مجله علمی مطالعات پژوهشی در حقوق آینده، ۱۴۰۵، دوره ۴، شماره ۱، ص ص ۹-۱۶

مجله علمی مطالعات پژوهشی

در حقوق آینده

www.journalhi.com/law/

حاکمیت سایبری و نقش دولت‌ها در توازن میان آزادی‌های فردی و الزامات امنیت ملی در فضای مجازی

مریم چشم نیام [۱،*]

۱- دانشجوی دکتری حقوق عمومی، دانشکده حقوق، دانشگاه آزاد اسلامی واحد تهران مرکز، تهران، ایران. ایمیل: maryam.chashmniam@iau.ir

* نویسنده مسئول

چکیده

هدف: این پژوهش به واکاوی چالش تعارض میان امنیت ملی و آزادی‌های فردی در بستر حاکمیت سایبری می‌پردازد. مسئله اصلی، مواجهه دولت‌ها با پارادوکسی دوگانه میان ضرورت صیانت از مرزهای دیجیتال در برابر تهدیدات نوین و الزام به حفظ حقوق بنیادین، حریم خصوصی و آزادی‌های شهروندان است. هدف تحقیق، ارائه چارچوبی تحلیلی برای سیاست‌گذاری متوازن در حکمرانی سایبری است تا ضمن حفظ اقتدار امنیتی، از لغزش به سوی اقتدارگرایی دیجیتال جلوگیری شود.

روش: این مطالعه با رویکرد کیفی و به روش اسنادی و تحلیلی-تطبیقی انجام شده است. در این پژوهش با تحلیل انتقادی منابع حقوقی، اسناد سیاستی و تجربه‌های بین‌المللی، نسبت میان سیاست‌های امنیتی و تضمین‌های حقوق بشری ارزیابی گردیده است. چارچوب نظری پژوهش بر پایه نظریه‌های حکمرانی شبکه‌ای و رویکرد چندجانبه‌گرایی استوار است؛ تا راهکارهایی فراتر از دیدگاه‌های سنتی دولت‌محور، برای مدیریت تعاملات فضای مجازی ارائه دهد.

یافته‌ها: یافته‌های پژوهش نشان می‌دهد، که حکمرانی سایبری موفق مستلزم عبور از تقابل صفر و یک میان امنیت و آزادی است. دستیابی به این هدف مستلزم تلفیق رویکردهای مختلف از جمله استقرار نظام‌های شفافیت و پاسخ‌گویی دولت‌ها در اقدامات امنیتی، بهره‌گیری از سازوکارهای حقوقی و فنی برای تحدید موجه آزادی‌ها بر پایه اصول تناسب و ضرورت تحت نظارت قضایی و در نهایت گذار به مدل حکمرانی مشارکتی میان دولت‌ها، بخش خصوصی و جامعه مدنی است. همچنین نتایج نشان می‌دهد که تمرکز بیش از حد بر ابزارهای کنترلی بدون لحاظ پیوست‌های حقوقی، منجر به فرسایش سرمایه اجتماعی می‌گردد.

نتیجه‌گیری: برقراری توازن میان کنترل و آزادی، ضرورتی برای بقای مشروعیت حکمرانی در عصر دیجیتال است. تأمین امنیت ملی بدون توجه به حقوق فردی، در بلندمدت با ایجاد بی‌اعتمادی اجتماعی، خود به تهدیدی برای ثبات سیاسی بدل می‌گردد. حکمرانی موفق سایبری مستلزم نهادینه کردن «نظارت مستمر» و «مشارکت‌پذیری» است.

کلمات کلیدی: آزادی‌های فردی، امنیت ملی، حاکمیت سایبری، حکمرانی دیجیتال، فضای مجازی

Cyber Sovereignty and the Role of States in Balancing Individual Liberties and National Security Imperatives in Cyberspace

Maryam chashmniam [1,*]

1- Ph.D. Candidate in Public Law, Faculty of Law, Islamic Azad University, Central Tehran Branch, Tehran, Iran. Email: maryam.chashmniam@iau.ir

* Corresponding Author

Abstract

Objective: This research examines the conflict between national security and individual liberties within the context of cyber sovereignty. The core issue is the paradox faced by states in balancing the necessity of protecting digital borders against emerging cyber threats with the obligation to uphold fundamental rights, privacy, and civil liberties. The study aims to provide an analytical framework for balanced policymaking in cyber governance to maintain security authority while preventing a slide toward digital authoritarianism.

Methods: Employing a qualitative approach, this study utilizes documentary and comparative-analytical methods. Through a critical analysis of legal sources, policy documents, and international experiences, the relationship between security policies and human rights guarantees is evaluated. The theoretical framework is grounded in network governance theories and multi-stakeholderism to propose solutions beyond traditional state-centric perspectives.
Findings: The research findings indicate that successful cyber governance necessitates moving beyond the binary "security vs. liberty" paradigm. Achieving this objective requires the integration of various approaches, including the establishment of systems for transparency and state accountability in security measures, the utilization of legal and technical mechanisms for the "just limitation" of freedoms based on the principles of proportionality and necessity under judicial oversight, and finally, the transition toward a participatory governance model among states, the private sector, and civil society. Furthermore, the results demonstrate that an excessive focus on control tools, without considering legal safeguards, leads to the erosion of social capital.
Conclusion: Establishing a balance between control and liberty is an existential necessity for the legitimacy of governance in the digital age. Ensuring national security without regard for individual rights becomes, in the long term, a threat to political stability by generating social distrust. Successful cyber governance necessitates the institutionalization of "continuous oversight" and "participatory engagement.
Keywords: Individual Liberties, National Security, Cyber Sovereignty, Digital Governance, Cyberspace

مقدمه

گسترش پرشتاب فناوری‌های ارتباطی و اطلاعاتی در دهه‌های اخیر، مرزهای سنتی حاکمیت ملی را با چالش‌های تازه‌ای مواجه ساخته است. فضای مجازی امروز نه تنها عرصه‌ای برای تبادل اطلاعات، توسعه اقتصادی و گسترش آزادی‌های فردی به شمار می‌رود، بلکه بستری برای بروز تهدیدات نوین علیه امنیت ملی نیز محسوب می‌شود. این وضعیت سبب شده است که مفهوم «حاکمیت سایبری» به یکی از موضوعات کلیدی در حوزه حکمرانی معاصر بدل گردد. دولت‌ها در مواجهه با این فضا ناگزیر از اتخاذ سیاست‌هایی هستند که دو هدف ظاهراً متعارض را همزمان تأمین کنند: حفظ امنیت ملی و صیانت از آزادی‌ها و حقوق بنیادین شهروندان. در حالی که تأکید یک‌جانبه بر الزامات امنیتی می‌تواند به محدودسازی آزادی‌های فردی و تضعیف اعتماد عمومی منجر شود، بی‌توجهی به مخاطرات امنیتی نیز زمینه‌ساز آسیب‌پذیری‌های جدی در سطح ملی خواهد بود. از این‌رو، دستیابی به توازن میان آزادی و امنیت در بستر فضای مجازی، یکی از مهم‌ترین چالش‌های دولت‌ها در دوران حکمرانی دیجیتال به شمار می‌رود. بررسی ابعاد نظری و عملی این توازن، تحلیل تجربه‌های بین‌المللی و واکاوی ظرفیت‌های حقوقی و نهادی دولت‌ها، می‌تواند مسیر دستیابی به الگوهای متعادل و پایدار در حاکمیت سایبری را روشن سازد.

۱- چارچوب مفهومی و مبانی نظری حاکمیت سایبری

۱-۱- تعریف و ابعاد حاکمیت سایبری

حاکمیت سایبری مفهومی است که انتقال اصول و وظایف حاکمیت سنتی به فضای دیجیتال و مجازی را در بر می‌گیرد و به مجموعه سیاست‌ها، سازوکارها و رویه‌هایی اشاره دارد که دولت‌ها و نهادهای حکومتی برای مدیریت، کنترل و نظارت بر فعالیت‌ها و منابع در فضای سایبری به کار می‌گیرند. این مفهوم هم شامل توانایی دولت در تدوین و اجرای قوانین و مقررات، هم ظرفیت اعمال سیاست‌های امنیتی و حفاظت از زیرساخت‌ها و داده‌های ملی است، بدون آنکه منافع عمومی و آزادی‌های فردی نادیده گرفته شوند. حاکمیت سایبری از ابعاد مختلفی قابل تحلیل است؛ از جمله بعد قانونی و حقوقی که چارچوب فعالیت‌های دیجیتال، حفاظت از داده‌ها، حقوق شهروندان و مسئولیت بازیگران مختلف را تعیین می‌کند و در آن دولت‌ها موظف‌اند توازن میان آزادی‌های فردی و الزامات امنیتی را رعایت کنند، بعد امنیتی که به توانایی دولت در حفاظت از زیرساخت‌های حیاتی، مقابله با تهدیدات سایبری و مدیریت بحران‌های دیجیتال مربوط می‌شود، بعد نهادی که شامل سازمان‌دهی و هماهنگی میان نهادهای دولتی، بخش خصوصی و جامعه مدنی برای اعمال حاکمیت موثر است، بعد فنی که به ایجاد استانداردها، پروتکل‌ها و فناوری‌های امنیتی و کنترلی در شبکه‌ها و سامانه‌های دیجیتال اشاره دارد، و بعد بین‌المللی که شامل تعاملات، همکاری‌ها و توافق‌های فراملی برای مقابله با تهدیدات سایبری و تضمین ثبات فضای مجازی در سطح جهانی می‌شود (برون، ۱۴۰۳). به طور کلی، حاکمیت سایبری فراتر از کنترل صرف شبکه‌ها و داده‌هاست و به برقراری تعادل میان امنیت، آزادی‌های فردی و بهره‌برداری مسئولانه از فضای دیجیتال برای توسعه اقتصادی، اجتماعی و فرهنگی می‌پردازد.

لازم به ذکر است که بخشی از ابعاد حاکمیت سایبری و امنیت فضای مجازی، پیوند با شاخص‌های کلان اقتصادی دارد، بدین معنا که اساساً حاکمیت سایبری و امنیت ملی در فضای مجازی ارتباط تنگاتنگی با شاخص‌های کلان اقتصادی مانند رشد سرمایه‌گذاری دیجیتال و اشتغال فناورانه دارد، زیرا این عوامل نه‌تنها زیرساخت‌های دیجیتال را تقویت می‌کنند، بلکه توانایی دولت در حفظ امنیت سایبری و توازن با آزادی‌های فردی را نیز ارتقا می‌دهند. در ایران، سیاست‌های شورای عالی فضای مجازی و قوانین موجود مانند قانون جرایم رایانه‌ای (مصوب ۱۳۸۸) بر توسعه اقتصاد دیجیتال و امنیت سایبری تأکید دارند. رشد سرمایه‌گذاری دیجیتال، از طریق جذب سرمایه‌های داخلی و خارجی در حوزه فناوری اطلاعات و ارتباطات (ICT)، زیرساخت‌های امن مانند شبکه ملی اطلاعات را تقویت می‌کند که به دولت امکان می‌دهد نظارت مؤثرتری بر فضای مجازی داشته باشد، بدون اینکه حریم خصوصی کاربران به‌طور غیرقانونی نقض شود. برای مثال، قانون مالیات‌های مستقیم (اصلاحی ۱۳۹۴) با ارائه معافیت‌های مالیاتی به شرکت‌های دانش‌بنیان، سرمایه‌گذاری در فناوری‌های دیجیتال را تشویق می‌کند، که می‌تواند به توسعه ابزارهای بومی امنیت سایبری منجر شود. این سرمایه‌گذاری‌ها، با ایجاد پلتفرم‌های امن و بومی، به کاهش وابستگی به فناوری‌های خارجی کمک می‌کند، که خود یک مؤلفه کلیدی امنیت ملی است. اشتغال فناورانه نیز از طریق ایجاد فرصت‌های شغلی در حوزه‌های برنامه‌نویسی، امنیت سایبری، و توسعه پلتفرم‌های دیجیتال، نیروی انسانی متخصص را افزایش می‌دهد که قادر به مقابله با تهدیدات سایبری مانند هک یا نشت داده‌ها هستند. رشد اقتصادی ناشی از سرمایه‌گذاری دیجیتال، منابع مالی دولت را برای نظارت و اجرای قوانین افزایش می‌دهد.

۱-۲- آزادی‌های فردی در فضای مجازی و جایگاه آن در نظام‌های حقوقی

آزادی‌های فردی در فضای مجازی به مجموعه حقوق و اختیاراتی اطلاق می‌شود که شهروندان در محیط دیجیتال و اینترنت از آن برخوردارند و شامل آزادی بیان، حق دسترسی به اطلاعات، حفظ حریم خصوصی، امنیت داده‌های شخصی و امکان مشارکت در فضای عمومی دیجیتال می‌شود. این آزادی‌ها نه تنها استمرار و بسط حقوق اساسی در بستر جدید فناوری اطلاعات هستند، بلکه ابزاری برای تحقق مشارکت اجتماعی، توسعه فرهنگی و گسترش فرصت‌های اقتصادی نیز محسوب می‌شوند. در نظام‌های حقوقی مختلف، جایگاه آزادی‌های فردی در فضای مجازی به شدت مورد توجه قرار گرفته و اغلب به عنوان امتداد حقوق بشر و آزادی‌های مدنی به رسمیت شناخته می‌شود. قوانین و مقررات ملی، منشورهای بین‌المللی و اسناد حقوق بشر تلاش دارند چارچوبی فراهم کنند که افراد بتوانند بدون ترس از سانسور، تعقیب یا نقض حریم خصوصی، از این آزادی‌ها بهره‌مند شوند (بحرینی، ۱۴۰۳).

با این حال، در عمل، این آزادی‌ها همیشه مطلق نیستند و در بسیاری از نظام‌ها محدودیت‌هایی بر اساس ضرورت‌های امنیت ملی، پیشگیری از جرایم سایبری، حفاظت از حقوق دیگران و منافع عمومی وضع می‌شود. در نتیجه، حفظ تعادل میان آزادی‌های فردی و الزامات امنیتی یکی از چالش‌های اصلی در طراحی سیاست‌ها و مقررات فضای مجازی است و نظام‌های حقوقی مختلف با ابزارهای قانونی، نظارتی و قضایی تلاش می‌کنند این تعادل را برقرار کنند، به گونه‌ای که هم حقوق شهروندان صیانت شود و هم امنیت و ثبات فضای دیجیتال تضمین گردد.

از منظر تقنینی نیز باید گفت که اساساً آزادی‌های فردی در فضای مجازی در ایران تحت چارچوب‌های حقوقی قانون اساسی و قوانین مرتبط مانند قانون جرایم رایانه‌ای (مصوب ۱۳۸۸) تعریف می‌شود، اما این آزادی‌ها با محدودیت‌هایی برای حفظ نظم عمومی و امنیت ملی همراه است. بر اساس اصل ۲۶ و ۲۷ قانون اساسی، آزادی و حقوق افراد تا جایی تضمین شده که به استقلال یا وحدت ملی آسیب نرسد. اصل ۲۴ قانون اساسی آزادی بیان در مطبوعات و نشریات را مشروط به عدم اخلال در مبانی اسلام و حقوق عمومی به رسمیت می‌شناسد، که این موضوع به فضای مجازی نیز تسری می‌یابد. همچنین، اصل ۲۵ قانون اساسی هرگونه تجسس و نقض حریم خصوصی را ممنوع کرده، مگر در مواردی که قانون اجازه دهد، مانند ضرورت‌های امنیتی. این اصل به معنای حمایت از حریم خصوصی دیجیتال شهروندان در برابر دسترسی غیرمجاز به اطلاعات شخصی است. قانون جرایم رایانه‌ای نیز در ماده ۱ دسترسی غیرمجاز به داده‌ها یا سیستم‌های رایانه‌ای را جرم‌انگاری کرده است. با این حال، موادی مانند ۱۶ و ۱۷ این قانون انتشار محتوای مغایر با شئونات اسلامی یا مخل نظم عمومی را ممنوع کرده و به دولت اختیار نظارت و محدودیت در فضای مجازی می‌دهد. در نتیجه، آزادی‌های فردی در فضای مجازی مانند آزادی بیان و حفظ حریم خصوصی در ایران به رسمیت شناخته شده، اما در عمل با محدودیت‌های قانونی برای حفظ ارزش‌های اسلامی، امنیت ملی و نظم عمومی مواجه است. فقدان قانون جامع حفاظت از داده‌های شخصی نیز سبب شده که حمایت از این آزادی‌ها گاه ناکافی باشد.

۱-۳- الزامات و تهدیدات امنیت ملی در بستر فضای مجازی

الزامات و تهدیدات امنیت ملی در بستر فضای مجازی مجموعه‌ای از چالش‌ها و نیازمندی‌هایی را شامل می‌شود که دولت‌ها برای حفاظت از ثبات، حاکمیت و منافع عمومی کشور با آن مواجه‌اند. الزامات امنیت ملی در فضای سایبری مستلزم ایجاد چارچوب‌های قانونی، نهادی و فنی است که بتوانند از زیرساخت‌های حیاتی، اطلاعات حساس، شبکه‌های دولتی و خدمات عمومی در برابر تهدیدات دیجیتال محافظت کنند و در عین حال امکان پاسخ سریع به حملات سایبری و مدیریت بحران‌های فناوری را فراهم سازند (جعفری نیا، ۱۴۰۳).

این الزامات همچنین ایجاب می‌کنند دولت‌ها توانمندی‌های لازم در شناسایی، پیشگیری و خنثی‌سازی حملات سایبری، جاسوسی دیجیتال، نفوذ غیرمجاز و فعالیت‌های مخرب گروه‌ها یا دولت‌های بیگانه را توسعه دهند. از سوی دیگر، تهدیدات امنیت ملی در فضای مجازی شامل حملات سایبری علیه زیرساخت‌های حیاتی مانند شبکه‌های برق، ارتباطات، حمل و نقل، سیستم‌های مالی و داده‌های دولتی، نفوذ به سامانه‌های اطلاعاتی و سوءاستفاده از داده‌های شخصی و سازمانی است. همچنین جنگ اطلاعاتی، انتشار اخبار جعلی، حملات سایبری هدفمند علیه نهادهای دولتی و خصوصی و اقدامات خرابکارانه دیجیتال نیز از جمله تهدیدات مهم به شمار می‌آیند. به دلیل ماهیت پیچیده و فراملی این تهدیدات، دولت‌ها ناچارند ترکیبی از سیاست‌های پیشگیرانه، تدابیر امنیتی فنی، همکاری با بخش خصوصی و جامعه مدنی و هماهنگی‌های بین‌المللی را به کار گیرند تا بتوانند امنیت ملی را در فضای سایبری حفظ کنند و در عین حال تعادل مناسبی میان حفاظت از کشور و احترام به آزادی‌های فردی برقرار سازند.

۲- نقش و جایگاه دولت‌ها در حکمرانی سایبری

۲-۱- وظایف و اختیارات دولت‌ها در اعمال حاکمیت دیجیتال

نقش و جایگاه دولت‌ها در حکمرانی سایبری به عنوان محور اصلی مدیریت فضای دیجیتال، شامل تضمین امنیت ملی، تنظیم قواعد فعالیت‌های مجازی، حفاظت از حقوق شهروندان و ایجاد زیرساخت‌های مطمئن است. دولت‌ها در این چارچوب نه تنها به عنوان قانون‌گذار و ناظر عمل می‌کنند، بلکه به عنوان بازیگر اصلی در ایجاد تعادل میان آزادی‌های فردی و الزامات امنیتی نیز شناخته می‌شوند (حاتمی و حیدری، ۱۴۰۳). وظایف دولت‌ها در اعمال حاکمیت دیجیتال شامل تدوین سیاست‌ها و مقررات مرتبط با فعالیت‌های اینترنتی، حفاظت از زیرساخت‌های حیاتی دیجیتال، مدیریت داده‌ها و اطلاعات حساس، پیشگیری و مقابله با جرایم سایبری و تضمین تداوم خدمات عمومی است. دولت‌ها همچنین مسئول ایجاد سازوکارهای نظارتی و پاسخ به تهدیدات، ارتقای توانمندی‌های فنی برای مقابله با حملات سایبری و توسعه ظرفیت‌های انسانی و نهادی برای مدیریت فضای دیجیتال هستند. از سوی دیگر، اختیارات دولت‌ها در این حوزه شامل حق وضع قوانین و مقررات، اعمال سیاست‌های امنیتی و کنترلی، تنظیم تعاملات میان نهادهای دولتی، بخش خصوصی و جامعه مدنی، و اعمال محدودیت‌های موقت در شرایط اضطراری برای حفاظت از امنیت ملی است.

با این حال، این اختیارات باید در چارچوب قانونی و با رعایت حقوق شهروندان اعمال شوند تا از سوءاستفاده یا محدودسازی غیرضروری آزادی‌های فردی جلوگیری شود. به طور کلی، دولت‌ها در حکمرانی سایبری نقش همزمان قانون‌گذار، ناظر، حافظ امنیت و تضمین‌کننده حقوق شهروندان را ایفا می‌کنند و موفقیت در این نقش مستلزم سیاست‌گذاری هوشمند، هماهنگی نهادی و پاسخ‌گویی شفاف به جامعه است.

از منظر تقنینی نیز طبق اصل ۲۵ قانون اساسی تجسس و نقض حریم خصوصی را ممنوع کرده است، مگر در مواردی که قانون اجازه دهد (مثلاً برای امنیت ملی یا پیشگیری از جرم). این اصل به دولت اختیار می‌دهد تا در شرایط خاص، نظارت دیجیتال را اعمال کند، اما باید با رعایت چارچوب‌های قانونی باشد.

در قانون جرایم رایانه‌ای (۱۳۸۸) نیز ماده ۱ دسترسی غیرمجاز به داده‌ها یا سیستم‌های رایانه‌ای را جرم‌انگاری کرده و به دولت اجازه می‌دهد با هکرها یا متجاوزان به حریم دیجیتال برخورد کند. ماده ۱۶ و ۱۷ نیز انتشار محتوای مجرمانه (مانند مطالب توهین‌آمیز یا غیراخلاقی) در فضای مجازی را جرم دانسته و به دولت اختیار نظارت و فیلترینگ در موارد خاص را می‌دهد. این قانون به دولت اجازه می‌دهد نهادهایی مانند پلیس فتا را برای رصد، پیشگیری و مقابله با جرایم سایبری فعال کند.

۲-۲- سیاست‌های امنیتی و حقوقی دولت‌ها در فضای مجازی

سیاست‌های امنیتی و حقوقی دولت‌ها در فضای مجازی نقش محوری در حکمرانی سایبری ایفا می‌کنند و تلاشی هستند برای مدیریت تهدیدات دیجیتال و تضمین استفاده ایمن، منصفانه و قانونمند از فضای دیجیتال. از منظر امنیتی، دولت‌ها سیاست‌هایی را طراحی و اجرا می‌کنند که هدف آن حفاظت از زیرساخت‌های حیاتی، شبکه‌های اطلاعاتی دولتی، سیستم‌های مالی و خدمات عمومی در برابر حملات سایبری، نفوذهای غیرمجاز و اقدامات خرابکارانه دیجیتال است (جلالی شاد، ۱۴۰۳). این سیاست‌ها شامل پیشگیری از تهدیدات، شناسایی و تحلیل ریسک‌ها، آموزش و ارتقای توانمندی‌های فنی نیروهای انسانی، و ایجاد سازوکارهای پاسخ سریع و مدیریت بحران‌های سایبری می‌شود. از منظر حقوقی، دولت‌ها مسئول وضع مقررات و قوانین مرتبط با استفاده از اینترنت، حفاظت از داده‌های شخصی، حقوق شهروندان در فضای مجازی، آزادی بیان و محدودیت‌های موجه فعالیت‌های آنلاین هستند. این سیاست‌ها تلاش می‌کنند تعادلی میان تضمین امنیت ملی و صیانت از آزادی‌ها و حقوق فردی برقرار کنند، به گونه‌ای که محدودیت‌ها در شرایط اضطراری مشروع و شفاف باشند و امکان نظارت و پاسخ‌گویی وجود داشته باشد. در مجموع، ترکیب سیاست‌های امنیتی و حقوقی دولت‌ها، پایه‌ای برای حکمرانی سایبری متوازن ایجاد می‌کند که هم از کشور در برابر تهدیدات دیجیتال محافظت می‌کند و هم حقوق و آزادی‌های شهروندان را در فضای مجازی محترم می‌شمارد.

۲-۳- چالش‌های فراملی و بین‌المللی در اجرای حاکمیت سایبری

چالش‌های فراملی و بین‌المللی در اجرای حاکمیت سایبری از مهم‌ترین موانع پیش روی دولت‌ها در مدیریت فضای دیجیتال هستند، زیرا فضای مجازی ذاتاً مرزناپذیر است و فعالیت‌ها و تهدیدات سایبری اغلب فراتر از مرزهای ملی رخ می‌دهند. یکی از این چالش‌ها تفاوت در قوانین، استانداردها و رویکردهای حقوقی میان کشورهاست، به گونه‌ای که آنچه در یک نظام قانونی مشروع و مجاز است، در نظام دیگر ممکن است نقض قانون تلقی شود و این موضوع هماهنگی بین‌المللی را دشوار می‌کند. علاوه بر این، تهدیدات سایبری می‌توانند منشأ خارجی داشته باشند و شامل حملات سایبری دولت‌ها یا گروه‌های غیر دولتی به زیرساخت‌های حیاتی، سرقت اطلاعات حساس یا جنگ اطلاعاتی باشند که پاسخ ملی به آنها بدون همکاری بین‌المللی محدود و ناکارآمد است (فرزام نیا و عبدی،۱۴۰۲).

چالش دیگر کمبود توافقات و مکانیسم‌های جهانی الزام‌آور برای کنترل و پیشگیری از فعالیت‌های مخرب دیجیتال است؛ بسیاری از پیمان‌ها و کنوانسیون‌های بین‌المللی هنوز جامعیت و ضمانت اجرایی کافی ندارند و هماهنگی میان کشورها در حوزه امنیت سایبری با کندی و دشواری همراه است. علاوه بر این، رقابت‌های ژئوپلتیک و اختلاف منافع ملی می‌تواند مانع شکل‌گیری چارچوب‌های مشترک شود و کشورها را به اتخاذ رویکردهای یکجانبه یا محافظه‌کارانه ترغیب کند. در این شرایط، دولت‌ها ناچارند با بهره‌گیری از دیپلماسی سایبری، مشارکت در سازمان‌های بین‌المللی، تبادل اطلاعات امنیتی و توسعه استانداردهای مشترک، تلاش کنند تا حاکمیت سایبری خود را در مرزهای ملی اعمال کنند و همزمان از همکاری‌های فراملی برای مقابله با تهدیدات گسترده و پیچیده بهره‌مند شوند، در حالی که حفظ تعادل میان امنیت ملی و آزادی‌های فردی همچنان یکی از پیچیده‌ترین مسائل سیاست‌گذاری در عرصه جهانی است.

۳- تعارض میان آزادی‌های فردی و الزامات امنیت ملی

۳-۱- نمونه‌ها و مصادیق تعارض در عرصه فضای مجازی

تعارض میان آزادی‌های فردی و الزامات امنیت ملی در عرصه فضای مجازی در عمل بسیار مشهود است و در قالب نمونه‌ها و مصادیق مختلف قابل مشاهده می‌باشد. یکی از شایع‌ترین نمونه‌ها محدودیت‌های دسترسی به اطلاعات و محتوای آنلاین است که دولت‌ها برای مقابله با تهدیدات امنیتی یا پیشگیری از انتشار محتوای مخل امنیت ملی اعمال می‌کنند، مانند فیلتر کردن وب‌سایت‌ها، شبکه‌های اجتماعی یا محتواهای خبری خاص، که همزمان می‌تواند آزادی بیان و دسترسی آزاد به اطلاعات را محدود سازد. نمونه دیگر جمع‌آوری گسترده داده‌های شخصی کاربران توسط نهادهای دولتی برای مقاصد امنیتی است، مانند پایش پیام‌ها و ارتباطات دیجیتال برای شناسایی فعالیت‌های مشکوک، که با حق حریم خصوصی و آزادی ارتباطات افراد در تضاد قرار می‌گیرد. همچنین، اعمال محدودیت‌های حرکتی دیجیتال یا توقیف موقت حساب‌های کاربری افراد و گروه‌ها در شبکه‌های اجتماعی به دلایل امنیتی، نمونه‌ای دیگر از تعارض میان حقوق فردی و الزامات امنیت ملی به شمار می‌رود. حملات سایبری خارجی یا تهدیدات تروریستی نیز گاهی موجب می‌شود دولت‌ها برای حفاظت از زیرساخت‌های حیاتی تصمیماتی اتخاذ کنند که دسترسی آزاد و مشارکت اجتماعی کاربران در فضای دیجیتال را محدود می‌کند. علاوه بر این، برخی سیاست‌های قانونی و قضایی برای پیشگیری از نفوذ یا جرایم سایبری، مانند الزام شرکت‌های فناوری به همکاری با نهادهای امنیتی و ارائه اطلاعات کاربران، می‌تواند آزادی فردی و اعتماد عمومی به فضای مجازی را کاهش دهد. این مصادیق نشان می‌دهند که حفظ توازن میان آزادی‌های فردی و الزامات امنیت ملی یکی از چالش‌های اصلی حکمرانی سایبری است و نیازمند تدوین سیاست‌ها و سازوکارهایی است که ضمن حفاظت از امنیت، حداقل محدودیت‌ها را بر حقوق شهروندان اعمال کنند.

۳-۲-پیامدهای افراط در امنیت‌گرایی

افراط در امنیت‌گرایی در فضای مجازی می‌تواند پیامدهای جدی و گسترده‌ای برای جامعه و نظام حکمرانی ایجاد کند. هنگامی که دولت‌ها با تمرکز افراطی بر الزامات امنیت ملی اقدام به محدودسازی گسترده آزادی‌های فردی می‌کنند، ابتدا اعتماد عمومی به نهادهای حکومتی کاهش می‌یابد، زیرا شهروندان احساس می‌کنند حریم خصوصی و حقوق اساسی آن‌ها نادیده گرفته شده است. این کاهش اعتماد می‌تواند به بی‌اعتمادی گسترده نسبت به خدمات دولتی و حتی به کنشگری مدنی منفی منجر شود (مومنی، ۱۴۰۳)؛ از نظر اجتماعی، محدودیت‌های بیش از حد آزادی بیان، دسترسی به اطلاعات و مشارکت دیجیتال، خلاقیت،

نوآوری و تبادل دانش در جامعه را محدود می‌کند و باعث کاهش ظرفیت‌های فرهنگی و اقتصادی می‌شود. در بعد حقوقی، اعمال محدودیت‌های افراطی ممکن است با تعارض با قوانین داخلی و بین‌المللی حقوق بشر مواجه شود و زمینه شکایت‌ها و چالش‌های قضایی را فراهم کند. همچنین، تمرکز صرف بر امنیت ملی می‌تواند به ایجاد ساختارهای نظارتی و کنترلی پیچیده و هزینه‌بر منجر شود که منابع مالی و انسانی کشور را صرفاً در جهت کنترل و پایش فعالیت‌های دیجیتال مصرف می‌کند، بدون آنکه به توسعه پایدار فضای مجازی کمک کند. در بعد سیاسی، افراط در امنیت‌گرایی ممکن است موجب تضعیف مشروعیت دولت‌ها شود، زیرا اعمال محدودیت‌های غیرضروری و غیرشفاف بر آزادی‌های فردی با انتقادات داخلی و بین‌المللی مواجه خواهد شد. به طور کلی، پیامدهای افراط در امنیت‌گرایی نشان می‌دهد که امنیت ملی در فضای مجازی بدون رعایت تعادل با آزادی‌های فردی نه تنها ناکارآمد خواهد بود، بلکه می‌تواند به بی‌اعتمادی اجتماعی، کاهش مشارکت مدنی، کندی توسعه فناوری و آسیب به مشروعیت سیاسی دولت‌ها منجر شود.

۳-۳- پیامدهای افراط در آزادی‌گرایی

افراط در آزادی‌گرایی در فضای مجازی نیز پیامدهای قابل توجهی دارد و می‌تواند امنیت ملی و ثبات اجتماعی را به مخاطره بیندازد. وقتی دولت‌ها با تأکید بیش از حد بر آزادی‌های فردی اقدام به کاهش کنترل و محدودیت‌های امنیتی می‌کنند، زیرساخت‌های حیاتی کشور، سیستم‌های اطلاعاتی و داده‌های حساس در معرض نفوذ، حملات سایبری و سوءاستفاده‌های دیجیتال قرار می‌گیرند. این وضعیت می‌تواند منجر به تضعیف امنیت اقتصادی، اختلال در خدمات عمومی و آسیب به شبکه‌های حیاتی شود. از بعد اجتماعی، نبود کنترل کافی بر محتوا و فعالیت‌های آنلاین ممکن است انتشار اطلاعات نادرست، اخبار جعلی، محتوای مخرب یا اقدامات تحریک‌آمیز را تسهیل کند و پیامدهای منفی بر انسجام اجتماعی و اعتماد عمومی داشته باشد (حسین پور و صابرنژاد، ۱۳۹۴). در بعد حقوقی و سیاسی، دولت‌هایی که از اعمال محدودیت‌های موقت و متناسب برای حفاظت از امنیت ملی اجتناب می‌کنند، با مخاطراتی همچون افزایش جرایم سایبری، حملات تروریستی دیجیتال یا نفوذهای خارجی مواجه خواهند شد که می‌تواند به چالش‌های قانونی و انتقادات سیاسی منجر شود. افزون بر این، افراط در آزادی‌گرایی ممکن است هماهنگی میان نهادهای امنیتی و مدیریتی را کاهش دهد و پاسخ سریع و مؤثر به تهدیدات سایبری را دشوار سازد. به طور کلی، پیامدهای افراط در آزادی‌گرایی نشان می‌دهد که عدم محدودیت‌های منطقی و متناسب برای حفاظت از فضای مجازی و زیرساخت‌های حیاتی می‌تواند به آسیب‌پذیری شدید ملی، اختلال در عملکرد کشور و کاهش امنیت عمومی منجر شود، و ضرورت ایجاد تعادل میان آزادی‌های فردی و الزامات امنیت ملی را برجسته می‌سازد.

۳-۴-ضمانت اجرای تخطی از اصل شفافیت و اصل پاسخگویی

حاکمیت سایبری در ایران مستلزم ایجاد توازن میان آزادی‌های فردی، مانند آزادی بیان و حریم خصوصی و الزامات امنیت ملی است که در چارچوب قانون اساسی و قانون جرایم رایانه‌ای (مصوب ۱۳۸۸) و همینطور قانون مدیریت داده‌ها و اطلاعات ملی مصوب ۱۴۰۱ تنظیم می‌شود. اصول شفافیت و پاسخگویی، هرچند به‌صورت صریح در قوانین ایران تعریف نشده‌اند، به‌طور ضمنی در تعهدات دولت و نهادهای خصوصی برای رعایت حقوق شهروندان و اجرای قانون مستتر هستند. تخطی از این اصول، مانند نقض حریم خصوصی یا سوءاستفاده از داده‌ها، با ضمانت‌های اجرایی مشخصی مواجه می‌شود. بر اساس اصل ۲۵ قانون اساسی، هرگونه تجسس غیرقانونی، از جمله دسترسی غیرمجاز به اطلاعات دیجیتال شهروندان توسط دولت یا نهادهای خصوصی، ممنوع است مگر در مواردی که قانون اجازه دهد. نقض این اصل می‌تواند به پیگیری قضایی منجر شود، اگرچه قانون اساسی به‌طور مستقیم مجازات خاصی برای نهادهای دولتی تعیین نکرده و این امر به قوانین عادی واگذار شده است. قانون جرایم رایانه‌ای در ماده ۱ دسترسی غیرمجاز به داده‌ها یا سیستم‌های رایانه‌ای را جرم‌انگاری کرده و برای متخلفان، اعم از اشخاص حقیقی یا حقوقی (از جمله شرکت‌های خصوصی)، حبس و جزای نقدی پیش‌بینی کرده است. ماده ۳ این قانون نقض حریم خصوصی از طریق شنود غیرقانونی محتوای دیجیتال را جرم دانسته و مجازات مشابهی را اعمال می‌کند. در صورت عدم شفافیت یا پاسخگویی شرکت‌های خصوصی در قبال داده‌های کاربران، ماده ۱۷ قانون جرایم رایانه‌ای انتشار یا سوءاستفاده از محتوای غیرقانونی را با حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج تا چهل میلیون ریال جریمه می‌کند. در مورد نهادهای دولتی، تخطی از شفافیت یا پاسخگویی ممکن است تحت نظارت نهادهایی مانند دیوان عدالت اداری (بر اساس اصل ۱۷۳ قانون اساسی) یا سازمان بازرسی کل کشور (اصل ۱۷۴) بررسی شود، اما ضمانت اجرایی مشخص برای مقامات دولتی در قوانین سایبری به‌صورت صریح ذکر نشده و بیشتر به تخلفات اداری یا قضایی ارجاع می‌شود. فقدان قانون جامع حفاظت از داده‌های شخصی در ایران، اجرای اصول شفافیت و پاسخگویی را در برابر تخلفات سایبری محدود کرده و خلأهایی در ضمانت‌های اجرایی به‌ویژه برای نهادهای دولتی ایجاد می‌کند.

۴- راهکارها و الگوهای ایجاد توازن

۴-۱- اصول بنیادین تحقق توازن میان آزادی و امنیت

تحقق توازن میان آزادی‌های فردی و الزامات امنیت ملی در فضای مجازی مستلزم رعایت اصول بنیادینی است که هم جنبه‌های حقوقی و اخلاقی را در نظر می‌گیرند و هم الزامات امنیتی و عملیاتی را پوشش می‌دهند. نخستین اصل، رعایت اصل تناسب است، به این معنا که هر محدودیت یا اقدام امنیتی باید متناسب با سطح تهدید و ضرورت حفاظت از امنیت ملی باشد و از اعمال محدودیت‌های غیرضروری یا افراطی بر آزادی‌های فردی خودداری شود. دومین اصل، شفافیت و پاسخ‌گویی است؛ دولت‌ها باید درباره سیاست‌ها و اقدامات امنیتی خود به جامعه اطلاع‌رسانی کنند و سازوکارهایی برای نظارت عمومی و پاسخگویی در برابر محدودیت‌های اعمال‌شده فراهم آورند تا اعتماد شهروندان حفظ شود. سومین اصل، رعایت چارچوب‌های قانونی و حقوقی است؛ تمام اقدامات امنیتی باید در چهارچوب قوانین ملی و استانداردهای بین‌المللی حقوق بشر انجام شود تا مشروعیت قانونی و اخلاقی آن‌ها تضمین شود. چهارمین اصل، مشارکت چندسطحی و همکاری میان نهادهای دولتی، بخش خصوصی و جامعه مدنی است، زیرا مدیریت تهدیدات سایبری و حفاظت از آزادی‌های دیجیتال نیازمند هماهنگی و تبادل اطلاعات میان بازیگران مختلف است (شمعی و احمدی، ۱۳۹۹). پنجمین اصل، انعطاف‌پذیری و انطباق‌پذیری سیاست‌ها با تغییرات فناوری و تهدیدات نوین است؛ سیاست‌های امنیتی و مقررات حریم خصوصی باید قابلیت بازبینی و به‌روزرسانی داشته باشند تا بتوانند هم امنیت ملی و هم آزادی‌های فردی را به شکل پویا حفظ کنند. رعایت این اصول بنیادین، چارچوبی ایجاد می‌کند که دولت‌ها بتوانند هم از امنیت ملی محافظت کنند و هم آزادی‌های شهروندان در فضای مجازی را صیانت نمایند، به طوری که تعادل میان کنترل و آزادی به شکل مستمر و پایدار برقرار بماند.

۴-۲- نقش شفافیت، پاسخ‌گویی و حاکمیت قانون

شفافیت، پاسخ‌گویی و حاکمیت قانون نقش محوری در ایجاد توازن میان آزادی‌های فردی و الزامات امنیت ملی در فضای مجازی دارند و به عنوان ستون‌های اصلی حکمرانی سایبری متوازن شناخته می‌شوند. شفافیت به این معناست که دولت‌ها درباره سیاست‌ها، اقدامات امنیتی، محدودیت‌ها و نحوه استفاده از داده‌ها اطلاع‌رسانی کنند و فرآیندهای تصمیم‌گیری خود را برای شهروندان قابل درک و پیگیری سازند. شفافیت، اعتماد عمومی را تقویت می‌کند و مانع سوءاستفاده یا اعمال محدودیت‌های غیرضروری بر آزادی‌های فردی می‌شود. پاسخ‌گویی مکمل شفافیت است و به معنای آن است که دولت‌ها مسئول اعمال خود در قبال شهروندان باشند و امکان نظارت، انتقاد و بازخواست وجود داشته باشد. سازوکارهای پاسخ‌گویی شامل نهادهای نظارتی مستقل، دادگاه‌ها، رسانه‌ها و ابزارهای مشارکت عمومی در ارزیابی سیاست‌ها و اقدامات سایبری می‌شود. حاکمیت قانون نیز تضمین می‌کند که تمام محدودیت‌ها و اقدامات امنیتی در چهارچوب قوانین ملی و استانداردهای بین‌المللی حقوق بشر اعمال شوند و هیچ نهادی از چارچوب قانونی مستثنی نباشد (غلامی، ۱۳۹۹). این اصل، مشروعیت قانونی و اخلاقی سیاست‌های امنیتی را تضمین می‌کند و از اعمال اقدامات خودسرانه یا افراطی جلوگیری می‌نماید. در مجموع، ترکیب شفافیت، پاسخ‌گویی و حاکمیت قانون بستری ایجاد می‌کند که دولت‌ها بتوانند هم امنیت ملی را در فضای دیجیتال تأمین کنند و هم حقوق و آزادی‌های شهروندان را حفظ نمایند، به طوری که تعادل میان کنترل و آزادی به شکل پایدار و مشروع برقرار شود.

۴-۳- همکاری میان دولت، بخش خصوصی و جامعه مدنی

همکاری میان دولت، بخش خصوصی و جامعه مدنی یکی از مهم‌ترین راهکارها برای ایجاد توازن میان آزادی‌های فردی و الزامات امنیت ملی در فضای مجازی به شمار می‌رود، زیرا امنیت و بهره‌برداری مسئولانه از فضای دیجیتال تنها با نقش‌آفرینی یک بازیگر امکان‌پذیر نیست. دولت‌ها مسئول تدوین سیاست‌ها، قوانین و چارچوب‌های نظارتی هستند و وظیفه دارند زیرساخت‌های حیاتی، داده‌های حساس و خدمات عمومی را محافظت کنند، اما بدون مشارکت بخش خصوصی، به ویژه شرکت‌های فناوری و ارائه‌دهندگان خدمات دیجیتال، توانایی عملیاتی برای پیاده‌سازی امنیت سایبری محدود خواهد بود. بخش خصوصی با ارائه راهکارهای فنی، استانداردهای امنیتی، سامانه‌های پایش و مدیریت داده‌ها نقش مستقیم در کاهش تهدیدات و حفاظت از کاربران دارد. از سوی دیگر، جامعه مدنی و سازمان‌های مردم‌نهاد، به نمایندگی از شهروندان، می‌توانند نظارت و بازخورد مستمر بر سیاست‌ها و اقدامات دولت ارائه دهند، شفافیت و پاسخ‌گویی را تقویت کنند و تضمین کنند که آزادی‌های فردی و حقوق دیجیتال شهروندان در تدوین و اجرای سیاست‌های امنیتی رعایت می‌شود (بذرگر، ۱۳۹۴).

همکاری میان دولت، بخش خصوصی و جامعه مدنی برای ایجاد توازن میان آزادی‌های فردی و الزامات امنیت ملی در فضای مجازی، از طریق سیاست‌های حمایتی دولت از بخش خصوصی، به‌ویژه در حوزه مشوق‌های مالیاتی، یارانه‌های امنیت سایبری و حمایت از استارتاپ‌ها، می‌تواند به‌طور مؤثری تقویت شود. در ایران، این همکاری‌ها در چارچوب قوانین موجود و سیاست‌های کلان شورای عالی فضای مجازی پیگیری می‌شود، هرچند هنوز برنامه‌های جامع و منسجمی در این زمینه به‌طور کامل اجرایی نشده است. دولت می‌تواند با ارائه مشوق‌های مالیاتی، مانند معافیت مالیاتی برای شرکت‌هایی که استانداردهای امنیت سایبری را رعایت می‌کنند یا پلتفرم‌هایی که از حریم خصوصی کاربران حفاظت می‌کنند، بخش خصوصی را به سرمایه‌گذاری در فناوری‌های امن و کاربرمحور ترغیب کند. برای مثال، ماده ۱۳۲ قانون مالیات‌های مستقیم (اصلاحی ۱۳۹۴) امکان معافیت مالیاتی برای شرکت‌های دانش‌بنیان را فراهم کرده است، که می‌تواند به شرکت‌های فعال در حوزه امنیت سایبری یا پلتفرم‌های دیجیتال نیز تسری یابد، به‌شرطی که فعالیت‌هایشان با الزامات امنیت ملی و حفظ حقوق کاربران هم‌راستا باشد. یارانه‌های امنیت سایبری، مانند تخصیص بودجه برای توسعه ابزارهای رمزنگاری داخلی یا آموزش شرکت‌ها در زمینه مقابله با تهدیدات سایبری، نیز می تواند هزینه‌های بخش خصوصی را کاهش دهد و آن‌ها را به رعایت استانداردهای امنیتی تشویق کند. دولت می‌تواند با ارائه یارانه به شرکت‌هایی که ابزارهای رمزنگاری و حفاظت از داده را توسعه می‌دهند، هم امنیت سایبری را تقویت کند و هم حریم خصوصی کاربران را حفظ نماید. حمایت از استارتاپ‌ها، به‌ویژه آن‌هایی که در حوزه فناوری اطلاعات و ارتباطات (ICT) فعالیت می‌کنند، از طریق تسهیلات مالی، دسترسی به زیرساخت‌های شبکه ملی اطلاعات، یا ایجاد پارک‌های فناوری، نیز نقش مهمی دارد. برای نمونه، بر اساس مصوبات شورای عالی فضای مجازی (۱۳۹۱)، دولت موظف به حمایت از کسب‌وکارهای دیجیتال بومی است، که می‌تواند شامل استارتاپ‌هایی باشد که راهکارهای نوآورانه برای حفظ توازن میان آزادی‌های فردی و امنیت ملی ارائه می‌دهند، مانند پلتفرم‌های بومی با پروتکل‌های امنیتی قوی. این حمایت‌ها، ضمن تشویق بخش خصوصی به مشارکت فعال در حاکمیت سایبری، می‌تواند از طریق نظارت دولت بر رعایت اصول شفافیت و پاسخگویی، از نقض حقوق کاربران جلوگیری کند.

اساساً تعامل میان این سه بخش باعث تبادل اطلاعات، هماهنگی در مقابله با تهدیدات پیچیده، ارتقای فرهنگ امنیت سایبری و ایجاد راهکارهای مبتنی بر نیازهای واقعی کاربران می‌شود. به عبارت دیگر، همکاری چندسطحی میان دولت، بخش خصوصی و جامعه مدنی بستری فراهم می‌کند که امنیت ملی تقویت شود، آزادی‌های فردی محترم شمرده شوند و حکمرانی سایبری به شکل متوازن، پایدار و مشروع تحقق یابد.

۵- تحلیل تطبیقی

۵-۱- تجربه ایالات متحده در تنظیم رابطه آزادی و امنیت سایبری

تجربه ایالات متحده در تنظیم رابطه میان آزادی‌های فردی و امنیت سایبری نمونه‌ای از تلاش برای ایجاد توازن میان حقوق شهروندان و الزامات امنیت ملی در یک نظام دموکراتیک است. در این کشور، چارچوب‌های قانونی و نهادی متعددی برای حفاظت از داده‌ها و امنیت دیجیتال ایجاد شده‌اند و همزمان آزادی بیان و حریم خصوصی شهروندان تا حد امکان مورد توجه قرار گرفته است. از بعد قانونی، قانون حریم خصوصی آنلاین، مقررات مرتبط با حفاظت از داده‌های کاربران و قوانین مرتبط با امنیت ملی مانند قانون آزادی اطلاعات و قانون PATRIOT ، نمونه‌هایی از تلاش برای تعیین محدوده اختیارات دولت و تعادل میان آزادی و امنیت هستند. از بعد نهادی، سازمان‌هایی مانند وزارت امنیت داخلی، آژانس امنیت ملی و کمیسیون فدرال ارتباطات، نقش هماهنگی و نظارت بر زیرساخت‌های حیاتی دیجیتال و مقابله با تهدیدات سایبری را بر عهده دارند. در عین حال، نهادهای قضایی و قوانین مدنی امکان بازخواست دولت و بررسی مشروعیت اقدامات امنیتی را فراهم می‌کنند و بخش خصوصی و جامعه مدنی نیز با ارائه شکایات، نقد سیاست‌ها و توسعه فناوری‌های محافظتی، نقش فعال در حفظ تعادل دارند (ملکی و جمالی، ۱۴۰۳)؛ با این وجود، تجربه آمریکا نشان می‌دهد که حتی در نظام‌های دموکراتیک، تعارض میان آزادی‌های فردی و الزامات امنیت ملی همچنان

وجود دارد و اقدامات امنیتی مانند جمع‌آوری گسترده داده‌ها، پایش ارتباطات و برنامه‌های ضدتروریستی، گاه انتقادات جدی از منظر حقوق بشر و آزادی‌های دیجیتال به همراه داشته است. این تجربه نشان می‌دهد که ایجاد توازن میان آزادی و امنیت سایبری نیازمند چارچوب‌های قانونی شفاف، نظارت مؤثر، مشارکت فعال بخش خصوصی و جامعه مدنی و بازنگری مستمر سیاست‌ها در مواجهه با تهدیدات نوین است.

۵-۲- تجربه اتحادیه اروپا و نظام‌های منطقه‌ای

تجربه اتحادیه اروپا و نظام‌های منطقه‌ای در تنظیم رابطه میان آزادی‌های فردی و امنیت سایبری نمونه‌ای از رویکرد مبتنی بر حقوق شهروندی و استانداردهای هماهنگ بین‌المللی است. اتحادیه اروپا با تدوین مقررات جامع مانند قانون حفاظت از داده‌ها (GDPR) تلاش کرده است چارچوبی قانونی ایجاد کند که حقوق حریم خصوصی و آزادی‌های دیجیتال شهروندان را در سطح فراملی تضمین نماید و همزمان الزامات امنیتی را در قالب استانداردها و دستورالعمل‌های مشترک پیاده‌سازی کند. در این نظام، کشورها ملزم به رعایت اصول شفافیت، پاسخ‌گویی و حداقل محدودیت‌های قانونی در مواجهه با تهدیدات سایبری هستند (معطری و مصلی نژاد، ۱۴۰۳). ساختارهای نهادی مانند آژانس اتحادیه اروپا برای امنیت شبکه و اطلاعات (ENISA) و شبکه‌های هماهنگی بین‌المللی، نقش کلیدی در ارتقای امنیت زیرساخت‌ها، تبادل اطلاعات و مقابله با تهدیدات سایبری ایفا می‌کنند. نظام‌های منطقه‌ای دیگر نیز مشابه اروپا تلاش می‌کنند با تدوین استانداردها و پروتکل‌های مشترک، همکاری میان کشورها را تقویت کنند، ظرفیت‌های فنی و قانونی را بهبود بخشند و تعارض میان آزادی‌های فردی و الزامات امنیتی را به حداقل برسانند. تجربه اتحادیه اروپا نشان می‌دهد که رویکرد مبتنی بر حقوق شهروندی، همراه با هماهنگی منطقه‌ای و همکاری بین‌دولتی، می‌تواند امنیت سایبری را ارتقا دهد و در عین حال آزادی‌ها و حریم خصوصی کاربران را حفظ کند، ولی این نظام‌ها نیز با چالش‌هایی همچون اختلاف منافع ملی، تهدیدات فراملی و نیاز به به‌روزرسانی مداوم سیاست‌ها مواجه‌اند.

۵-۳- تجربه کشورهای در حال توسعه

تجربه کشورهای در حال توسعه در مدیریت رابطه میان آزادی‌های فردی و امنیت سایبری با چالش‌ها و محدودیت‌های خاص خود همراه است. بسیاری از این کشورها زیرساخت‌های دیجیتال نوپایی دارند و ظرفیت فنی، نهادی و قانونی آن‌ها برای مقابله با تهدیدات سایبری هنوز به سطح کافی نرسیده است، در حالی که نیاز به حفاظت از داده‌ها و خدمات حیاتی و همزمان تضمین آزادی‌های شهروندان وجود دارد. برخی کشورها با تمرکز بیش از حد بر امنیت ملی، محدودیت‌های گسترده‌ای بر دسترسی به اینترنت، شبکه‌های اجتماعی و محتوای آنلاین اعمال می‌کنند که پیامدهایی مانند کاهش آزادی بیان، تضعیف اعتماد عمومی و کاهش مشارکت دیجیتال را به همراه دارد. در مقابل، کشورهایی که رویکرد آزادی‌گرایانه‌تری دارند، گاه با آسیب‌پذیری بالای زیرساخت‌ها و افزایش جرایم سایبری مواجه می‌شوند، زیرا سازوکارهای امنیتی و نظارتی کافی توسعه نیافته‌اند (احترام و رشیدی، ۱۳۹۳). تجربه این کشورها نشان می‌دهد که موفقیت در حکمرانی سایبری نیازمند ترکیبی از تدوین قوانین مؤثر، سرمایه‌گذاری در ظرفیت‌های فنی، تقویت نهادهای نظارتی، آموزش کاربران و ایجاد همکاری میان دولت، بخش خصوصی و جامعه مدنی است. همچنین، پیوستن به شبکه‌ها و توافقات بین‌المللی و بهره‌گیری از تجربیات کشورهای پیشرفته می‌تواند به کاهش تعارض میان آزادی‌های فردی و الزامات امنیت ملی کمک کند و مسیر دستیابی به حاکمیت سایبری متوازن را هموار سازد.

نتایج و پیشنهادات

فضای مجازی به دلیل ماهیت بی‌مرز و چندلایه خود، هم فرصت‌های بی‌سابقه‌ای برای توسعه اقتصادی، فرهنگی و اجتماعی فراهم کرده و هم تهدیدات نوینی را به همراه آورده است که امنیت ملی و حقوق شهروندان را همزمان به چالش می‌کشد. از این منظر، حاکمیت سایبری نه تنها ابزار کنترل و مدیریت فعالیت‌ها و منابع دیجیتال است، بلکه چارچوبی برای تحقق تعادل میان آزادی‌ها و امنیت محسوب می‌شود. دولت‌ها در این عرصه نقش‌های متعددی ایفا می‌کنند؛ آن‌ها قانون‌گذار، ناظر، حافظ امنیت و تضمین‌کننده حقوق شهروندان هستند و موفقیت آن‌ها در حکمرانی سایبری مستلزم سیاست‌گذاری هوشمند، هماهنگی نهادی، مشارکت فعال بخش خصوصی و جامعه مدنی و پاسخ‌گویی شفاف به شهروندان است. تجزیه و تحلیل ابعاد قانونی و حقوقی نشان می‌دهد که تدوین مقررات شفاف و منطبق با استانداردهای بین‌المللی، پایه‌ای برای محدودسازی مشروع و متناسب آزادی‌های فردی در شرایط اضطراری فراهم می‌آورد و امکان بازخواست دولت را از منظر حقوق شهروندی تضمین می‌کند. از بعد امنیتی، دولت‌ها باید توانمندی‌های فنی و نهادی لازم برای مقابله با تهدیدات سایبری پیچیده، مدیریت بحران‌ها، محافظت از زیرساخت‌های حیاتی و تضمین تداوم خدمات عمومی را توسعه دهند. در عین حال، تجارب تطبیقی نشان می‌دهد که حتی در نظام‌های دموکراتیک پیشرفته مانند ایالات متحده و اتحادیه اروپا، تعارض میان آزادی‌های فردی و الزامات امنیت ملی همواره وجود دارد و تلاش برای یافتن توازن نیازمند بازنگری مستمر در سیاست‌ها، قوانین و سازوکارهای نظارتی است. کشورهای در حال توسعه نیز با محدودیت‌های فناورانه، نهادی و قانونی مواجه‌اند و تجربه آن‌ها نشان می‌دهد که تمرکز افراطی بر هر یک از دو محور امنیت یا آزادی می‌تواند پیامدهای منفی گسترده‌ای داشته باشد؛ از جمله کاهش اعتماد عمومی، آسیب‌پذیری زیرساخت‌ها، کاهش مشارکت دیجیتال، تضعیف نوآوری و حتی مخاطرات حقوقی و سیاسی.

پیشنهادها و راهکارهای عملی برای تحقق توازن، شامل رعایت اصول بنیادین مانند تناسب اقدامات امنیتی، شفافیت، پاسخ‌گویی، حاکمیت قانون، انعطاف‌پذیری سیاست‌ها و مشارکت چندسطحی میان دولت، بخش خصوصی و جامعه مدنی است. شفافیت و پاسخ‌گویی، اعتماد عمومی را تقویت کرده و از اعمال محدودیت‌های غیرضروری جلوگیری می‌کنند، در حالی که حاکمیت قانون تضمین می‌کند اقدامات امنیتی مشروع و قابل دفاع باشند. همکاری میان سه ضلع اصلی حکمرانی سایبری باعث می‌شود ظرفیت‌های فنی، نظارتی و اجتماعی ارتقا یافته و تعارض میان آزادی و امنیت به حداقل برسد. علاوه بر این، تجربه‌های تطبیقی بین‌المللی و منطقه‌ای نشان می‌دهد که تدوین استانداردهای هماهنگ، مشارکت در توافقات فراملی و به‌کارگیری راهکارهای مبتنی بر حقوق شهروندی، از مؤلفه‌های کلیدی ایجاد توازن پایدار در سطح ملی و فراملی هستند. موفقیت در حکمرانی سایبری مستلزم نگاه جامع و چندبعدی است که به همزمانی الزامات امنیتی و حفاظت از آزادی‌های فردی توجه داشته باشد. دولت‌ها نمی‌توانند تنها بر امنیت تمرکز کنند بدون آنکه اعتماد و مشارکت شهروندان را از دست دهند، و از سوی دیگر، آزادی‌های دیجیتال نمی‌تواند بدون تمهیدات امنیتی کافی رها شود. توازن میان این دو عنصر نیازمند سیاست‌گذاری مستمر، ارزیابی ریسک‌ها، بازنگری قوانین، توسعه ظرفیت‌های فناورانه و نهادی، و تعامل فعال با بخش خصوصی و جامعه مدنی است. به عبارت دیگر، حکمرانی سایبری موفق، ترکیبی از

امنیت، آزادی، شفافیت، پاسخ‌گویی و همکاری چندسطحی است که نه تنها کشورها را در برابر تهدیدات نوین محافظت می‌کند، بلکه امکان استفاده مسئولانه، مطمئن و پایدار از فضای مجازی را برای شهروندان فراهم می‌آورد و پایه‌ای برای توسعه دیجیتال، انسجام اجتماعی و مشروعیت سیاسی در قرن بیست و یکم ایجاد می‌کند. به همین دلیل، دولت‌ها باید همواره تعادل میان آزادی و امنیت را به عنوان یک فرآیند پویا و مستمر مدیریت کنند و ضمن بهره‌گیری از تجربه‌های داخلی و بین‌المللی، سیاست‌ها و راهکارهای خود را با تغییرات فناوری و تهدیدات نوین تطبیق دهند تا حاکمیت سایبری متوازن و پایدار تحقق یابد.

منابع

۱) احترام، محسن و رشیدی، قاسم (۱۳۹۳). بررسی و وضع قوانین و امنیت سایبری در توسعه اقتصادی کشورهای در حال توسعه. مقاله ارائه شده به سومین همایش سراسری علوم و مهندسی دفاعی در سپاه، ۱-۲۱.

۲) بحرینی، محمدرسول (۱۴۰۳). چالش‌ها و راهکارهای حفاظت از آزادی‌های مدنی در برابر نظارت دیجیتال در فضای مجازی. مقاله ارائه شده به نهمین کنفرانس بین‌المللی فقه، حقوق در ایران و جهان اسلام، ۱-۲۵.

۳) بذرگر، امیر (۱۳۹۴). نقش دولت و جامعه مدنی در پیشگیری از وقوع جرم در فضای مجازی. پایان‌نامه کارشناسی ارشد، دانشگاه علامه طباطبایی.

۴) برون، مهرداد (۱۴۰۳). حکمرانی سایبری، مفهوم و ضرورت. مقاله ارائه شده به اولین کنفرانس ملی حکمرانی و نظام سیاست‌گذاری فرهنگی، ۱-۲۲.

۵) جعفری‌نیا، محمدجواد (۱۴۰۳). امنیت در فضای مجازی. تهران: نشر نسیم کوثر.

۶) جلالی‌شاد، سیدمهدی (۱۴۰۳). فضای مجازی در نظم حقوقی. تهران: نشر ارشدان.

۷) حاتمی، فاطمه و حیدری، کوثر (۱۴۰۳). حاکمیت و رهبری دیجیتال. مقاله ارائه شده به اولین همایش ملی حسابداری و مدیریت کسب‌وکار در دنیای دیجیتال، ۱-۲۵.

۸) حسین‌پور، پری و صابرنژاد، علی (۱۳۹۴). آزادی اطلاعات در فضای سایبر از منظر حقوق بین‌الملل. تهران: نشر مجد.

۹) شمعی، محمد و احمدی، سیدمحمدصادق (۱۳۹۹). تقابل و توازن امنیت و آزادی در دولت قانون‌مدار. تهران: نشر میزان.

۱۰) غلامی، مصطفی (۱۳۹۹). فضای مجازی از دریچه قانون. تهران: نشر شیل.

۱۱) فرزام‌نیا، نیما و عبدی، بهنام (۱۴۰۲). ارائه چهارچوب معماری حاکمیت امنیت سایبری در سازمان‌های دفاعی جمهوری اسلامی ایران. نشریه علوم و فنون نظامی، ۱۹(۶۴): ۲۴۱-۲۶۸.

۱۲) معطری، محمدعلی و مصلی‌نژاد، احمد (۱۴۰۳). امنیت سایبری اتحادیه اروپا: فرصت‌ها، تهدیدات و اقدامات. مقاله ارائه شده به اولین کنفرانس بین‌المللی فناوری اطلاعات، مدیریت و کامپیوتر، ۱-۲۰.

۱۳) ملکی، روح‌الله و جمالی، جواد (۱۴۰۳). مطالعه مقایسه‌ای قوانین سایبری چین، ایالات متحده آمریکا و روسیه، بایسته‌ها و ضرورت‌های امنیت سایبری جمهوری اسلامی ایران. نشریه آماد و فناوری دفاعی، ۷(۲۳): ۷۷-۱۰۸.

۱۴) مؤمنی، حسین (۱۴۰۳). نظریه‌ها و رویکردها در فضای مجازی. تهران: نشر زرنوشت.