Jurisprudence, Law, and Politics*, 6(4), 223-238. <https://doi.org/10.61838/csjpg.6.4.14>
- Mohammadi, Z., Delsouz, K., & Sayyah, E. (2019). Filtering Social Networks and Its Role in Protecting and Securing Citizen Rights in Cyber Defense in Iran. Second National Conference on Cyber Defense,
- Moradi, M., Dadashi, M. M., & Ashna, H. (2019). Investigating Violations of User Privacy in Cyberspace from the Perspective of Iranian Criminal Law. Second National Conference on Cyber Defense,
- Nasrollahi, M. S. (2023). Historical-Legal Analysis of Cyberspace Filtering Regulations in Iran. *Journal of Media Jurisprudence and Law Studies*, 1, 61-93.
- Ogungbemi, O. S. A. U. E. F. A., Olaniyi, O. O., Akinola, O. I., & Oladoyinbo, O. B. (2024). Overcoming remote workforce cyber threats: A comprehensive ransomware and bot net defense strategy utilizing VPN networks.
<https://doi.org/10.2139/ssrn.4911878>
- Rahimi, S., Soheili, F., Mahdipour, R., Rahimi, F., & Soheili Moghadam, S. M. (2021). The Status of Privacy Protection for Users in Cyberspace: A Case Study of Public Library Librarians in Ilam Province. State Sovereignty Over Cyberspace: A Case Study of Saudi Arabia's Approach to Opponents. *Human-Information Interaction*, 3, 57-72.
- Rahmani, N., Vahabzadeh Manshi, S., & Mehrani, H. (2023). Designing a Local Digital Marketing Model for Small Online Retail Businesses in Iran. *Entrepreneurship Development VL - 1*, 109-120.
- Ramak, M., Velavi, M., & Hosseini, M. (2019). Research Article: Providing a Strategic Model for International Cooperation to Enhance Cybersecurity Based on National Interests of the Islamic Republic of Iran and Combating Cybercrimes. *National Security*, 33, 273-314.
- Sadeghi, H., & Ghasemi, A. (2022). State Civil Liability Regarding Filtering (Censorship) with a View to Foreign Laws and International Human Rights Documents. *Public Law Thoughts*, 1, 69-80.
- Soleimani, M. (2018). Threats and Opportunities of Filtering: How China Implements Filtering. *Communication Management*, 58, 28-36.
- Tashev, S. N. (2024). PACKET FILTERING TECHNIQUES FOR NETWORK SECURITY. Next Scientists Conferences,
- Vali Asl, A. (2024). Resolving the Conflict Between the Principles of Privacy Respect and Information Dissemination. *Ethics*, 4, 221-251.
- Zaroudi, A., & Borzoui, M. R. (2022). Potential Impacts of Cyberspace on Social Sacrifice. *Letter of Culture and Communication*, 1, 35EP - 70.