Legal Studies in Cyberspace

مطالعات حقوقی فضای مجازی

Received: 2025/04/30
Accepted: 2025/08/29
Publish: 2025/12/28
Pages: 21 - 35

ISSN: 2821-126X
https://sanad.iau.ir/journal/cyberlaw :وبگاه مجله

Volume 4, Issue 15, Fall 2025
Article Type: **Research**
DOI: 10.71488/cyberlaw.2025.1229824

Good Governance and Ensuring Cybersecurity

Glena Khalil Hasan

Department of Law Public, Na.C., Islamic Azad University, Najafabad, Iran

Masoud Raei

Department of Law, Na.C., Islamic Azad University, Najafabad, Iran

(Corresponding Author), Email: masoudraei@yahoo.com

Alireza Ansari Mahyari

Department of Law, Na.C., Islamic Azad University, Najafabad, Iran

Abstract

Today, cybersecurity is a highly important and vital issue in all countries, and all nations are striving to ensure the security of this space by enacting and implementing numerous rules and laws in this regard. Cyberspace requires assurance, and naturally, the existence of this assurance depends on the presence of transparent, accountable, and participatory structures, a concept that is observable in good governance. The absence of transparent, accountable, and participatory structures in the governance domain exacerbates cyber vulnerabilities and diminishes the capacity to counter threats. In a good governance system, transparency in cyber laws and regulations plays a central role. This transparency enables organizations and citizens to understand cyber risks and take appropriate preventive measures. Laws must be clearly formulated and easily accessible to the public. Additionally, responsible institutions must be accountable for their actions against cyber threats, and effective mechanisms for follow-up and accountability must exist. Using a descriptive-analytical method, the researcher has concluded that good governance in the field of cybersecurity also requires an efficient and effective organizational structure. This structure must have the capability for coordination, planning, and implementation of preventive and responsive measures. In summary, good governance in cybersecurity contributes to building trust and security in cyberspace and leads to the country's economic and social progress. Neglecting this issue can result in irreparable economic and social damages.

Keywords: Ensuring Cybersecurity, Cybercrimes, Challenges of Good Governance, Good Governance.

❋Citation (APA): Khalil Hasan, G, Raei, M. Ansari Mahyari, A. (2025). Good Governance and Ensuring Cybersecurity. *Cyberspace legal studies, 4(15), 21 - 35*

مطالعات حقوقی فضای مجازی
Legal Studies in Cyberspace
ISSN: 2821-126X
ویگاه مجله: https://sanad.iau.ir/journal/cyberlaw

تاریخ دریافت: ۱۴۰۴/۰۲/۱۰
تاریخ پذیرش: ۱۴۰۴/۰۶/۰۷
تاریخ انتشار: ۱۴۰۴/۱۰ /۰۷
صفحه: ۲۱ الی ۳۵

دوره ۴ / شماره ۱۵ / پاییز ۱۴۰۴
نوع مقاله: پژوهشی
DOI: 10.71488/cyberlaw.2025.1229824

حکمرانی خوب و تضمین امنیت سایبری

گلینه خلیل حسن

گروه حقوق عمومی، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران

مسعود راعی

گروه حقوق، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران

(نویسنده مسئول) ایمیل: masoudraei@yahoo.com

علیرضا انصاری مهیاری

گروه حقوق، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران

چکیده

امروزه امنیت سایبری در تمامی کشورها، موضوعی بسیار مهم و حیاتی بوده و تمامی کشورها برای تضمین امنیت این فضا در تلاش بوده و قواعد و قوانین متعددی را در این زمینه وضع و اجرا می نمایند. فضای سایبر نیازمند تضمین بوده و طبیعتاً وجود این تضمین منوط بر وجود ساختارهای شفاف، پاسخگو و مشارکتی بوده و این معنا در حکمرانی خوب قابل مشاهده می باشد. عدم وجود ساختارهای شفاف، پاسخگو و مشارکتی در حوزه حکمرانی، آسیب‌پذیری‌های سایبری را تشدید می‌کند و از توانایی مقابله با تهدیدات می‌کاهد. در یک سیستم حکمرانی خوب، شفافیت در قوانین و مقررات سایبری، نقش محوری دارد. این شفافیت، به سازمان‌ها و شهروندان اجازه می‌دهد تا خطرات سایبری را درک کرده و اقدامات پیشگیرانه مناسبی انجام دهند. قوانین باید به‌طور شفاف تدوین شده و به آسانی در دسترس عموم قرار گیرند. همچنین نهادهای مسئول باید در قبال اقدامات خود در برابر تهدیدات سایبری پاسخگو باشند و مکانیزم‌های موثری برای پیگیری و رفع مسئولیت وجود داشته باشد. پژوهشگر با استفاده از روش توصیفی تحلیلی، به این نتیجه رسیده است که حکمرانی خوب در زمینه امنیت سایبری نیز مستلزم وجود یک ساختار سازمانی کارآمد و موثر است. این ساختار باید از توانایی هماهنگی، برنامه‌ریزی و اجرای اقدامات پیشگیرانه و واکنشی برخوردار باشد. در مجموع حکمرانی خوب در زمینه امنیت سایبری به ایجاد اعتماد و امنیت در فضای سایبری کمک می‌کند و به پیشرفت اقتصادی و اجتماعی کشور می‌انجامد. عدم توجه به این موضوع، می‌تواند منجر به خسارات اقتصادی و اجتماعی جبران‌ناپذیری شود.

کلیدواژگان: تضمین امنیت سایبری، جرایم سایبری، چالشهای حکمرانی خوب، حکمرانی خوب.

*استناددهی (APA): خلیل حسن، گلینه. راعی، مسعود. انصاری مهیاری، علیرضا. (۱۴۰۴). حکمرانی خوب و تضمین امنیت سایبری. *مطالعات حقوقی فضای مجازی، ۴(۱۵)*، ۲۱ – ۳۵

مقدمه

در عصری که فناوری اطلاعات و ارتباطات به سرعت در حال تحول است و زندگی روزمره را به طور فزاینده‌ای تحت تأثیر قرار می‌دهد، امنیت سایبری به یکی از مهم‌ترین چالش‌های پیش روی جوامع تبدیل شده است. وابستگی روزافزون به زیرساخت‌های دیجیتالی، از سیستم‌های بانکی و مالی گرفته تا سیستم‌های انرژی و مراقبت‌های بهداشتی، ما را در معرض طیف وسیعی از تهدیدات سایبری قرار می‌دهد. از حملات سایبری هدفمند توسط گروه‌های تروریستی و دولتی گرفته تا حملات باج‌افزاری توسط مجرمان سایبری، هر روز شاهد ظهور تهدیدات جدید و پیچیده‌تری هستیم. این تهدیدات نه تنها می‌توانند به خسارات مالی سنگین منجر شوند، بلکه می‌توانند به زیرساخت‌های حیاتی آسیب رسانده و امنیت ملی را به خطر اندازند. در این میان، نقش حکمرانی خوب در تضمین امنیت سایبری از اهمیت ویژه‌ای برخوردار است. حکمرانی خوب، به معنای وجود ساختارهای شفاف، پاسخگو و مشارکتی در حوزه مدیریت و نظارت بر سیستم‌های سایبری است. این ساختارها باید بتوانند به‌طور موثر با تهدیدات سایبری مقابله کرده و از امنیت داده‌ها و سیستم‌ها محافظت کنند.عدم وجود حکمرانی خوب در زمینه امنیت سایبری می‌تواند پیامدهای جبران‌ناپذیری داشته باشد. شفافیت نبودن قوانین و مقررات، موجب ابهام و عدم اطمینان می‌شود و سازمان‌ها را در مقابله با تهدیدات سایبری ناتوان می‌کند. عدم پاسخگویی نهادهای مسئول، به ایجاد فرهنگ بی‌مسئولیتی و بی‌توجهی به امنیت سایبری می‌انجامد. عدم مشارکت ذینفعان مختلف در تصمیم‌گیری‌ها نیز می‌تواند به ضعف و ناتوانی در مقابله با تهدیدات سایبری منجر شود. در یک سیستم حکمرانی خوب، تمام ذینفعان، از بخش دولتی و بخش خصوصی گرفته تا جامعه مدنی و افراد، باید در تصمیم‌گیری‌ها و اجرای سیاست‌های مرتبط با امنیت سایبری شرکت داشته باشند .(Cooray et al, 2024: 26)یک سیستم حکمرانی خوب در زمینه امنیت سایبری، باید بر اساس اصول مهمی مانند شفافیت، پاسخگویی، مشارکت، و کارایی استوار باشد. شفافیت به معنای در دسترس بودن اطلاعات مرتبط با سیاست‌های امنیت سایبری و خطرات موجود برای عموم است. پاسخگویی به معنای مسئولیت‌پذیری نهادهای مسئول در قبال اقدامات خود و توانایی پیگیری و رفع مسئولیت در صورت وقوع حمله سایبری است. مشارکت به معنای در نظر گرفتن نظرات و دیدگاه‌های تمام ذینفعان در طراحی و اجرای سیاست‌های امنیت سایبری است. و در نهایت، کارایی به معنای توانایی سیستم در مقابله موثر با تهدیدات سایبری و حفاظت از زیرساخت‌های دیجیتالی است. تأمین امنیت سایبری نیازمند یک رویکرد چند جانبه و یکپارچه است که در آن تمام بخش‌ها و نهادهای مرتبط به طور هماهنگ با هم کار کنند. حکمرانی خوب، نقش اساسی در ایجاد این رویکرد یکپارچه و موثر داشته و به ایجاد یک سیستم امنیت سایبری قوی و پایدار کمک می‌کند. این سیستم باید از توانایی پیشگیری، کاهش و واکنش به تهدیدات سایبری برخوردار باشد. و در نهایت، حکمرانی خوب به ایجاد اعتماد به نفس و امنیت در فضای سایبری کمک می‌کند و زمینه را برای رشد و توسعه اقتصادی و اجتماعی فراهم می‌آورد. سوال اصلی در این پژوهش این است که حکمرانی خوب چه نقشی در زمینه تضمین امنیت سایبری دارد؟ در این زمینه می توان عنوان نمود که حکمرانی خوب با ایجاد چارچوب‌های قانونی شفاف و پاسخگو، مشارکت ذینفعان و سرمایه‌گذاری در زیرساخت‌های امن، به ارتقای امنیت سایبری کمک می‌کند. این امر از طریق افزایش آگاهی عمومی، تقویت همکاری بین‌المللی و توانمندسازی نهادهای مسئول در مقابله با تهدیدات سایبری محقق می‌شود. در نتیجه، حکمرانی خوب به ایجاد اعتماد و پایداری در فضای سایبری و کاهش آسیب‌پذیری‌ها در برابر حملات سایبری منجر می‌شود. بنابراین، توجه به حکمرانی خوب در زمینه امنیت سایبری، نه تنها یک اصل مهم بلکه یک ضرورت است. با توجه به افزایش روزافزون تهدیدات سایبری، نیازمند یک سیستم حکمرانی قوی و موثر هستیم که بتواند از امنیت ملی و منافع کشور محافظت کند. این سیستم باید بر اساس شفافیت، پاسخگویی، مشارکت و کارایی طراحی شده و به طور مداوم ارزیابی و به‌روزرسانی شود تا بتواند با تهدیدات جدید و پیچیده مقابله کند.

۱- حکمرانی خوب

حکمرانی خوب، مفهومی چندوجهی و پویا، در قلب تلاش‌های توسعه‌ای و حقوق بشری معاصر قرار دارد. شورای حقوق بشر سازمان ملل متحد، به عنوان مرجع اصلی بین‌المللی در زمینه حقوق بشر، بر اهمیت حکمرانی خوب به عنوان زیربنایی برای تحقق حقوق بشر و توسعه پایدار تاکید فراوان داشته است. بر اساس تعاریف و معیارهای ارائه شده توسط این شورا، حکمرانی خوب را می‌توان به عنوان چارچوبی نظام‌مند برای مدیریت امور عمومی تعریف کرد که در آن قدرت به شکل شفاف، مسئولانه و مشارکت‌آمیز اعمال می‌شود و بر اصول حقوق بشر، حاکمیت قانون و عدالت اجتماعی استوار است. در این تعریف، شفافیت به معنای دسترسی آزاد و آسان به اطلاعات مرتبط با تصمیمات و سیاست‌های دولت است(ساری ،۴۲:۲۰۲۳). این شامل حق دسترسی به اطلاعات، انتشار اطلاعات عمومی به صورت منظم و قابل فهم، و وجود سازوکارهایی برای پاسخگویی به سوالات و ابهامات شهروندان است. یک دولت با حکمرانی خوب، نه تنها اطلاعات را در دسترس قرار می‌دهد بلکه فعالانه به دنبال تعامل با شهروندان و دریافت بازخورد از آنها است(چانسا چاندا ،۶۱۴:۲۰۲۴).مسئولیت‌پذیری عنصر دیگری از حکمرانی خوب است که به معنای پاسخگو بودن دولت و نهادهای عمومی در قبال اقدامات و تصمیمات خود است. این شامل وجود سازوکارهایی برای پیگیری و رسیدگی به شکایات شهروندان، ارائه توضیحات منطقی برای تصمیمات، و تضمین مجازات در صورت سوء استفاده از قدرت است. یک دولت مسئولیت‌پذیر نه تنها در قبال قانون، بلکه در برابر مردم خود نیز پاسخگو است.

مقوله مشارکت، به معنای درگیر کردن شهروندان در فرآیندهای تصمیم‌گیری و سیاست‌گذاری است. این شامل حق شرکت در انتخابات آزاد و عادلانه، حق دسترسی به مکانیسم‌های مشاوره و نظارت عمومی، و حق ابراز نظر در مورد مسائل عمومی است. حکمرانی خوب زمانی به بهترین شکل عمل می‌کند که صدای همه ذینفعان، به ویژه گروه‌های حاشیه‌نشین و آسیب‌پذیر، شنیده شود. این مشارکت نه تنها مشروعیت تصمیمات را افزایش می‌دهد بلکه منجر به نتایج بهتر و عادلانه‌تر نیز می‌شود(آستوتی ،۱۴:۲۰۲۱). حاکمیت قانون، به معنای الزام همه، از جمله دولت، به پیروی از قانون است. این شامل وجود یک نظام قضایی مستقل و کارآمد، تضمین حقوق متهمان، و اعمال یکسان قانون بر همه افراد است. حاکمیت قانون، نه تنها از حقوق فردی محافظت می‌کند بلکه از سوء استفاده از قدرت و فساد جلوگیری می‌کند. یک نظام مبتنی بر حاکمیت قانون، تضمینی برای ثبات و امنیت سیاسی و اجتماعی است. عدالت اجتماعی، به معنای توزیع عادلانه منابع و فرصت‌ها و ایجاد شرایطی برای مشارکت برابر همه در زندگی اقتصادی، اجتماعی و سیاسی است. این شامل دسترسی برابر به خدمات اساسی مانند آموزش و بهداشت، حمایت از حقوق گروه‌های آسیب‌پذیر، و تضمین فرصت‌های برابر برای همه است. حکمرانی خوب، به دنبال ایجاد یک جامعه عادلانه و فراگیر است که در آن همه افراد از حقوق و فرصت‌های برابر برخوردار باشند(ریزال ،۱۷۶:۲۰۲۱). در مجموع، حکمرانی خوب با این معیارها و تعاریف به دنبال ایجاد یک جامعه‌ای است که در آن حقوق بشر رعایت شود، توسعه پایدار شکل بگیرد و عدالت اجتماعی برقرار باشد.

۲- امنیت سایبری

مبحث امنیت سایبری به مجموعه‌ای از فناوری‌ها، فرآیندها و رویه‌ها اشاره دارد که هدف آن حفاظت از سیستم‌های کامپیوتری، شبکه‌ها، داده‌ها و اطلاعات در برابر حملات، دسترسی‌های غیرمجاز و آسیب‌هاست. با توجه به پیشرفت‌های تکنولوژیکی و فزونی استفاده از اینترنت و سیستم‌های دیجیتال، امنیت سایبری به یکی از دغدغه‌های اصلی سازمان‌ها، دولت‌ها و افراد تبدیل شده است. این امنیت نه تنها شامل حفاظت از سخت‌افزار و نرم‌افزار، بلکه همچنین مستلزم تأمین امنیت داده‌ها و اطلاعاتی است که در این زیرساخت‌ها ذخیره و پردازش می‌شوند(ودیکا ،۱۳۴:۲۰۲۴).یکی از چالش‌های کلیدی در امنیت سایبری، شناسایی و ارزیابی تهدیدات است. تهدیدات سایبری می‌توانند از انواع مختلفی نشأت بگیرند، از جمله حملات سایبری ناشی از هکرها، بدافزارها و حملات داس . هر یک از این تهدیدات می‌تواند به عملکرد سازمان‌ها آسیب برساند و حتی به نشت اطلاعات حساس و خصوصی منجر شود(صدیقی، ۱۴۰۱: ۲۶). به همین دلیل، شناسایی زودهنگام این تهدیدات و ارزیابی

آسیب‌پذیری‌های موجود در سیستم‌ها اهمیت فوق‌العاده‌ای دارد. در این راستا، به‌کارگیری ابزارهای روزآمد شناسایی و تجزیه و تحلیل تهدیدات ضروری است. به‌علاوه، مدیریت ریسک یکی از ارکان اصلی امنیت سایبری محسوب می‌شود. این فرایند شامل شناسایی، ارزیابی و اولویت‌بندی ریسک‌های امنیتی و سپس اتخاذ اقداماتی برای کاهش آن‌ها است(علاء تکلیف، ۱۴۰۲: ۴۱). بسیاری از حملات سایبری نتیجه رفتارهای ناامن کاربران است، از قبیل استفاده از رمزهای عبور ضعیف یا نادیده گرفتن هشدارهای امنیتی. به همین دلیل، آموزش مستمر کاربران و کارکنان در مورد بهترین شیوه‌های امنیت سایبری و حملات رایج، می‌تواند به کاهش خطرات و حفاظت از اطلاعات کمک شایانی کند. برگزاری کارگاه‌های آموزشی و شبیه‌سازی حملات می‌تواند به کاربران کمک کند تا به‌خوبی با خطرات آشنا شوند و توانایی واکنش مناسب در برابر آن‌ها را پیدا کنند. علاوه بر این، مقررات و سیاست‌های قانونی در زمینه امنیت سایبری نقش بسیار مهمی ایفا می‌کنند(جاسب جاسب، ۱۴۰۲: ۶۸). دولت‌ها و نهادهای بین‌المللی مانند سازمان ملل متحد و اتحادیه اروپا، تلاش می‌کنند تا چارچوب‌های قانونی و استانداردهای بین‌المللی را برای پیشگیری از جرائم سایبری و حفاظت از داده‌های شخصی تدوین کنند. امنیت سایبری یک امر پویا و در حال تحول است که مستلزم همکاری و تبادل اطلاعات در سطح ملی و بین‌المللی است. با توجه به پیچیدگی حملات و تغییرات سریع فناوری، هیچ سازمانی به‌تنهایی نمی‌تواند به‌طور کامل از خود در برابر تهدیدات سایبری محافظت کند(رحمدل و کامکار، ۱۴۰۰: ۴۲). به همین دلیل، ایجاد شبکه‌های همکاری، اشتراک‌گذاری اطلاعات و توسعه راهکارهای مشترک از اهمیت ویژه‌ای برخوردار است. این نوع همکاری می‌تواند به تقویت امنیت سایبری جهانی کمک کرده و توانمندی نهادها و کشورهای مختلف را در مواجهه با تهدیدات سایبری افزایش دهد.

۳- ضرورت امنیت سایبری

امنیت سایبری به‌عنوان یک عنصر حیاتی در عصر دیجیتال معاصر، نقشی اساسی در حفاظت از اطلاعات و زیرساخت‌های حیاتی دارد. با توجه به رشد روزافزون استفاده از فناوری‌های اطلاعاتی و ارتباطی، تهدیدات سایبری به‌صورت فزاینده‌ای در حال افزایش هستند. این تهدیدات می‌توانند ناشی از اعمال خرابکارانه هکرها، بازیگران دولتی و گروه‌های سازمان‌یافته باشند که هدف آن‌ها تخریب، سرقت یا دسترسی غیرمجاز به اطلاعات حساس است(کریس ،۹۴۷:۲۰۲۱). بنابراین، اهمیت امنیت سایبری به‌ویژه در حفاظت از داده‌های شخصی، مالی و سازمانی قابل‌توجه است. حفاظت از این اطلاعات نه‌تنها به‌منظور جلوگیری از خسارات مالی، بلکه به‌دلیل حفظ اعتبار و اعتماد کاربران نیز ضروری است(صادقی ساروکلائی، ۱۴۰۱: ۴۱). یکی از جنبه‌های حیاتی امنیت سایبری، تأمین امنیت زیرساخت‌های ارتباطی و فناوری اطلاعات است که بخش‌های مختلف کشور، از جمله بهداشت، حمل‌ونقل و انرژی، به آن وابسته هستند. اختلالات در این زیرساخت‌ها می‌تواند منجر به بحران‌های جدی و تضعیف عملکرد نهادهای عمومی و خصوصی گردد. به‌ویژه در زمان شیوع بحران‌های بهداشتی یا حوادث طبیعی، الزامات امنیتی سایبری در سطح ملی و بین‌المللی دوچندان می‌شود. بنابراین، سرمایه‌گذاری در امنیت سایبری و تقویت توانمندی‌های دفاعی در این حوزه از اولویت‌های کلیدی سیاست‌گذاران و سازمان‌ها به شمار می‌آید(رضوی پور و همکاران، ۱۴۰۱: ۰۷). اهمیت امنیت سایبری در حمایت از حقوق بشر و حریم خصوصی نیز غیرقابل‌انکار است. در عصر دیجیتال، بسیاری از اطلاعات شخصی کاربران در فضای آنلاین ذخیره می‌شود و هرگونه نقض امنیتی می‌تواند به افشای این اطلاعات و نقض حریم خصوصی منجر شود. این مسئله از طرفی می‌تواند به تبعات اجتماعی و روانی منفی برای افراد منجر شده و از سوی دیگر، به تخریب اعتماد عمومی به نهادها و سازمان‌های دولتی و خصوصی آسیب بزند. لذا، تأمین امنیت اطلاعات شخصی و حساس در برابر دسترسی غیرمجاز برای حمایت از حقوق بنیادین شهروندان امری ضروری است(محمودی و بحرکاظمی، ۱۴۰۳: ۱۲۵). از دیگر ابعاد اهمیت امنیت سایبری، تأثیر آن بر رشد و توسعه اقتصادی کشورهاست. با توجه به دیجیتالی شدن فرآیندهای اقتصادی و تجاری، امنیت سایبری به یکی از مولفه‌های کلیدی در جذب سرمایه‌گذاری و حفظ رقابت‌پذیری تبدیل شده است. سرمایه‌گذاران و شرکت‌ها به دنبال محیط‌هایی هستند که امنیت و ثبات سایبری در آن‌ها تضمین شده باشد. بنابراین، کشورهایی که قادر به ایجاد بسترهای امن سایبری هستند، از مزایای رقابتی در جذب سرمایه‌گذاری و رشد اقتصادی برخوردار خواهند بود. همچنین، امنیت سایبری از

بروز نارضایتی‌های اجتماعی و تهدیدات امنیتی داخلی جلوگیری می‌کند(بلوجی، ۱۴۰۱: ۱۹۳). حملات سایبری می‌توانند منجر به نارضایتی‌های اجتماعی و تضعیف اعتماد به نهادهای دولتی شوند. به‌ویژه در جوامعی که به‌دلیل مشکلات اقتصادی و اجتماعی در بحران به سر می‌برند، تهدیدات سایبری می‌تواند به تشدید تضادها و تنش‌ها منجر گردد. لذا، تأمین امنیت سایبری به‌عنوان یک ابزار پیشگیرانه در کاهش این تنش‌ها و حفظ ثبات اجتماعی و سیاسی مورد توجه قرار می‌گیرد(پرادیتا ،۱۵:۲۰۲۳). در نهایت، اهمیت امنیت سایبری می‌تواند از منظر ملی و جهانی نیز بررسی شود. تهدیدات سایبری نه‌تنها محدود به مرزهای یک کشور نمی‌شوند، بلکه می‌توانند به‌صورت فرامرزی گسترش یابند(افراشته و همکاران، ۱۴۰۳: ۰۳). با توجه به چالش‌های جهانی که جوامع امروز با آن مواجه هستند، مانند تروریسم سایبری و حملات پیچیده، همکاری‌های بین‌المللی می‌تواند به تقویت امنیت سایبری در سطح جهانی و حفاظت از منافع مشترک بشر کمک کند.

۴- رابطه حکمرانی خوب و امنیت سایبری

رابطه حکمرانی خوب و امنیت سایبری به عنوان دو مفهوم کلیدی در دنیای معاصر، اهمیت ویژه‌ای پیدا کرده است. حکمرانی خوب به مجموعه‌ای از اصول و شیوه‌های مدیریتی اشاره دارد که هدف آن ارتقاء کیفیت زندگی شهروندان و تضمین حقوق آن‌هاست(جوانمردزاده و همکاران، ۱۴۰۰: ۰۳). از سوی دیگر، امنیت سایبری به حفاظت از سیستم‌ها، شبکه‌ها و داده‌ها در برابر تهدیدات دیجیتال مربوط می‌شود. این دو مفهوم به طور مستقیم با یکدیگر مرتبط هستند و وجود حکمرانی خوب می‌تواند به تقویت امنیت سایبری کمک کند(نگهدار و همکاران، ۱۴۰۲: ۰۶). حکمرانی خوب شامل شفافیت، پاسخگویی، مشارکت و حاکمیت قانون است. این اصول به دولت‌ها کمک می‌کند تا به طور مؤثرتر با چالش‌های امنیتی مواجه شوند. برای مثال، شفافیت در فرآیندهای تصمیم‌گیری می‌تواند به افزایش اعتماد عمومی نسبت به اقدامات امنیتی کمک کند. اگر شهروندان احساس کنند که دولت در زمینه امنیت سایبری شفاف عمل می‌کند، احتمال بیشتری وجود دارد که همکاری کنند و اطلاعات لازم را برای مقابله با تهدیدات ارائه دهند(فرزام نیا و عبدی، ۱۴۰۰: ۱۴). پاسخگویی نیز یکی از ارکان حکمرانی خوب است. دولت‌ها باید در قبال اقدامات خود در حوزه امنیت سایبری پاسخگو باشند. این بدین معناست که اگر یک نقص امنیتی رخ دهد، دولت باید بتواند توضیح دهد که چه اقداماتی انجام داده و چه تدابیری برای جلوگیری از تکرار آن اتخاذ خواهد کرد .

مشارکت عمومی نیز در حکمرانی خوب از اهمیت بالایی برخوردار است. دولت‌ها باید فضایی را فراهم کنند که شهروندان بتوانند در فرآیندهای تصمیم‌گیری مرتبط با امنیت سایبری مشارکت داشته باشند. این مشارکت می‌تواند شامل مشاوره با متخصصان فناوری اطلاعات، برگزاری جلسات عمومی و استفاده از نظرات مردم در تدوین سیاست‌های امنیتی باشد. این رویکرد نه تنها باعث افزایش کیفیت تصمیمات می‌شود بلکه احساس تعلق و مسئولیت‌پذیری را در میان شهروندان تقویت می‌کند(بیات کمیتکی و موهبتی، ۱۴۰۳: ۲۶۳). حاکمیت قانون نیز یکی دیگر از جنبه‌های مهم حکمرانی خوب است که تأثیر زیادی بر امنیت سایبری دارد. وجود قوانین مشخص و شفاف در زمینه حفاظت از داده‌ها و اطلاعات شخصی می‌تواند به کاهش تهدیدات سایبری کمک کند. اگر قوانین به وضوح تعیین کنند که چه اقداماتی غیرقانونی است و چه مجازاتی برای نقض آن‌ها وجود دارد، احتمال وقوع جرائم سایبری کاهش می‌یابد(سراوانان و سوره، ۶:۲۰۲۴). علاوه بر این، حکمرانی خوب می‌تواند به توسعه زیرساخت‌های فناوری اطلاعات و ارتباطات کمک کند. زیرساخت‌های قوی و امن برای تبادل اطلاعات ضروری هستند و بدون آن‌ها، تلاش‌ها برای تقویت امنیت سایبری ممکن است ناکام بماند. دولت‌ها باید سرمایه‌گذاری لازم را در توسعه زیرساخت‌های فناوری اطلاعات انجام دهند تا بتوانند با تهدیدات جدید مقابله کنند(زابیدی ،۸:۲۰۲۴). ایجاد یک فرهنگ امنیتی در جامعه نیز بخشی از حکمرانی خوب است. آموزش شهروندان درباره تهدیدات سایبری و روش‌های پیشگیری از آن‌ها می‌تواند به کاهش آسیب‌پذیری جامعه کمک کند(داراب نیا و همکاران، ۱۴۰۱: ۳۶). اگر مردم نسبت به خطرات سایبری آگاه باشند و بدانند چگونه از خود محافظت کنند، احتمال موفقیت حملات سایبری کاهش می‌یابد.

۱-۴- حکمرانی خوب و بهبود زیرساختهای امنیت سایبری

حکمرانی خوب به مجموعه‌ای از اصول، رویه‌ها و نهادهای مؤثر اشاره دارد که به منظور مدیریت منابع عمومی و اجرای سیاست‌ها به‌کار گرفته می‌شود. این مفهوم در دنیای دیجیتال و در زمینه امنیت سایبری اهمیت ویژه‌ای پیدا کرده است. با افزایش تهدیدات سایبری و حملات دیجیتال، حکمرانی خوب می‌تواند به‌طرز قابل توجهی امنیت زیرساخت‌های سایبری را بهبود بخشد. اولین اثر حکمرانی خوب بر امنیت سایبری، ایجاد مقررات و سیاست‌های مناسب برای حفاظت از داده‌ها و زیرساخت‌های دیجیتال است(پاپل ،۲۰۲۴:۱۶۱). دولت‌ها و نهادهای خصوصی با تدوین قوانین و استانداردهای امنیت سایبری، چارچوبی را فراهم می‌آورند که سازمان‌ها باید بر اساس آن عمل کنند. این قوانین می‌توانند شامل الزامات حفاظتی، مسئولیت‌ها و مجازات‌ها برای نقض امنیت باشند. دومین اثر حکمرانی خوب، هم‌افزایی بین نهادهای مختلف و بخش‌های عمومی و خصوصی است. همکاری و هماهنگی میان این نهادها می‌تواند به بهبود تبادل اطلاعات، تجارب و بهترین شیوه‌ها منجر شود(محمدعلی ، ۶:۲۰۲۴). این تعاملات نه تنها به شناسایی تهدیدات جدید کمک می‌کند، بلکه سرعت واکنش به حملات سایبری را نیز افزایش می‌دهد. حکمرانی خوب همچنین به بهبود آموزش و آگاهی در زمینه امنیت سایبری کمک می‌کند. با فراهم کردن آموزش‌های لازم برای کارمندان دولتی و خصوصی، سازمان‌ها قادر خواهند بود مهارت‌های لازم برای شناسایی و مقابله با تهدیدات سایبری را کسب کنند. این آموزش‌ها می‌توانند شامل دوره‌های آموزشی، کارگاه‌ها و حتی کمپین‌های آگاهی عمومی باشند. اثر دیگری از حکمرانی خوب بر امنیت سایبری، تسهیل دسترسی به منابع مالی و سرمایه‌گذاری در زیرساخت‌های امنیت سایبری است. دولت‌ها می‌توانند از طریق تخصیص منابع مالی مناسب و ارائه تسهیلات به سازمان‌ها، امکانات لازم برای بهبود زیرساخت‌های امنیتی را فراهم کنند(رجبی، ۱۴۰۲: ۱۲). این سرمایه‌گذاری‌ها می‌توانند شامل خرید نرم‌افزارهای امنیتی، استخدام متخصصان در این حوزه و به‌روزرسانی سیستم‌های قدیمی باشند. علاوه بر این، حکمرانی خوب می‌تواند به تقویت بخش تحقیق و توسعه در حوزه امنیت سایبری کمک کند. حمایت از نوآوری و ایجاد شرایط مناسب برای تحقیقات می‌تواند به پیدایش راهکارهای جدید که قادر به مقابله با تهدیدات سایبری هستند، منجر شود. این نوآوری‌ها می‌توانند به شکل تکنولوژی‌های پیشرفته، الگوریتم‌های هوش مصنوعی و نرم‌افزارهای تحلیلی بروز دهند. حکمرانی خوب همچنین بر روی استانداردسازی و مطابقت‌پذیری اثرگذار است. تدوین و اجرای استانداردهای بین‌المللی امنیت سایبری می‌تواند به سازمان‌ها کمک کند تا بهترین شیوه‌ها را در زمینه‌های امنیتی پیاده‌سازی کنند(صالحی، ۱۴۰۲: ۳۲۱). این مسئله نه تنها به افزایش کیفیت امنیت سایبری کمک می‌کند، بلکه اعتماد عمومی به زیرساخت‌های دیجیتال را نیز تقویت می‌کند.

۲-۴- اصول حکمرانی خوب و تضمین امنیت سایبری

نقش اصول حکمرانی خوب در تقویت امنیت سایبری امری حیاتی و چندوجهی می باشد؛ بدون اتکا به اصول اساسی حکمرانی خوب، تلاش‌ها برای ایجاد امنیت سایبری کارآمد و پایدار محکوم به شکست می باشد(اوبوسکا و کرولیسکو ،۲۰۲۲:۱۳۴). این اصول، ستون‌های اصلی یک سیستم امنیتی سایبری قوی و قابل اعتماد را تشکیل می‌دهند:

۱-۲-۴- شفافیت

شفافیت از ارکان اصلی حکمرانی خوب محسوب می‌شود. شفافیت به معنای قابلیت دسترسی به اطلاعات و فرآیندهای تصمیم‌گیری است و در زمینه حکمرانی خوب، به این معناست که حکومت باید بتواند اطلاعات مربوط به فعالیت‌ها، تصمیمات و منابع خود را به‌طور آزادانه و قابل فهم در اختیار شهروندان قرار دهد(زارع زاده، ۱۴۰۰: ۱۵). این اصل به افزایش اعتماد عمومی کمک می‌کند و باعث می‌شود که شهروندان در امور عمومی و حکومتی احساس مشارکت کنند. وقتی که شهروندان به اطلاعات حقیقی و قابل اعتماد دسترسی دارند، می‌توانند نظارت مؤثری بر فعالیت‌های حکومت داشته باشند. این امر باعث می‌شود که شبهه‌ها و شکایت‌های کمتری وجود داشته باشد و در نتیجه، اعتماد عمومی به حکومت افزایش یابد. شفافیت همچنین به عنوان یک ابزار مؤثر در مبارزه با فساد عمل می‌کند(آنانوستاکی ،۲۰۲۲:۲۴۷). زمانی که فرآیندها و اطلاعات در

دسترس عموم قرار گیرند، احتمال وقوع فساد کاهش می‌یابد. این موضوع به ویژه در زمینه استفاده از منابع مالی عمومی و قراردادهای دولتی اهمیت زیادی دارد. همچنین، شفافیت به شهروندان این امکان را می‌دهد که در فرآیندهای سیاسی و اجتماعی مشارکت کنند. هنگامی که اطلاعات مربوط به تصمیمات و برنامه‌های حکومت به‌دست مردم می‌رسد، آنها می‌توانند نظرات و پیشنهادات خود را ارائه دهند و در نتیجه، سیاست‌گذاری‌ها متناسب با نیازها و تمایلات جامعه باشد(ملکی عزین آبادی و جمالی، ۱۴۰۳: ۹۸). در زمینه امنیت سایبری، شفافیت به حکومت‌ها و سازمان‌ها کمک می‌کند تا خطرات و تهدیدات سایبری را شناسایی و ارزیابی کنند. با ارائه اطلاعات در مورد حملات سایبری و نقاط ضعف سیستم‌ها، می‌توان برنامه‌های امنیتی بهتری طراحی کرد. ارتباطات شفاف بین دولت و شهروندان از اهمیت ویژه‌ای برخوردار است. حکومت باید بتواند اطلاعات مربوط به سیاست‌های امنیت سایبری و اقدامات لازم برای حفاظت از داده‌ها را به‌صورت شفاف به مردم گزارش کند(الکسی ،۲۰۲۱:۳۵). این ارتباطات مؤثر به شهروندان این اطمینان را می‌دهد که حکومت در حفظ امنیت سایبری تلاش می‌کند.

۲-۲-۴- پاسخگویی

پاسخگویی مستلزم این است که نهادها مسئولیت هر گونه نقص و مشکل را بر عهده بگیرند و به سؤالات جامعه پاسخ دهند. شفافیت و پاسخگویی به تقویت اعتماد عمومی کمک می‌کنند(تارمیز و سیفرودین ،۲۰۲۴:۱۴). وقتی شهروندان می‌بینند که اطلاعات به‌صورت عمومی در دسترس است و نهادها در برابر اقدامات خود پاسخگو هستند، احساس امنیت بیشتری نسبت به استفاده از فضای دیجیتال می‌کنند. این اعتماد به نوبه خود، مشارکت بیشتر افراد در حمایت از سیاست‌های امنیت سایبری را تسهیل می‌کند. پاسخگویی به معنای پذیرش خطاها و یادگیری از آن‌ها نیز است(سو.ریک ،۲۰۲۳:۴۸).هنگامی که نهادها در مواجهه با نقایص یا تهدیدات سایبری با صداقت رفتار کنند و نتایج بررسی‌ها را منتشر کنند، می‌توانند از تجربیات خود به‌عنوان بیانیه‌ای در جهت بهبود عملکرد استفاده کنند. این حلقه یادگیری به پیشرفت مستمر سیستم‌های امنیتی کمک می‌کند. وجود فضا برای نقد و نظارت عمومی، به فعالان اجتماعی و شهروندان اجازه می‌دهد تا به نهادهای امنیتی فشار بیاورند تا به بهترین شیوه‌ها عمل کنند. انتقادات و پیشنهادات عمومی می‌توانند به اصلاح فرآیندها و بهبود روش‌ها منجر شوند و در نتیجه یک محیط امنیتی سایبری بهینه‌تر ایجاد کنند. شفافیت همچنین به کاهش شکاف‌های اطلاعاتی بین نهادهای دولتی و بخش خصوصی کمک می‌کند. وقتی اطلاعات به‌طور آزادانه بین این نهادها تبادل می‌شود، امکان شناسایی نقاط ضعف و تهدیدات بهتر فراهم می‌شود. به همین دلیل، تبادل اطلاعات بین نهادهای مختلف، یک جزء کلیدی در ایجاد امنیت پایدار می باشد. نقش شفافیت و پاسخگویی در جلوگیری از فساد نیز برجسته است(متین ،۲۰۲۴:۲۷). نبود شفافیت می‌تواند به بروز فسادهای اداری و سوءاستفاده‌ها منجر شود و در نتیجه میزان آسیب‌پذیری امنیت سایبری افزایش یابد. فرایندهای غیر شفاف می‌توانند اعتماد عمومی را کاهش دهند و بر روابط بین نهادها و شهروندان تأثیر منفی بگذارند.

۳-۲-۴- مشارکت

مشارکت به معنای درگیر کردن تمامی ذینفعان در فرآیندهای تصمیم‌گیری و برنامه‌ریزی مرتبط با امنیت سایبری است. این ذینفعان شامل نهادهای دولتی، بخش خصوصی، جامعه مدنی و حتی کاربران نهایی هستند. با مشارکت همه ذینفعان، می‌توان نیازها و نظرات مختلف را در نظر گرفت که به ایجاد سیاست‌ها و راهکارهای مؤثرتر کمک می‌کند. مشارکت افراد و گروه‌های مختلف باعث می‌شود که تنوع دیدگاه‌ها در تصمیم‌گیری‌ها وجود داشته باشد. این تنوع می‌تواند به شناسایی بهتر تهدیدات و چالش‌ها کمک کند و از اتخاذ تصمیمات یک‌بعدی و ناکارآمد جلوگیری کند(مولوگتا ،۲۰۲۳:۳۳۱). با تبادل نظرات مختلف، راهکارهای جامع‌تری برای مقابله با مشکلات امنیت سایبری ارائه می‌شود. وقتی ذینفعان در فرآیند تصمیم‌گیری مشارکت می‌کنند، احساس مالکیت بیشتری نسبت به نتایج آن پیدا می‌کنند. این حس مالکیت می‌تواند به التزام و حمایت بیشتری از سیاست‌ها و اقدامات مربوط به امنیت سایبری منجر شود. در واقع، مشارکت باعث می‌شود که هر ذینفع خود را به‌عنوان یک بازیگر کلیدی در امنیت سایبری ببیند. مشارکت همچنین می‌تواند به آموزش و توانمندسازی ذینفعان کمک کند(نجفی رستاقی و

دهقانیان، ۱۴۰۰: ۸۳). از طریق تبادل اطلاعات و تجربیات بین نهادها، آگاهی عمومی در مورد تهدیدات سایبری و چگونگی مدیریت آن‌ها افزایش می‌یابد. این افزایش آگاهی به ساختن یک جامعه آگاه و مقاوم در برابر تهدیدات سایبری کمک می‌کند. تاب‌آوری به معنای توانایی یک سیستم در مواجهه با تهدیدات و ظهور آن‌ها است. با مشارکت فعال ذینفعان، امکان تقویت تاب‌آوری سازمان‌ها و جوامع در برابر حملات سایبری افزایش می‌یابد(تاشین ،۳۸:۲۰۲۴). شبکه‌سازی و توانمندسازی نهادها همچنین می‌تواند منجر به بهبود سرعت واکنش به تهدیدات و رویدادهای ناگهانی شود. در نهایت، مشارکت در زمینه امنیت سایبری یک ضرورت است. این اصل نه تنها به بهبود کیفیت تصمیم‌گیری‌ها کمک می‌کند، بلکه به ایجاد حس مسئولیت جمعی و همکاری در جامعه نیز منجر می‌شود. بدون مشارکت، به‌ویژه در دنیای دیجیتال پیچیده امروزی، توانایی مقابله با تهدیدات سایبری به شدت کاهش می‌یابد.

۴-۲-۴- قانون‌مداری و حاکمیت قانون

قانون‌مداری به معنای رعایت قوانین و مقررات در راستای امنیت سایبری است. حاکمیت قانون نیز به تأسیس و اجرای قوانین به‌منظور حفاظت از حقوق شهروندان و تأمین امنیت فضای سایبری اشاره دارد. این اصول در ساختارهای حکمرانی خوب نقش حیاتی دارند و تضمین می‌کنند که امنیت سایبری تنها به عنوان یک ابزار حفاظتی درنظر گرفته نشود، بلکه به حقوق و آزادی‌های فردی نیز احترام گذاشته شود. با پیشرفت فناوری، نیاز به به‌روزرسانی و تطابق قوانین امنیت سایبری با تحولات جدید ضروری است. قوانین باید منعطف بوده و قابلیت انطباق با شرایط جدید را داشته باشند. این انطباق قادر به تقویت حفاظت از داده‌ها و اطلاعات حساس است و رضایت عمومی را افزایش می‌دهد. قانون‌مداری به تأمین حقوق شهروندان در فضای سایبری کمک می‌کند. ایجاد چارچوب‌های قانونی مشخص برای حفاظت از داده‌های شخصی، اطلاعات مالی و حریم خصوصی به شهروندان اطمینان می‌دهد که حقوق آنها حفظ می‌شود(روگوست ،۱۷۶:۲۰۲۴) حاکمیت قانون همچنین اطمینان می‌دهد که اقدامات امنیتی با رعایت حقوق بشر صورت می‌گیرد. وجود قوانین روشن و جامع زمینه‌ساز تعیین مسئولیت‌ها و نقش‌ها در حوزه امنیت سایبری می‌شود. این مشخص‌سازی دیگر ضمانت‌کننده این است که هر نهاد یا فرد در زمینه امنیت سایبری دارای مسئولیت‌های مشخصی است(ایقنای ،۱۵۵:۲۰۲۳). این وضعیت از ابهام و عدم وضوح جلوگیری کرده و به عملکرد مؤثر نهادها کمک می‌کند. قانون‌مداری به عنوان یک ابزار برای جلوگیری از فساد و سوءاستفاده در حوزه امنیت سایبری عمل می‌کند. زمانی که قوانین به‌طور مؤثر اجرا شوند و نهادهای نظارتی وجود داشته باشند، احتمال فساد و عدم رعایت اصول امنیتی کاهش می‌یابد. این مسئله به ایجاد یک محیط سایبری امن و قابل اعتماد کمک می‌نماید.

۴-۲-۵- عدالت و برابری

عدالت و برابری از اصول کلیدی حکمرانی خوب هستند که به حفاظت از حقوق بنیادی افراد کمک می‌کنند. در زمینه امنیت سایبری، این اصول به معنای دسترسی برابر به اطلاعات و منابع امنیتی و هم‌چنین پیشگیری از تبعیض در برابر گروه‌های خاص است. این اصول تضمین می‌کنند که همه شهروندان به‌صورت عادلانه از حمایت‌های امنیتی بهره‌مند شوند(یوسیف و حافظ ،۴۹۶:۲۰۲۱). تساوی در دسترسی به منابع و اطلاعات امنیت سایبری به‌ویژه برای جمعیت‌های آسیب‌پذیر و گروه‌های کم‌درآمد ضروری است. این افراد ممکن است به دلیل نداشتن دانش یا اطلاعات کافی، آسیب‌پذیری بیشتری در برابر تهدیدات سایبری داشته باشند. حکمرانی خوب باید به‌گونه‌ای طراحی شود که این شکاف‌ها را پر کند و به همه افراد فرصت‌هایی برابر برای حفاظت از خود فراهم کند. عدالت در امنیت سایبری همچنین به حفاظت از حقوق اقلیت‌ها و گروه‌های آسیب‌پذیر مربوط می‌شود. گروه‌هایی که ممکن است در معرض تهدیدات خاص قرار گیرند باید دارای حفاظت قانونی و امنیتی ویژه‌ای باشند. این می‌تواند شامل ارائه راهکارهای خاص برای حفاظت از داده‌ها و اطلاعات شخصی آنها باشد(ورونیکا و هونمین ،۲۰۸:۲۰۲۱). در دنیای دیجیتال، آسیب‌های ناشی از حملات سایبری می‌تواند به‌صورت ناعادلانه توزیع شود. افراد و سازمان‌هایی که زیرساخت‌های ضعیف‌تری دارند، ممکن است بیشتر تحت تأثیر قرار بگیرند. بنابراین، اجرای سیاست‌هایی که بار هزینه‌های

امنیتی را به‌طور عادلانه بین تمام بخش‌ها تقسیم کند، امری ضروری است(لوماس ،۲۰۲۰:۱۴). تبعیض در امنیت سایبری می‌تواند منجر به ایجاد فضاهای ناامن برای گروه‌های خاص شود. برای مثال، اگر سیاست‌های امنیتی به‌گونه‌ای طراحی شوند که تنها به گروه‌های خاصی خدمت کنند، این موضوع می‌تواند سبب شعله‌ور شدن تنش‌های اجتماعی و نارضایتی عمومی گردد. بنابراین ایجاد سیاست‌هایی که از تبعیض‌ها جلوگیری کند، از اهمیت بالایی برخوردار است. عدالت و برابری همچنین به تقویت تاب‌آوری جامعه در برابر تهدیدات سایبری کمک می‌کند. وقتی همه گروه‌ها احساس کنند که در حفاظت از امنیت سایبری سهیم‌اند و به‌طور عادلانه مورد حمایت قرار دارند، بی‌اعتمادی و نارضایتی کمتری وجود خواهد داشت. این مسئله باعث ایجاد یک محیط امنیتی قوی‌تر و پایدارتر خواهد شد.

۵- چالشهای حکمرانی خوب در تضمین امنیت سایبری

چالش‌های حکمرانی خوب در تضمین امنیت سایبری به عنوان یکی از مسائل مهم در دنیای دیجیتال امروز، نیازمند توجه ویژه‌ای است(رضاپور و همکاران، ۱۴۰۱: ۰۳) چالش‌های متعددی نیز در این زمینه وجود دارد که باید مورد بررسی قرار گیرند:

۵-۱- کمبود منابع

کمبود منابع به عنوان یکی از چالش‌های حکمرانی خوب در تضمین امنیت سایبری، مسئله‌ای است که در بسیاری از کشورها و سازمان‌ها به وضوح مشاهده می‌شود. این کمبود منابع می‌تواند شامل محدودیت‌های مالی، انسانی و فناوری باشد که به طور مستقیم بر توانایی دولت‌ها و نهادها در مقابله با تهدیدات سایبری تأثیر می‌گذارد(گاله ،۲۰۲۰:۲۱).در دنیای دیجیتال امروز، جایی که تهدیدات سایبری به سرعت در حال افزایش هستند، این کمبود منابع می‌تواند عواقب جدی برای امنیت ملی و زیرساخت‌های حیاتی داشته باشد(فرزام نیا و عبدی، ۱۴۰۰: ۲۵). یکی از جنبه‌های مهم این چالش، محدودیت‌های مالی است(نجفی رستاقی و عبدالحسین زاده، ۱۴۰۲: ۱۴). علاوه بر محدودیت‌های مالی، کمبود نیروی انسانی متخصص نیز یک چالش جدی است. چالش دیگر مربوط به زیرساخت‌های فناوری اطلاعات است. بسیاری از کشورها هنوز زیرساخت‌های لازم برای ارائه خدمات الکترونیکی امن را ندارند. عدم وجود زیرساخت‌های مناسب می‌تواند مانع از اجرای مؤثر سیاست‌های امنیتی شود. بنابراین، سرمایه‌گذاری در توسعه زیرساخت‌ها باید جزء اولویت‌های حکمرانی خوب باشد تا بتوانند با تهدیدات جدید مقابله کنند. عدم هماهنگی بین نهادهای مختلف نیز یکی دیگر از چالش‌هایی است که ناشی از کمبود منابع است. در بسیاری از کشورها، نهادهای مختلف مسئولیت‌های متفاوتی در زمینه امنیت سایبری دارند و این عدم هماهنگی می‌تواند منجر به ضعف در پاسخگویی به تهدیدات شود. اگر یک نهاد نتواند اطلاعات لازم را با نهادهای دیگر به اشتراک بگذارد، احتمال وقوع حملات سایبری افزایش می‌یابد(رمضانی و بنو ،۲۰۲۰:۷۳). علاوه بر این، قوانین و مقررات موجود در بسیاری از کشورها قادر به پاسخگویی به چالش‌های جدید امنیت سایبری نیستند. عدم وجود قوانین شفاف و جامع می‌تواند منجر به سردرگمی و عدم اطمینان در میان شهروندان و کسب‌وکارها شود. بنابراین، بازنگری و اصلاح قوانین یکی از اقدامات ضروری برای تقویت حکمرانی خوب در زمینه امنیت سایبری است. چالش دیگری که باید مورد توجه قرار گیرد، فرهنگ عمومی نسبت به امنیت سایبری است. بسیاری از افراد هنوز نسبت به تهدیدات سایبری آگاهی کافی ندارند و این موضوع می‌تواند منجر به رفتارهای خطرناک مانند استفاده از رمزهای عبور ضعیف یا عدم رعایت اصول امنیتی شود.آموزش عمومی درباره تهدیدات سایبری و نحوه مقابله با آن‌ها باید جزو برنامه‌های حکمرانی خوب قرار گیرد تا شهروندان بتوانند نقش فعالی در حفاظت از اطلاعات خود ایفا کنند(ساواس و کاراناس ،۲۰۲۲:۱۵). توسعه زیرساخت‌های فناوری اطلاعات نیز یکی از چالش‌های اساسی حکمرانی خوب در زمینه امنیت سایبری است. بسیاری از کشورها هنوز زیرساخت‌های لازم برای ارائه خدمات الکترونیکی امن را ندارند. عدم وجود زیرساخت‌های مناسب می‌تواند مانع از اجرای مؤثر سیاست‌های امنیتی شود. بنابراین، سرمایه‌گذاری در توسعه زیرساخت‌ها باید جزء اولویت‌های حکمرانی خوب باشد.در مجموع، نیاز به نظارت و ارزیابی مستمر بر روی سیاست‌ها و اقدامات امنیت سایبری وجود دارد .

۲-۵- مسائل فنی

مسائل فنی به عنوان یکی از چالش‌های حکمرانی خوب در تضمین امنیت سایبری، موضوعی پیچیده و چندبعدی است که به طور مستقیم بر توانایی دولت‌ها و سازمان‌ها در مقابله با تهدیدات سایبری تأثیر می‌گذارد(دامیلاره ،۵۸:۲۰۲۲).این مسائل شامل کمبود زیرساخت‌های فناوری، عدم هماهنگی بین سیستم‌های مختلف، پیچیدگی‌های فنی و نیاز به آموزش مستمر برای نیروی انسانی می‌شود. در دنیای امروز که تهدیدات سایبری به سرعت در حال افزایش هستند، این چالش‌ها می‌توانند عواقب جدی برای امنیت ملی و زیرساخت‌های حیاتی داشته باشند. یکی از جنبه‌های مهم مسائل فنی، کمبود زیرساخت‌های فناوری اطلاعات است(تلو ،۵:۲۰۲۱). بسیاری از کشورها به ویژه در حال توسعه، هنوز زیرساخت‌های لازم برای ارائه خدمات الکترونیکی امن را ندارند. این عدم وجود زیرساخت‌های مناسب می‌تواند مانع از اجرای مؤثر سیاست‌های امنیتی شود و به افزایش آسیب‌پذیری در برابر حملات سایبری منجر گردد. بنابراین، سرمایه‌گذاری در توسعه زیرساخت‌ها باید جزء اولویت‌های حکمرانی خوب باشد تا بتوانند با تهدیدات جدید مقابله کنند(گوپتا ،۱۹۸:۲۰۲۰). عدم هماهنگی بین نهادهای مختلف نیز یکی دیگر از چالش‌هایی است که ناشی از مسائل فنی است. در بسیاری از کشورها، نهادهای مختلف مسئولیت‌های متفاوتی در زمینه امنیت سایبری دارند و این عدم هماهنگی می‌تواند منجر به ضعف در پاسخگویی به تهدیدات شود. اگر یک نهاد نتواند اطلاعات لازم را با نهادهای دیگر به اشتراک بگذارد، احتمال وقوع حملات سایبری افزایش می‌یابد. بنابراین، ایجاد یک سیستم همکاری مؤثر بین نهادها یکی از الزامات حکمرانی خوب در این حوزه است.

نتیجه گیری

در عصر دیجیتال، مفهوم حکمرانی خوب به‌عنوان یکی از ارکان اساسی مدیریت دولتی و تعاملات اجتماعی شناخته می‌شود، که در آن شفافیت، پاسخگویی، مشارکت عمومی، عدالت، و حاکمیت قانون به‌شکل مؤثری اجرا می‌گردد. یکی از ارکان برجسته حکمرانی خوب در دنیای امروز، تأمین امنیت سایبری است؛ چرا که زیرساخت‌های ارتباطی و فناوری اطلاعات به‌شدت با زندگی انسان‌ها گره خورده‌اند و هرگونه نقص در امنیت سایبری، به‌ویژه در حوزه حاکمیت، می‌تواند تأثیرات گسترده‌ای بر سیستم‌های دولتی، خدمات عمومی و همچنین اعتماد شهروندان به نهادهای حکومتی داشته باشد. تضمین امنیت سایبری مستلزم اتخاذ سیاست‌هایی دقیق و منطبق بر اصول حکمرانی خوب است. اولویت‌بندی در حفاظت از داده‌های شهروندان، مقابله با جرایم سایبری، و تقویت پایداری زیرساخت‌های ملی از جمله ملزوماتی است که دولت‌ها در مسیر تحقق این هدف باید مدنظر قرار دهند. شفافیت در فرآیندهای امنیت سایبری و اطلاع‌رسانی مناسب در هنگام بروز تهدیدات سایبری نه‌تنها به تقویت اطمینان عمومی می‌انجامد، بلکه مشارکت مردم و ذی‌نفعان مختلف را در تحقق امنیت دیجیتال ممکن می‌سازد. از سوی دیگر، عدالت در دسترسی به منابع نوین تکنولوژیک و حمایت از گروه‌های آسیب‌پذیر در برابر حملات و آسیب‌های سایبری نیز یکی از چالش‌های مهم حکمرانی خوب است. تأمین امنیت دیجیتال باید به‌گونه‌ای باشد که هیچ‌یک از طبقات اجتماعی یا گروه‌های محروم، قربانی تبعیض یا خط‌مشی‌های ناکارآمد نشوند. مقابله با چالش‌های بین‌المللی، نظیر جرایم سازمان‌یافته سایبری و حملات دولتی یا غیردولتی، نیازمند همکاری منطقه‌ای و جهانی است؛ که این همکاری‌ها تنها با وجود تعهد به اصول حکمرانی خوب در نهادهای بین‌المللی و منطقه‌ای معنا پیدا می‌کند. بنابراین، امنیت سایبری نه‌فقط به‌عنوان یک مسأله فنی، بلکه به‌عنوان یک موضوع ساختاری و مدیریتی ارتباطی عمیق با حکمرانی خوب دارد. دولت‌ها با اتخاذ نگرش جامع و تقویت چارچوب‌های قانونی برای حفاظت از داده‌ها و زیرساخت‌های حیاتی، باید به هدف ایجاد یک اکوسیستم پایدار و انسانی در فضای سایبری دست یابند. در نهایت، تنها با ادغام اصول حکمرانی خوب و امنیت سایبری می‌توان به جامعه‌ای ایمن، شفاف، و پایدار در عصر دیجیتال رسید که نه‌تنها امنیت فیزیکی، بلکه اعتماد و حقوق شهروندان را نیز تضمین کند. به‌منظور تحقق این اهداف، پیشنهادات زیر می‌تواند مورد توجه قرار گیرد:

-تدوین و اجرای قوانین و مقررات جامع در زمینه امنیت سایبری که به‌صورت مستمر با تحولات فناوری به‌روز شود و شامل الزامات شفافیت و پاسخگویی باشد؛

-ایجاد و تقویت همکاری‌های بین‌المللی در زمینه امنیت سایبری از طریق کنفرانس‌ها، اجلاس‌ها و معاهدات؛ به‌نحوی که تبادل اطلاعات و تجارب میان کشورهای مختلف تسهیل گردد؛

-برگزاری دوره‌های آموزشی و کارگاه‌های توانمندسازی برای عموم و کارکنان نهادهای دولتی و خصوصی به‌منظور ارتقای آگاهی و دانش امنیت سایبری.

منابع

۱. افراشته، نسرین؛ محمدی، افسانه؛ آهنگری، آرام؛ آسور، امی(۱۴۰۳). «بررسی چالش‌ها و راهکارهای امنیت سایبری در دنیای امروز». کنفرانس پژوهش‌های مدیریت، تعلیم و تربیت در آموزش و پرورش؛ مجموعه مقالات دومین کنفرانس بین‌المللی پژوهش‌های مدیریت، تعلیم و تربیت در آموزش و پرورش۰۱-۲۰.

۲. بلوجی، حیدرعلی(۱۴۰۱). «تکنولوژی های جدید و امنیت بین‌المللی: آثار و تحولات». مجله مطالعات راهبردی، ۹۵، ۱۸۵-۲۱۰.

۳. بیات کمیتکی، مهناز(۱۴۰۳). موهبتی، احسان. «حکمرانی خوب به مثابه هدف مشترک حقوق عمومی و توسعه». مجله پژوهشهای حقوقی، ۵۵(۱۴): ۲۴۱-۲۷۸.

۴. جوانمردزاده، روح‌الله؛ یاسمی، منوچهر؛ جان محمدی، امیر(۱۴۰۰). «درآمدی تحلیلی بر تمایزات حکمرانی خوب و حکمرانی متعالی». مقالات دومین همایش ملی حکمرانی اسلامی، ۱۶ خرداد، ۰۱-۲۶.

۵. داراب نیا، سعید؛ کریمی فرد، حسین؛ مرادی، جهانبخش؛ بختیارپور، علی(۱۴۰۱). «بررسی رابطه میان شاخص‌های حکمرانی خوب و امنیت انسانی در ایران: مطالعه موردی ۱۴۰۰-۱۳۹۲». فصلنامه علمی پژوهشی، توسعه اجتماعی، (۱۷)۰۲: ۲۵-۴۵.

۶. رجبی، صادق(۱۴۰۲). «حکمرانی خوب». دهمین کنفرانس ملی ایده های نوین در فنی و مهندسی. ایران: تهران، ۰۱-۲۰.

۷. رحمدل، ناصر؛ کامکار، مهدی(۱۴۰۰). «نقش باورهای انسانی در جذب دانش برای امنیت سایبری». نشریه امنیت پژوهی، ۷۳: ۳۶-۵۹.

۸. ضاپور، حمیدرضا؛ زاکاریان، آرمین؛ بشکنی، محمدکاظم(۱۴۰۱). «بررسی حملات و چالشهای امنیت سایبری و راهکارهای مقابله با حملات سایبری». نهمین کنفرانس ملی ایده های نوین در فنی و مهندسی، ایران: تهران، ۰۱-۲۰.

۹. رضوی پور، فضل اله؛ فتحی، فرشته؛ نورمحمدیان، زهرا(۱۴۰۱). «رابطه امنیت سایبری با تهدیدات سایبری». سومین کنفرانس ملی پدافند سایبری، ایران: مراغه، ۰۱-۲۰.

۱۰. زارع زاده، رسول(۱۴۰۰). «آسیب‌ها و چالش‌های امنیتی‌سازی مسائل داخلی؛ مطالعه موردی شبکه‌های اجتماعی مجازی». فصلنامه مطالعات راهبردی، ۲۴(۰۲)، ۱۰-۳۶.

۱۱. صالحی، مطهره(۱۴۰۲). «بررسی و تبیین شاخص های تحقق حکمرانی خوب در راستای توسعه یافتگی». مجله جغرافیا و روابط انسانی، (۰۶)۲۱: ۳۱۷-۳۳۶.

۱۲. ملکی عزین آبادی، روح اله؛ جمالی، جواد(۱۴۰۳). «مطالعه مقایسه‌ای قوانین سایبری چین، ایالات‌متحده آمریکا و روسیه؛ بایسته‌ها و ضرورت‌های امنیت سایبری جمهوری اسلامی ایران». فصلنامه آماد و فناوری دفاعی، (۰۷)۲۳: ۷۹-۱۰۱.

۱۳. فرزام نیا، نیما؛ عبدی، بهنام(۱۴۰۰). «ارائه الگوی حکمرانی خوب امنیت فضای مجازی». مقالات دومین همایش ملی حکمرانی اسلامی. مقالات دومین همایش ملی حکمرانی اسلامی. ۱۶ خرداد۱۴۰۰: ۰۱-۳۶.

۱۴. محمودی، امیررضا؛ بحرکاظمی، مریم(۱۴۰۳). «هوش مصنوعی و تاثیر آن بر امنیت سایبری و حفاظت از داده ها». نشریه پژوهش های بنیادین در حقوق، (۰۱)۰۳: ۱۲۰-۱۳۹.

۱۵. نجفی رستاقی، حیدر؛ دهقانیان، حمید(۱۴۰۰). «چالشهای معرفتی در حکمرانی فناوری و ارائهٔ راهکارهایی برای جمهوری اسلامی ایران» . سیاست نامه علم و فناوری، ۱۱(۰۳): ۷۵-۹۹.

۱۶. نجفی رستاقی، حیدر؛ عبدالحسین زاده، محمد(۱۴۰۲). «چالش ها و راهکارهای تحقق حکمرانی هوشمند در کشور و ارائه توصیه های سیاستی برای مجلس شورای اسلامی». ماهنامه گزارش های کارشناسی مرکز پژوهش های مجلس شورای اسلامی، ۳۱(۰۳): ۰۱-۶۰.

۱۷. نگهدار، ایرج؛ پورقهرمانی، بابک؛ بیگی، جمال(۱۴۰۲). «رهیافتهای حکمرانی ایران در قبال نقض امنیت سایبری». چهارمین کنفرانس ملی پدافند سایبری، ۱۴۰۲: ۰۱-۲۵.

۱۸. جاسب جاسب، زینه سعد(۱۴۰۲). «استفاده از امنیت سایبری برای مبارزه با جرایم الکترونیکی بررسی تطبیقی حقوق عراق و لبنان». استاد راهنما: سیدمحمدمهدی احمدی. پایان نامه کارشناسی ارشد، دانشگاه ادیان و مذاهب.

۱۹. صادقی ساروکلائی، منصور(۱۴۰۲). «استفاده از هوش مصنوعی برای تقویت امنیت ملی و مقابله با تهدیدات سایبری». استاد راهنما: عین اله جعفر زاده قمی، پایان نامه کارشناسی ارشد، موسسه آموزش عالی صالحان.

۲۰. صدیقی، نگار(۱۴۰۱). «اثر امنیت سایبری بر شاخص توسعه انسانی در کشورهای منتخب با استفاده از رویکرد پویایی‌شناسی سیستم». استاد راهنما: سعید راسخی، پایان نامه کارشناسی ارشد، دانشگاه مازندران.

۲۱. علاء تکلیف، حیدر(۱۴۰۲). «نقش امنیت سایبری در چشم انداز استراتژیک امنیت ملی عراق». استاد راهنما: محمد جواد نوروزی. پایان نامه کارشناسی ارشد، جامعه المصطفی العالمیه.

22. Anagnostakis, Dimitrios, (2022). ”The External Face of the EU’s Cybersecurity Policies: Promoting Good Cybersecurity Governance Abroad?” EU Good Governance Promotion in the Age of Democratic Decline, Vol: 01, 237-265.

23. Alexei, Arina, (2022). “Ensuring Information Security in Public Organizations in the Republic of Moldova Through the ISO 27001 Standard”. Security and defense, Social Informatics, ICT Information and Communications Technologies Published by: Universitatea Tehnică a Moldovei, 11.

24. Cooray. Arusha, Kumar Jha. Chandan, Sarangi. Sudipta, (2024). “Good governance in troubled times: What we know and what experts say”. Economic Modelling, Volume 136, July 2024, 106761.

25. Czuryk, Małgorzata, (2023). “Cybersecurity and Protection of Critical Infrastructure”. Studia Iuridica Lublinensia, Vol30, 43-52.

26. Creese. Sadie, Dutton. William H, Esteve-González. Patricia, (2021). “The social and cultural shaping of cybersecurity capacity building: a comparative study of nations and region”. Personal and Ubiquitous Computing, 10 May 2021 Volume 25, pages 941–955.

27. Chansa Chanda. Thelma, Madoda. Derick, Hassan Sain. Zohaib, Chisebe. Sylvester, (2024). “Good Governance: A Pillar to National Development”. International Journal of Research Publication and Reviews 5(6):621-635.

28. Damilare Oyeniyi. Lawrence, Esther Ugochukwu. Chinonye, Zamanjomane Mhlongo. Noluthando, (2024). “Developing Cybersecurity Frameworks for Financial Institutions: A Comprehensive Review and Best Practices”. Computer Science & IT Research Journal, 5(4), 903-925. https://doi.org/10.51594/csitrj.v5i4.1049.

29. Islam Papel. Md Saidul, Ashraf Mridha. A B M, Rahman. Anisur, Ashrafuzzaman. Md, (2024). “Enhancing Government IT Infrastructure: Develop Frameworks for Modernizing Government IT Systems to Improve Security, Efficiency, and Citizen Engagement”. AIM INTERNATIONAL JOURNALPublisherFrontiers in Applied Engineering and Technology, 2024;1(01):157-174. DoI: 10.70937/faet.v1i01.31.

30. Gale. Megan, Bongiovanni. Ivano, Slapnicar. Sergeja, (2020). “Governing cybersecurity from the boardroom: Challenges, drivers, and ways ahead”. Computers & Security. Volume 121, October 2022, 102840, 14-39.

31. Gupta. Rajan, Pal, Saibal K, Muttoo. Sunil K, (2020). “Cyber Security Assessment Education for E-Governance Systems”. Innovations in Cybersecurity Education, First Online: 22 November 2020, pp 181–212.

32. Ifeanyi-Ajufo, Nnenna, (2023).“Cyber governance in Africa: at the crossroads of politics, sovereignty and cooperation”. Policy Design and Practice Volume 6, 2023 - Issue 2: 147-159.

33. Kusuma Astuti. Rita, Ponco Aji. Koesmoyo, Wilonotomo, (2021). “The Urgency of Utilizing Open Data Platform by the Foreigner Supervision Team to Promote Good Governance During the Covid-19 Pandemic”. Series:Advances in Social Science, Education and Humanities Research, Vol.01, 01-36. 10.2991/assehr.k.210506.045.

34. Lomas, Elizabeth, (2020). “Information Governance and Cybersecurity: Framework for Securing and Managing Information Effectively and Ethically”. Cybersecurity for Information Professionals. 1st Edition, Auerbach Publications.

35. Mulugeta Melaku, Henock, (2023). “A Dynamic and Adaptive Cybersecurity Governance Framework.J.Cybersecur”.Priv. 2023, 3(3), https://doi.org/10.3390/jcp3030017, 327-350.

36. Muhammad Ali. Sardar, Razzaq. Abdul, Abbass. Haider, Yousaf. Muhammad, Shan. Rafi us, (2024). “A Hybrid Analytical Framework for Enhancing Cybersecurity in Underdeveloped Countries”. Preprints.org (www.preprints.org).doi:10.20944/preprints202410.1442.v1,01-25.

37. Metin. Bilgin, Gül Özhan. Fatma, Wynn. Martin, (2024). “Digitalisation and Cybersecurity: Towards an Operational Framework”. Electronics 2024, 13(21), 4226; https://doi.org/10.3390/electronics13214226.

38. Praditya. Editha, Maarif. Syamsul, Ali. Yusuf, Juni Risma Saragih. Herlina, Duarte. Rui, An Suprapto. Firre, Nugroho. Riant, (2023). "National Cybersecurity Policy Analysis for Effective Decision-Making in the Age of Artificial Intelligence". Journal of Human Security, Vol. 19 No. 2 (2023): Volume 19, Issue 2.

39. Ramazzini Bechara. Fabio, Bueno Schuch. Samara, (2020). "Cybersecurity and global regulatory challenges". Journal of Financial Crime, ISSN: 1359-0790, Article publication date: 2 November 2020, 69-86.

40. Rhogust, Muhammad, (2024). "Legal Framework for Cybersecurity in the Digital Economy: Challenges and Prospects for Indonesia". Journal of Law, Social Science and Humanities,1(2).Retrievedfromhttps://myjournal.or.id/index.php/JLSSH/article/view/213,166-180.

41. Rizal. Muhammad, Askafi. Eka, Supriyono, (2021). "Implementation of the Performance Accountability System for Government Agencies (SAKIP) in Realizing Good Governance at the Kediri City Health Office". International Journal of Business, Economics & Management, 4(1), 174-179. https://doi.org/10.31295/ijbem.v4n1.1463.

42. Savas. Serkan, Karatas. Süleyman, (2022). "Cyber governance studies in ensuring cybersecurity: anoverview of cybersecurity governance". Int. Cybersecur. Law Rev. (2022) 3:7–34. https://doi.org/10.1365/s43439-021-00045-4.

43. Saravanan. Srisakthi, Suresh Babu. C V, (2024). "Cybersecurity: Protecting Information in a Digital World. Hindustan Institute of Technology and Science". https://www.researchgate.net/publication/380125676,01-36.

44. Sari, Ade Risna, (2023). "The Impact of Good Governance on the Quality of Public Management Decision Making". Journal of Contemporary Administration and Management (ADMAN) ISSN: 2988-0394 Print / 2988-3121 Online, Vol 1, Issue 2, August 2023, Page 39-46, DOI: https://doi.org/10.61100/adman.v1i2.21.

45. Tahsin Hossain. Sk, Yigitcanlar. Tan, Nguyen. Kien, Xu. Yue, (2024). "Local Government Cybersecurity Landscape: A Systematic Review and Conceptual Framework". School of Computer Science, Faculty of Science, Queensland University of Technology, Vol 36: 21-60.

46. Telo, J, (2021). "Privacy and Cybersecurity Concerns in Smart Governance Systems in Developing Countries". Tensorgate Journal of Sustainable Technology and Infrastructure for Developing Countries,

4(1),113.Retrievedfromhttps://research.tensorgate.org/index.php/tjstidc/article/view/17.

47. Tarmizi. Tarmizi, Syafruddin. Syafruddin, (2024). "The Urgency of Optimizing Digital Service Policies in Order to Realize Good Governance". International Journal of Multicultural and Multireligious Understanding. Vol 01, http://dx.doi.org/10.18415/ijmmu.v11i1.523, 01-24.

48. Ubowska. Agnieszka, Królikowski. Tomasz, (2022). "Building a cybersecurity culture of public administration system in Poland". Procedia Computer Science, Volume 207, 2022, Pages 122-150.

49. Włodyka, Ewa Maria, (2024). "Cyber Security as A Research Subject: Quantitative and Qualitative Analysis of Data in Scopus Database Covering in 2020–2024". Cybersecurity and Law nr 2 (12), 132-147.

50. Weronika. Jakubczak , Hon-min, Yau, (2021). "Trends in cybersecurity regulations of Taiwan (Republic of China) – Phases of Promotion of major cyber security plans and programs in the National Cyber Security Program of Taiwan (2021–2024)". Zeszyty Naukowe sgsp 2021-2021, Nr 80 (tom 1), s. 199–216 issn: 0239-5223 Creative Commons Attribution 4.0 International License doi: 10.5604/01.3001.0015.6485.

51. Yusif. Salifu, Hafeez-Baig. Abdul, (2021). "A Conceptual Model for Cybersecurity Governance". Pages 490-513,Published online: 10 May 2021. Cite this article https://doi.org/10.1080/19361610.2021.1918995.

52. Zabidi. Nadirah, Abidi. Mohdmahdee Ismail, Zatul. Himmah Adnan, Mohd Izani. Mohd Zain, (2024). "Good Governance Practices for Sustainable Development in the Public Sector Services in Malaysia. Akademika 94(2), 252-266 https://doi.org/10.17576/akad-2024-9402-14.