


Research Article

Digital Citizenship in a Borderless World: Demographic Shifts and Governance Challenges in the Digital Age

Babak Elsan¹ , Mehdi Abbasi Sarmadi^{2*} 

¹ Ph.D. in English Language Teaching, LL.M. in International Law, Department of International Law, Faculty of Law and Political Science, Kharazmi University, Tehran, Iran.

² Associate Professor of International Law, Department of International Law, Faculty of Law and Political Science, Kharazmi University, Tehran, Iran.

ARTICLE INFO

Received: 20 January 2025

Accepted: 19 February 2025

Keywords:

Digital Citizenship, Digital Identity, Digital Divide, Virtual Migration, Global Governance, International Law, Cybersecurity.

ABSTRACT

The transformative advancements in digital technologies in recent decades have fundamentally reshaped traditional notions of citizenship, which were historically rooted in geographical boundaries and territorial sovereignty, introducing digital citizenship as an innovative alternative. This study adopts a systematic approach to examine the origins and evolution of digital citizenship from a demographic perspective while analyzing its associated governance challenges. Estonia's e-residency program and cross-border digital platforms for education and employment are highlighted as prominent examples, showcasing their potential to redefine identity, participation, and access within a transnational digital space. Nevertheless, the transition to digital citizenship faces significant challenges, including digital divides, legal ambiguities, and cybersecurity threats. Employing an interdisciplinary perspective, this research investigates the implications of digital societies on demographic mobility, fluid identities, and transnational employment opportunities, emphasizing the urgent need for adaptive governance frameworks to ensure digital equity. Finally, by analyzing successful global examples, the study offers practical recommendations for policymakers and professionals to strengthen digital justice and social inclusion, providing sustainable solutions to the complexities of the interconnected digital world. The findings underscore the necessity of innovative governance in addressing the multifaceted challenges of the contemporary digital ecosystem.

Introduction

The rapid evolution of digital technologies in recent decades has fundamentally reshaped traditional notions of citizenship, once inextricably linked to geographical borders and territorial sovereignty. As digital tools and platforms proliferate, they create opportunities for individuals to forge identities and engage in socio-economic activities independent of their physical location. This paradigm shift gives rise to the concept of digital citizenship—a framework in which rights, responsibilities, and social participation are redefined in a borderless environment. The emergence of digital diaspora communities, virtual migration, and cross-border labor markets challenges the conventional state-centric model of citizenship, necessitating new approaches to governance and legal regulation. This paper examines digital citizenship from a demographic perspective, exploring its

transformative impact on identity, social inclusion, and governance while addressing challenges such as cybersecurity, data privacy, and legal jurisdiction.

Method and Data

To capture the multifaceted nature of digital citizenship, this study adopts an interdisciplinary approach that integrates demographic analysis, case studies, and comparative legal review. Data were collected from diverse sources, including international reports by organizations such as the International Telecommunication Union (ITU, 2024), scholarly literature on digital diaspora communities, and empirical case studies focusing on pioneering initiatives like Estonia's e-residency program and India's Aadhaar system. The demographic analysis draws on quantitative data that elucidate trends in virtual

* Corresponding Author: Associate Professor of International Law, Department of International Law, Faculty of Law and Political Science, Kharazmi University, Tehran, Iran.

E-mail address: sarmadi@khu.ac.ir

E-ISSN: 3208-2717 / © National Institute for Population Research, Iran. This is an open access article under the CC BY 4.0 License (<https://creativecommons.org/licenses/by/4.0/>).

Cite this article:

Elsan, B., & Abbasi Sarmadi, M. (2025). Digital Citizenship in a Borderless World: Demographic Shifts and Governance Challenges in the Digital Age. *Iranian Population Studies Journal*, 9(1), 67-90. <https://doi.org/10.22034/jips.2025.500971.1256>

migration, population mobility, and generational differences in digital engagement. In parallel, qualitative methods—including policy analysis and comparative legal review—are used to assess the effectiveness of legal frameworks such as the Budapest Convention on Cybercrime (2001) and the European Union's General Data Protection Regulation (GDPR, 2016) in addressing the complexities of transnational digital interactions. By combining these methodological strands, the study seeks to provide a comprehensive overview of how digital identity initiatives influence demographic patterns and challenge established legal norms.

Findings

The findings of the study reveal significant demographic and legal shifts associated with the rise of digital citizenship. On the demographic front, there is a clear trend toward virtual migration, where individuals leverage digital platforms to access global employment, education, and entrepreneurial opportunities without the need for physical relocation. Estonia's e-residency program is a prime example, demonstrating how digital identity systems can attract a diverse pool of global entrepreneurial talent by bypassing traditional bureaucratic hurdles. Conversely, India's Aadhaar system illustrates the potential of biometric-based identification to foster financial and social inclusion on a massive scale, even as it raises important questions regarding data security and individual privacy.

Despite these promising developments, the study also highlights persistent digital divides that undermine equitable access to digital citizenship. Rural populations, older citizens, and economically marginalized groups continue to face significant barriers, ranging from inadequate technological infrastructure to limited digital literacy. These disparities are compounded by the uneven distribution of digital resources, which not only affects access to services but also exacerbates broader social and economic inequalities.

From a governance perspective, the research finds that traditional legal frameworks are often ill-equipped to handle the borderless nature of digital interactions. Instruments such as the GDPR and the Budapest Convention on Cybercrime have made important strides in addressing issues of data privacy and cybersecurity; however, they are frequently outpaced by the rapid evolution of digital technologies and the increasingly complex landscape of transnational data flows. The study underscores the challenges of applying territorial legal principles to activities that occur seamlessly across borders, noting that extraterritorial application of national laws can lead to legal ambiguities and conflicts. Additionally, the concentration of power among large technology firms introduces further complications, as these entities wield significant influence over data flows and digital interactions, often beyond the reach of conventional regulatory frameworks.

Discussion and Conclusion

The findings of this study underscore the need for a reimagined approach to citizenship and governance in the digital age. As digital citizenship challenges the long-established paradigms of territoriality and state control, there is an urgent call for adaptive governance frameworks that can accommodate the fluidity and borderless nature of digital interactions. Policymakers must consider multi-stakeholder governance models that bring together governments, technology companies, civil society, and international organizations to collaboratively address issues of data privacy, cybersecurity, and digital inclusion.

Moreover, the persistence of digital divides—whether along geographic, generational, or socio-economic lines—calls for targeted investments in digital infrastructure and literacy programs. Ensuring that marginalized communities have equitable access to digital resources is not only a matter of social justice but also essential for the sustainable development of global digital ecosystems. The study recommends implementing comprehensive policies that prioritize the expansion of broadband connectivity, the development of affordable digital tools, and the enhancement of digital skills training, particularly in underserved regions.

In terms of legal and regulatory challenges, the study advocates for a more flexible and internationally coordinated legal framework that can effectively address the unique issues posed by digital citizenship. Establishing common standards for data protection, cybersecurity, and digital identity recognition will require enhanced international cooperation and dialogue. Such an approach could help bridge the gap between national legal systems and the realities of a digital world where data and digital interactions transcend traditional borders.

Finally, the research emphasizes that the transformative potential of digital citizenship hinges on finding a balance between innovation and accountability. While digital platforms have the power to democratize access to information, services, and opportunities, they also pose risks related to privacy, surveillance, and unequal power dynamics. Achieving this balance will require ongoing efforts to refine legal frameworks, bolster digital literacy, and promote ethical governance practices that are responsive to the evolving digital landscape.

In conclusion, this study provides a comprehensive demographic perspective on the emergence of digital citizenship, highlighting both its transformative potential and its inherent challenges. By examining case studies such as Estonia's e-residency and India's Aadhaar, the research demonstrates that while digital technologies can enhance social inclusion and drive economic growth, they also necessitate significant adaptations in governance and legal regulation. Addressing these challenges will be critical for ensuring that the benefits of digital citizenship are realized equitably, paving the way for a more inclusive and just digital future.

شهروندی دیجیتال در جهانی بدون مرز: تحولات جمعیتی و چالش‌های حکمرانی در عصر دیجیتال

بابک السان^۱، مهدی عباسی سرمدی^{۲*}

^۱ دکترای آموزش زبان انگلیسی، دانشجوی کارشناسی ارشد حقوق بین‌الملل، دانشکده حقوق و علوم سیاسی، گروه حقوق بین‌الملل، دانشگاه خوارزمی، تهران، ایران.
^۲ دانشیار حقوق بین‌الملل، گروه حقوق بین‌الملل، دانشکده حقوق و علوم سیاسی، دانشگاه خوارزمی، تهران، ایران.

چکیده

تحولات چشمگیر فناوری‌های دیجیتال در دهه‌های اخیر مفاهیم سنتی شهروندی مبتنی بر مرزهای جغرافیایی و حاکمیت سرزمینی را به‌طور بنیادین دگرگون کرده و شهروندی دیجیتال را به‌عنوان جایگزینی نوآورانه معرفی نموده است. این پژوهش با رویکردی نظام‌مند، خاستگاه و شکل‌گیری شهروندی دیجیتال را از منظر جمعیت‌شناسی بررسی کرده و چالش‌های حکمرانی آن را تحلیل می‌کند. برنامه اقامت الکترونیکی استونی و پلتفرم‌های دیجیتال فرامرزی در حوزه آموزش و اشتغال به‌عنوان نمونه‌هایی برجسته معرفی شده‌اند که ظرفیت بازتعریف هویت، مشارکت و دسترسی در فضای دیجیتال فراملی را نشان می‌دهند. با این حال، گذار به شهروندی دیجیتال با چالش‌هایی همچون شکاف‌های دیجیتالی، ابهامات حقوقی و تهدیدات امنیت سایبری مواجه است. این پژوهش با رویکرد میان‌رشته‌ای، اثرات ظهور جوامع دیجیتال بر پویایی‌های جمعیتی، هویت‌های سیال و فرصت‌های شغلی فراملی را بررسی می‌کند و بر ضرورت چارچوب‌های حکمرانی تطبیقی برای تضمین عدالت دیجیتال تأکید دارد. در نهایت، با تحلیل نمونه‌های موفق جهانی، این مطالعه توصیه‌هایی عملی برای سیاست‌گذاران و متخصصان ارائه می‌دهد تا با تقویت عدالت دیجیتال و شمولیت اجتماعی، پاسخی پایدار به پیچیدگی‌های جهان به‌هم‌پیوسته دیجیتال ارائه دهند. یافته‌ها بر ضرورت حکمرانی نوآورانه در مدیریت ابعاد متکثر زیست‌بوم دیجیتال تأکید دارند.

اطلاعات مقاله

دریافت: ۱۴۰۳/۱۱/۰۱

پذیرش: ۱۴۰۳/۱۲/۰۱

کلیدواژه‌ها:

شهروندی دیجیتال، هویت دیجیتال، شکاف دیجیتال، مهاجرت مجازی، حکمرانی جهانی، حقوق بین‌الملل، امنیت سایبری.

۱. مقدمه

به‌عنوان یک مفهوم نوین، برخاسته از اکوسیستم متصل و بدون مرز، بر مشارکت مجازی، مسئولیت‌های مشترک جهانی و دسترسی بی‌سابقه به فرصت‌ها تأکید دارد و چارچوب‌های محدودکننده دولت‌ملت‌های سنتی را به چالش می‌کشد.

به‌طور کلی، شهروندی دیجیتال به معنای «توانمندی، حس تعلق و امکان مشارکت در جامعه اطلاعاتی» تعریف می‌شود

تحولات سریع فناوری‌های دیجیتال، ابعاد جدیدی به تعاملات جهانی، ساختارهای حکومتی و هویت‌های اجتماعی افزوده است. این تحولات باعث شده‌اند که مفهوم سنتی شهروندی، که به‌شدت با جغرافیا و حاکمیت سرزمینی گره خورده بود، در مواجهه با پارادایم نوظهور شهروندی دیجیتال^۱ دچار تغییر شود. شهروندی دیجیتال

1. Digital Citizenship

* نویسنده مسئول: دانشیار حقوق بین‌الملل، گروه حقوق بین‌الملل، دانشکده حقوق و علوم سیاسی، دانشگاه خوارزمی، تهران، ایران.
نشانی ایمیل: sarmadi@khu.ac.ir

استناد به این مقاله:

السان، بابک، و عباسی سرمدی، مهدی (۱۴۰۴). شهروندی دیجیتال در جهانی بدون مرز: تحولات جمعیتی و چالش‌های حکمرانی در عصر دیجیتال، دوفصلنامه مطالعات جمعیتی، دوره ۹، شماره ۱ (۱۷)، ۶۷-۹۰. <https://doi.org/10.22034/jips.2025.500971.1256>

مدل‌های حکمرانی موجود را نیز با چالش‌های اساسی روبه‌رو ساخته است. ابهامات مرتبط با صلاحیت قضایی، حاکمیت بر داده‌ها و تهدیدات امنیت سایبری، ناکارآمدی قوانین سنتی را که برای زمینه‌های محدود به جغرافیا طراحی شده‌اند، برجسته کرده است (Chander, 2013). علاوه بر این، تمرکز قدرت در دستان شرکت‌های بزرگ فناوری، نگرانی‌هایی درباره پاسخگویی، حفظ حریم خصوصی و حکمرانی اخلاق محور ایجاد کرده است. رخدادهایی همچون رسوایی «تحلیل داده کمبریج»^{۱۱} لزوم ایجاد ساختارهای حقوقی قوی برای حفاظت از حقوق دیجیتال و پاسخ به این چالش‌ها را نشان می‌دهند (Zuboff, 2019).

این مقاله با اتخاذ رویکردی میان‌رشته‌ای، پیامدهای شهروندی دیجیتال را از منظر تحولات جمعیتی و چالش‌های حکمرانی بررسی می‌کند. تحلیل ارائه‌شده بر پایه مطالعات جمعیت‌شناسی و حقوق بین‌الملل است و تلاش دارد تا درکی جامع از تأثیر محیط‌های دیجیتال بر مفاهیم شهروندی، حقوق و تحولات اجتماعی ارائه دهد. هدف نهایی، پیوند دادن ابعاد نظری و عملی شهروندی دیجیتال و ارائه چارچوبی جامع برای درک پیامدهای اجتماعی و حقوقی آن است. این مقاله قصد دارد بینش‌های کاربردی برای سیاست‌گذاران، دانشگاهیان و متخصصانی که در حوزه پیچیدگی‌های عصر دیجیتال فعالیت می‌کنند، فراهم آورد.

۲. زمینه‌های نظری و تجربی پژوهش

۲-۱. از رعیت‌بودگی تا شهروندی دیجیتال

شهروندی به‌عنوان یک مفهوم تاریخی، همواره نقشی کلیدی در سازمان‌دهی جوامع و تعریف رابطه میان افراد و دولت‌ها ایفاء کرده است. در یونان باستان، شهروندی نمادی از شمول محدود بود که فقط به مردان آزاد و مشارکت‌کننده در امور عمومی تعلق داشت (Heater, 2004). در حالی که در امپراتوری روم، این مفهوم گسترش یافت و به ابزاری برای ادغام سیاسی و حکمرانی بر اقوام مختلف

(Mossberger et al., 2007: 2). این مفهوم حوزه‌هایی چون هویت دیجیتال^۱، سواد دیجیتال^۲، حقوق و وظایف کاربران را شامل می‌شود و حس تعلق فراملی ایجاد می‌کند که مرزهای جغرافیایی را کنار می‌گذارد. برخلاف شهروندی سنتی که بر پایه چارچوب‌های حقوقی و مرزهای سرزمینی ثابت استوار بود، شهروندی دیجیتال رویکردی پویا، داوطلبانه و غیرمتمرکز ارائه می‌دهد. نمونه‌هایی چون برنامه «اقامت الکترونیکی استونی»^۳ نشان می‌دهند که چگونه شهروندی دیجیتال می‌تواند حکمرانی را متحول کرده و امکان دسترسی به خدمات دولتی و اقتصادی را برای افراد غیرمقیم فراهم آورد (Kotka et al., 2013). همچنین، پلتفرم‌هایی نظیر «آکادمی خان»^۴، «کورسرا»^۵، «اداکس»^۶، «فیور»^۷ و «آپ‌ورک»^۸ جلوه‌ای از فرصت‌های دیجیتال بدون مرز هستند که دسترسی به آموزش و اشتغال را فراتر از مرزهای سیاسی و جغرافیایی امکان‌پذیر می‌سازند.

در عین حال، این تحولات چالش‌های قابل‌توجهی را نیز به همراه داشته‌اند. عصر دیجیتال موجب جابه‌جایی‌های جمعیتی جدیدی همچون مهاجرت مجازی^۹ و شکل‌گیری «جوامع پراکنده دیجیتال»^{۱۰} شده است. این جوامع امکان مشارکت‌های فرهنگی و سیاسی فراملی را فراهم کرده و بستر همکاری و هم‌افزایی جهانی را تقویت کرده‌اند. با این حال، دستاوردهای این اتصال دیجیتال به شکلی نابرابر توزیع شده است. تفاوت در دسترسی به زیرساخت‌های فناوری، نابرابری‌های اقتصادی و اجتماعی موجود را تشدید کرده و شکاف‌های دیجیتال میان جوامع از یک سو و نسل‌های مختلف از سوی دیگر را گسترش داده است (Van Dijk, 2020). علاوه بر این، شکاف‌های بین‌نسلی در استفاده از فناوری نشان می‌دهد که نسل‌های جوان، به‌عنوان پیشگامان تغییر، بیشترین تعامل را با جهان دیجیتال دارند، در حالی که نسل‌های مسن‌تر همچنان با چالش‌های فراوانی روبه‌رو هستند (Prensky, 2001; Van Deursen & Helsper, 2015).

ماهیت بدون مرز فضا‌های دیجیتال، نظام‌های حقوقی و

1. Digital Identity
2. Digital Literacy
3. Estonia's e-Residency Program
4. Khan Academy: <https://www.khanacademy.org/>
5. Coursera: <https://www.coursera.org/>
6. edEx: <https://www.edx.org/>
7. Fiverr: <https://www.fiverr.com/>
8. Upwork: <https://www.upwork.com/>
9. Virtual Migration
10. Digital Diaspora Communities
11. Cambridge Analytica

تبدیل شد (Marshall, 1950). ظهور دولت-ملت‌های مدرن در قرون هفدهم و هجدهم، سرزمینی بودن را به‌عنوان مبنای اصلی شهروندی تثبیت کرد و اصولی نظیر «حق خاک» و «حق خون» سازوکارهایی برای کسب شهروندی تدوین کردند که حقوق و تعهدات افراد را در چارچوب حاکمیت دولت‌ها مشخص می‌کردند (Isin, 2002; Brubaker, 1992). با این حال، این مدل که بر مرزهای ملی سختگیرانه استوار بود، به‌واسطه تحولاتی همچون مهاجرت، تجارت و انقلاب صنعتی با چالش‌هایی مواجه شد که چارچوب‌های سنتی شهروندی را متزلزل کرد و زمینه‌ساز تفاسیر جدیدتری از این مفهوم شد.

جهانی شدن در اواخر قرن بیستم و اوایل قرن بیست‌ویکم، نقطه عطفی در فاصله گرفتن از شهروندی مبتنی بر سرزمین ایجاد کرد. جریان آزاد کالاها، افراد و ایده‌ها از مرزها، ناکارآمدی مدل‌های سنتی دولت-ملت را برجسته ساخت. این پویایی‌ها به ظهور شهروندی دوگانه و چندگانه منجر شدند که افراد را قادر ساخت تا با بیش از یک دولت رابطه حقوقی داشته باشند. نمونه‌هایی مانند اعلامیه جهانی حقوق بشر^۱ (۱۹۴۸) و معاهده ماستریخت^۲ (۱۹۹۲) نشان‌دهنده تلاش برای تقویت حقوق و مسئولیت‌های فراملی است. مفهوم شهروندی جهانی نیز با تأکید بر شمولیت جهانی و همکاری بین‌المللی برای مقابله با چالش‌های مشترک ظهور کرد، اما کاستلز و دیویدسون^۳ (۲۰۰۰) هشدار می‌دهند که جهانی شدن نابرابری‌های عمیق‌تری ایجاد کرده است، چرا که بسیاری از مزایای مرتبط با تحرک فراملی تنها برای گروه‌های خاص اقتصادی و اجتماعی در دسترس است و جوامع حاشیه‌نشین از این فرصت‌ها بی‌بهره مانده‌اند. این چالش‌ها، نیاز به سیاست‌هایی برای توزیع عادلانه‌تر مزایا و ارتقای عدالت اجتماعی را برجسته می‌کنند. مطالعات انجام‌شده در ایران نشان می‌دهند که جهانی شدن با تمرکز بر بازارهای آزاد، نابرابری‌های اجتماعی و اقتصادی را افزایش داده، دسترسی گروه‌های آسیب‌پذیر به منابع و فرصت‌های اقتصادی را محدود کرده و سیاست‌های بازتوزیعی و نظارت‌های اجتماعی را برای کاهش این شکاف‌ها ضروری ساخته است (یزدانی، ۲۰۲۱، ص. ۱۲).

چالش‌های بی‌سابقه متحول ساخت. فضاها دیجیتال بستری برای مشارکت فراملی فراهم کرده‌اند که محدودیت‌های جغرافیایی را از میان برداشته و هویت‌ها را بازتعریف کرده‌اند. به گفته موسبرگر و همکاران (۲۰۰۷)، شهروندی دیجیتال امکان تعامل در شبکه‌های جهانی را بدون وابستگی به موقعیت فیزیکی فراهم می‌کند. نمونه‌هایی نظیر برنامه اقامت الکترونیکی استونی و پلتفرم‌های آموزشی و کاری مانند «کورسرا» و «آپورک»، نشان‌دهنده نقش فناوری در تقویت حس تعلق جهانی و مشارکت فعالانه هستند. با این حال، گذار به شهروندی دیجیتال پرسش‌های اساسی در مورد حکمرانی، عدالت و پاسخگویی ایجاد کرده است. چارچوب‌های حقوقی سنتی در برابر مسائل پیچیده‌ای مانند حاکمیت داده‌ها و حفاظت از حقوق دیجیتال ناکارآمدی خود را نشان داده‌اند. افزون بر این، «شکاف دیجیتال»^۴ میان جوامع و نسل‌های مختلف، نیاز به سیاست‌های هدفمند برای کاهش این نابرابری‌ها را برجسته می‌کند (Van Dijk, 2020). در عین حال، تمرکز قدرت در دستان شرکت‌های بزرگ فناوری، ضرورت ایجاد چارچوب‌های حقوقی و اخلاقی مناسب را برجسته کرده است. این بخش تأکید می‌کند که تحولات تاریخی در مفهوم شهروندی، به‌ویژه در عصر دیجیتال، نیازمند بازاندیشی در سیاست‌ها و رویکردهای حقوقی است تا شمولیت و عدالت اجتماعی به بهترین نحو تقویت شود.

جهانی شدن در اواخر قرن بیستم و اوایل قرن بیست‌ویکم، نقطه عطفی در فاصله گرفتن از شهروندی مبتنی بر سرزمین ایجاد کرد. جریان آزاد کالاها، افراد و ایده‌ها از مرزها، ناکارآمدی مدل‌های سنتی دولت-ملت را برجسته ساخت. این پویایی‌ها به ظهور شهروندی دوگانه و چندگانه منجر شدند که افراد را قادر ساخت تا با بیش از یک دولت رابطه حقوقی داشته باشند. نمونه‌هایی مانند اعلامیه جهانی حقوق بشر^۱ (۱۹۴۸) و معاهده ماستریخت^۲ (۱۹۹۲) نشان‌دهنده تلاش برای تقویت حقوق و مسئولیت‌های فراملی است. مفهوم شهروندی جهانی نیز با تأکید بر شمولیت جهانی و همکاری بین‌المللی برای مقابله با چالش‌های مشترک ظهور کرد، اما کاستلز و دیویدسون^۳ (۲۰۰۰) هشدار می‌دهند که جهانی شدن نابرابری‌های عمیق‌تری ایجاد کرده است، چرا که بسیاری از مزایای مرتبط با تحرک فراملی تنها برای گروه‌های خاص اقتصادی و اجتماعی در دسترس است و جوامع حاشیه‌نشین از این فرصت‌ها بی‌بهره مانده‌اند. این چالش‌ها، نیاز به سیاست‌هایی برای توزیع عادلانه‌تر مزایا و ارتقای عدالت اجتماعی را برجسته می‌کنند. مطالعات انجام‌شده در ایران نشان می‌دهند که جهانی شدن با تمرکز بر بازارهای آزاد، نابرابری‌های اجتماعی و اقتصادی را افزایش داده، دسترسی گروه‌های آسیب‌پذیر به منابع و فرصت‌های اقتصادی را محدود کرده و سیاست‌های بازتوزیعی و نظارت‌های اجتماعی را برای کاهش این شکاف‌ها ضروری ساخته است (یزدانی، ۲۰۲۱، ص. ۱۲).

ظهور فناوری‌های دیجیتال، شهروندی را با فرصت‌ها و

۲-۲. تفاوت‌های شهروندی دیجیتال با شهروندی سنتی

شهروندی دیجیتال با مدل‌های سنتی شهروندی، که بر مبنای روابط سرزمینی و حقوقی میان افراد و دولت‌ها استوار است، تفاوت‌های بنیادینی دارد. این تمایزات بازتاب‌دهنده تحولات اجتماعی و فناورانه‌ای است که در عصر جهانی شدن و دیجیتالی شدن پدید آمده‌اند. در مدل‌های کلاسیک، همان‌طور که مارشال (۱۹۵۰) توضیح می‌دهد، شهروندی بر پایه حق خاک و حق خون تعریف می‌شود و حقوق و وظایف شهروندان در چارچوب‌های قانونی و مرزهای جغرافیایی مشخص قرار می‌گیرد. هیتز (۲۰۰۴) نیز بر این نکته تأکید دارد که این مدل‌های تاریخی روابط حقوقی میان افراد و دولت‌ملت‌ها را تثبیت می‌کردند. لذا، اصولاً یک رابطه نظیربه‌نظیر بین شهروندان و دولت وجود داشت به طوری که هر دولت فقط

1. Universal Declaration of Human Rights (UDHR), United Nations
2. Maastricht Treaty
3. Castles & Davidson
4. Digital Divide

قوانین رسمی تعریف و اجرا می‌شوند. در شهروندی دیجیتال، حقوقی مانند آزادی بیان و حفاظت از حریم خصوصی داده‌ها بر اساس سیاست‌های پلتفرمی و مقررات پراکنده تعریف شده‌اند. با این حال، همان‌طور که **سولوو**^۳ (۲۰۱۰) بیان می‌کند، این حقوق در سطح جهانی به‌طور نابرابر اجرا می‌شوند. به‌علاوه، **لینگستون**^۴ (۲۰۰۴) بر مسئولیت‌های خاص فضای دیجیتال مانند تعامل اخلاقی و مقابله با اطلاعات نادرست تأکید دارد که برای تقویت اعتماد و مشارکت آگاهانه در محیط‌های متصل ضروری است. در همین راستا، فناوری اطلاعات امکان ارائه خدمات عمومی الکترونیک و شفاف‌سازی را فراهم می‌کند، اما مسئولیت و پاسخ‌گویی در این مدل‌ها تنها به کنش‌گری شهروندان محدود نمی‌شود. بلکه رفتار متقابل و تعهد دولت به شفافیت و عدالت، عامل کلیدی در تقویت اعتماد عمومی و پایداری اجتماعی به‌شمار می‌رود (**خلیلی**، ۱۳۹۴).

در زمینه حکمرانی، شهروندی دیجیتال در مقایسه با مدل سنتی که مبتنی بر مدیریت مستقیم دولت‌هاست، از اکوسیستمی غیرمتمرکز شامل دولت‌ها، شرکت‌های فناوری، سازمان‌های غیردولتی، و افراد بهره می‌برد. به گفته **کِر**^۵ (۲۰۱۹)، این سیستم‌های غیرمتمرکز چالش‌هایی مانند پاسخ‌گویی و عدالت را به همراه دارند. از سویی دیگر، هوش مصنوعی^۶ با پیچیده‌تر کردن روابط میان دولت‌ها، صنایع، و افراد، بر اهمیت بهره‌گیری از نیروی متخصص و آموزش دیده برای واکنش سریع و مؤثر به تحولات ناشی از این پدیده می‌افزاید (**دهقانی فیروزآبادی و چهرآزاد**، ۱۴۰۲). بنابراین، توسعه چارچوب‌های تطبیقی و همکاری‌های بین‌المللی برای مدیریت این محیط‌ها ضروری است. در نهایت، هرچند شهروندی دیجیتال با شمولیت بیشتری همراه است و هر فرد دارای دسترسی به اینترنت می‌تواند بخشی از آن باشد، اما شکاف دیجیتال همچنان مانع مشارکت کامل جمعیت‌های حاشیه‌نشین می‌شود. **وان‌دایک** (۲۰۲۰) بر این نکته تأکید دارد که دسترسی نابرابر به زیرساخت‌ها و ابزارهای دیجیتال همچنان چالشی جدی برای تحقق عدالت دیجیتال^۷ محسوب می‌شود. برای

بر شهروندان خود و قلمرو خود اعمال حاکمیت می‌کرد و هر شهروندی نیز صرفاً تحت حاکمیت دولت متبوع خود بوده است. این رابطه نظیر به نظیر در دهه‌های اخیر به دنبال جهانی شدن کم‌رنگ‌تر شده و با افزایش مهاجرت‌ها و مسافرت‌های فرامرزی، ظهور و گسترش شرکت‌های چند ملیتی، و از همه مهم‌تر پیدایش شبکه جهانی وب و ظهور عصر دیجیتال، دیگر نه دولت‌ها، همانند سابق، حاکمیت مطلق بر شهروندان خود می‌توانند اعمال نمایند و نه شهروندان لزوماً تحت حاکمیت یک دولت قرار دارند. به عبارتی دیگر، شهروندی دیجیتال مرزهای جغرافیایی را پشت سر گذاشته و بر هویت‌های خودتعریف‌شده و مشارکت داوطلبانه در فضای مجازی مبتنی است. این نوع شهروندی نشان‌دهنده تغییری بنیادی در نحوه ارتباط افراد با جوامع و نهادهای حکمرانی بوده و امکان مشارکت جهانی و تعامل آزاد را فراهم می‌آورد.

البته، دولت‌ها نیز در رقابت با شکل‌گیری شهروندی دیجیتال جهانی به دنبال ایجاد نسخه دیجیتالی خود و حفظ حاکمیت خود بر اتباعشان و در هر حال، به دنبال اعمال قدرت بر شهروندان به روش‌های نوین هستند. این قدرت، برخلاف رویکردهای مستقیم و کنترل‌گرانه گذشته، از طریق ابزارهای دیجیتال و شبکه‌های اطلاعاتی اعمال می‌شود. همان‌طور که در پژوهش **شهریاری و رهبر**^۱ (۱۴۰۲) آمده است، دولت‌های دیجیتال همواره قدرت نامرئی خود را بر شهروندان اعمال می‌کنند و آن‌ها را متقاعد و متلازم می‌سازند تا در زنجیره سودفایده و اهداف دولت دیجیتال^۲ همراه باشند (صص. ۲۴۹-۲۴۸). این تحولات نشان می‌دهد که هدف دولت‌ها از دیجیتالی‌سازی نمودن خود، علاوه بر ارائه خدمات رفاهی، به دنبال کنترل و رصد رفتارهای شهروندان از طریق فناوری‌های پیشرفته و نهایتاً رقابت با حاکمیت‌های دیجیتالی دولت‌ها یا نهادهای برون‌مرزی بر اتباع خود هستند.

حقوق و مسئولیت‌های شهروندی در این دو نوع مدل سنتی و دیجیتال به‌طور قابل توجهی متفاوت هستند. در مدل سنتی، حقوق شامل دسترسی به خدمات عمومی، حمایت قانونی، و مشارکت سیاسی در چارچوب دولت‌ملت است و این حقوق از طریق

1. Shahriari & Rahbar (2023)
2. Digital government
3. Solove
4. Livingstone
5. Kerr
6. Artificial intelligence
7. Digital justice

رفع این نابرابری‌ها، توسعه زیرساخت‌ها و آموزش سواد دیجیتال ضروری است.

۲-۳. شهروندی دیجیتال و تحول در مفاهیم هویت و تعلق

شهروندی دیجیتال مفاهیم سنتی هویت و تعلق را به‌طور بنیادینی متحول کرده و چارچوب‌های قدیمی مبتنی بر جغرافیا و فرهنگ را به چالش کشیده است. در عصر دیجیتال، هویت به شکلی سیال و چندوجهی تعریف می‌شود و از طریق تعاملات مجازی شکل می‌گیرد. **بایم^۱ (۲۰۱۵)** توضیح می‌دهد که رسانه‌های اجتماعی و دیگر پلتفرم‌های دیجیتال به‌عنوان محیطی برای بازنمایی و کاوش هویت عمل می‌کنند و به افراد امکان می‌دهند جنبه‌های مختلف هویت خود را بیان و با جوامعی ارتباط برقرار کنند که ارزش‌ها و علایقشان را منعکس می‌کنند. پلتفرم‌هایی مانند ردیت^۲ و دیسکورد^۳، به‌عنوان میزبان جوامع هدفمند، حس تعلق را ایجاد می‌کنند که اغلب در محیط‌های غیرمجازی دست‌نیافتنی است. این تحول، فرصت‌هایی برای بازسازی هویت جمعی و شکل‌گیری جوامع جدید فراهم کرده است، اما پرسش‌هایی درباره تأثیرات آن بر روابط اجتماعی سنتی، مرزهای فرهنگی و سیاست‌گذاری‌های هویتی به وجود آورده است. ساخت هویت در فضای دیجیتال با چالش‌هایی مانند اصالت، حریم خصوصی و تجاری‌سازی مواجه است. توانایی کاربران در ایجاد مدیریت هویت‌های آنلاین، گاه شکافی میان هویت دیجیتال و واقعی ایجاد می‌کند و اعتماد و اعتبار را تحت تأثیر قرار می‌دهد. **زوباف (۲۰۱۹)** هشدار می‌دهد که تجاری‌سازی داده‌های شخصی توسط پلتفرم‌های دیجیتال، هویت را به کالایی بازاری تبدیل کرده است و کاربران را در معرض تبلیغات هدفمند و پروفایل‌سازی الگوریتمی قرار می‌دهد. این موضوع اهمیت تنظیم مقررات اخلاقی برای حفاظت از داده‌ها و تأمین خودمختاری کاربران را برجسته می‌کند. هم‌زمان، حس تعلق در عصر دیجیتال مرزهای ملی را پشت سر گذاشته و پیوندهای فراملی ایجاد کرده است. جوامع مجازی امکان مشارکت در گفتمان‌های جهانی را فراهم کرده و در عین حال، ارتباط با میراث فرهنگی را حفظ کرده‌اند. **برینگرهوف (۲۰۰۹)** نشان می‌دهد که گروه‌های مهاجر از پلتفرم‌های دیجیتال برای حفظ فرهنگ و پیشبرد اهداف سیاسی استفاده می‌کنند، و این تعاملات به کاهش شکاف

میان کشورهای مبدأ و محل سکونت کمک می‌کند. با این حال، فضاهای دیجیتال می‌توانند قطبیت و تفرقه را افزایش دهند. **واردل و درخشان (۲۰۱۷)** تأکید می‌کنند که اتاق‌های پژواک و اطلاعات نادرست می‌توانند دسترسی به دیدگاه‌های متنوع را محدود کرده و نگرش‌های تفرقه‌آمیز را تقویت کنند. ارتقاء سواد دیجیتال و ایجاد سازوکارهایی برای مشارکت فراگیر از جمله اقدامات ضروری برای کاهش این چالش‌ها است. این اقدامات می‌توانند تعادل میان فرصت‌ها و تهدیدهای فضای دیجیتال را برقرار کرده و پایداری اجتماعی را تقویت کنند. در این راستا، سیاست‌گذاری‌هایی برای حفاظت از داده‌ها، افزایش شمولیت و بهره‌برداری از مزایای شهروندی دیجیتال، مکمل شهروندی کلاسیک خواهند بود.

همان‌طور که مطرح شد، تحولات جمعیتی در عصر دیجیتال، با ظهور مفاهیمی مانند مهاجرت مجازی و دیاسپوراها دیجیتال، نشان‌دهنده تغییرات بنیادین در هویت و تعاملات اجتماعی هستند. در این میان، ابتکارهای نوآورانه‌ای مانند سیستم آدهار هند و برنامه اقامت الکترونیکی استونی، نمونه‌های برجسته‌ای از تطبیق حکمرانی با این تحولات محسوب می‌شوند. آدهار، با ارائه هویت دیجیتال یکپارچه به شهروندان هندی، شمول اجتماعی و مالی را تقویت کرده و فرصت‌هایی برای کاهش نابرابری‌ها فراهم آورده است. از سوی دیگر، برنامه اقامت الکترونیکی استونی، با گسترش مفهوم شهروندی دیجیتال فراتر از مرزهای جغرافیایی، بستری برای تعاملات اقتصادی بین‌المللی و حکمرانی جهانی ایجاد کرده است. این دو نمونه، با تأکید بر بهره‌گیری از فناوری برای شمولیت و نوآوری، نشان می‌دهند که چگونه دیجیتالی‌سازی می‌تواند مفاهیم سنتی هویت و تعلق را بازتعریف کرده و زمینه‌ساز عدالت اجتماعی و اقتصادی در مقیاس جهانی شود. در ادامه، این دو برنامه اجمالی مورد بررسی قرار می‌گیرند تا به درک ملموس‌تری از چگونگی تأثیر فناوری بر حکمرانی مدرن دست یابیم.

۲-۴. سیستم آدهار هند: ابتکاری پیشگام در هویت دیجیتال و شمول اجتماعی

سیستم آدهار هند، به‌عنوان یکی از جامع‌ترین پروژه‌های هویت دیجیتال، از زمان راه‌اندازی خود در سال ۲۰۰۹ تحول شگرفی در ارائه

1. Baym
2. Reddit
3. Discord

کاربران منجر شوند. الزام به پیوند آدهار با خدمات ضروری مانند حساب‌های بانکی، تلفن همراه و یارانه‌های دولتی نیز چالش‌برانگیز بوده است. این الزام، گرچه شفافیت و کارایی را افزایش داده، اما ممکن است منجر به حذف گروه‌های حاشیه‌نشین شود. از این رو، ایجاد چارچوب‌های حفاظتی قوی برای تقویت اعتماد عمومی برای این قبیل پروژه‌ها حائز اهمیت است. همچنین، چاندر و لی (۲۰۱۵) بر لزوم تعادل میان شمول اجتماعی، امنیت داده‌ها و کارایی سیستم تأکید می‌کنند. آن‌ها هشدار می‌دهند که بدون نظارت دقیق و سیاست‌گذاری جامع، این سیستم‌ها می‌توانند به تهدیدی برای عدالت اجتماعی تبدیل شوند. در نهایت، آدهار نمونه‌ای بارز از استفاده از فناوری برای رفع شکاف‌های هویتی و ارتقای شمول اجتماعی است. این سیستم، با بهبود کارایی، کاهش فساد و افزایش شفافیت، دستاوردهای قابل توجهی داشته است. اما چالش‌های مرتبط با حریم خصوصی، امنیت داده‌ها و نابرابری در دسترسی، بر اهمیت سیاست‌گذاری هوشمند و طراحی شمول‌محور تأکید دارند. تجربه آدهار نشان می‌دهد که فناوری دیجیتال می‌تواند تحولات اجتماعی و اقتصادی عمیقی ایجاد کند، اما موفقیت پایدار آن مستلزم تعادل دقیق میان امنیت، کارایی و عدالت اجتماعی است.

۲-۵. برنامه اقامت الکترونیکی استونی: بازتعریف شهروندی دیجیتال و حکمرانی جهانی

برنامه اقامت الکترونیکی استونی که از سال ۲۰۱۴ آغاز شد، مفهومی نوین از شهروندی دیجیتال را ارائه می‌دهد. این برنامه با کنار زدن محدودیت‌های سنتی جغرافیایی، امکان دسترسی جهانی به خدمات دولتی دیجیتال، نظیر ثبت شرکت و امضای اسناد، را فراهم کرده است. اقامت الکترونیکی استونی الگویی نوین از حکمرانی جهانی مبتنی بر شمولیت، نوآوری و دسترسی آسان ارائه کرده و تعاملات اقتصادی بین‌المللی را تسهیل می‌کند. این برنامه با عملی نمودن مفهوم «اقتصاد دیجیتال بدون مرز»^۶ این امکان را داده است که افراد، به‌ویژه از کشورهای در حال توسعه، بدون حضور فیزیکی در اروپا کسب‌وکار ثبت کرده و از بازارهای بین‌المللی بهره‌مند شوند. این نوآوری فرصت‌های جدیدی برای کوچ‌نشینان دیجیتال و

خدمات دولتی و گسترش شمول اجتماعی و مالی ایجاد کرده است. این طرح، که توسط سازمان شناسایی منحصر به فرد هند^۱ (UIDAI) مدیریت می‌شود، به هر فرد یک شماره شناسایی ۱۲ رقمی اختصاص می‌دهد که با داده‌های بیومتریک و اطلاعات جمعیتی مرتبط است. هدف اصلی آدهار، رفع شکاف‌های هویتی و توانمندسازی گروه‌های حاشیه‌نشین از طریق ادغام در سیستم اقتصادی رسمی بوده است. تاکنون بیش از ۱.۳ میلیارد نفر در این سیستم ثبت‌نام کرده‌اند.

به بیان راتو و نایر (۲۰۱۹)^۲ یکی از دستاوردهای کلیدی آدهار، اجرای موفق طرح انتقال مستقیم مزایا^۳ (DBT) است. این سیستم با حذف واسطه‌ها، پرداخت یارانه‌ها و کمک‌های دولتی را به‌طور مستقیم به حساب‌های بانکی افراد نیازمند تسهیل کرده است. این مکانیزم به کاهش فساد و نشت مالی کمک کرده است. یارانه‌های گاز پخت‌وپز، مستمری‌ها و بورسیه‌های تحصیلی نمونه‌هایی از خدماتی هستند که از طریق آدهار به‌صورت مؤثرتر ارائه شده‌اند. آدهار همچنین در گسترش شمول مالی تأثیرگذار بوده است. این سیستم به افراد فاقد مدارک هویتی رسمی کمک کرده تا حساب‌های بانکی افتتاح کنند. ادغام این طرح با برنامه‌هایی نظیر «جان‌دهن یوجانا»^۴ میلیون‌ها نفر را به خدمات مالی و تسهیلات اعتباری متصل کرده است. همچنین، ادغام آدهار در اکوسیستم پرداخت دیجیتال هند باعث تسهیل تراکنش‌های موبایلی و تقویت اقتصاد دیجیتال این کشور شده است. این سیستم در بخش‌های بهداشت و آموزش نیز نقشی اساسی ایفاء کرده است. در حوزه بهداشت، آدهار با ساده‌سازی فرآیند شناسایی بیماران و ثبت سوابق پزشکی، دسترسی به خدمات درمانی را بهبود داده است. در آموزش، آدهار به شناسایی دانش‌آموزان مستحق بورسیه و گسترش خدمات آموزشی در مناطق کمتر توسعه‌یافته کمک کرده است. این دستاوردها توان بالقوه فناوری دیجیتال در بهبود ارائه خدمات عمومی در مقیاس وسیع را نشان می‌دهد.

با این حال، آدهار با چالش‌ها و انتقادات متعددی مواجه است. چاندر و لی^۵ (۲۰۱۵) به مسائل امنیت داده‌ها و حریم خصوصی اشاره کرده‌اند و هشدار داده‌اند که سیستم‌های متمرکزی مانند آدهار، بدون حفاظت‌های کافی، ممکن است به نقض حریم خصوصی

1. Unique Identification Authority of India (UIDAI)

2. Rao & Nair

3. Direct Benefit Transfer (DBT)

4. Pradhan Mantri Jan Dhan Yojana (طرح نخست‌وزیر برای ثروت مردم)

5. Chander & Le

6. Borderless Digital Economy

از طریق بررسی معاهدات و چارچوب‌های نظارتی مانند «کنوانسیون بوداپست در مورد جرایم سایبری»^۳ و «مقررات عمومی حفاظت از داده‌های اتحادیه اروپا»^۴ به‌عنوان نمونه‌هایی از ابزارهای حقوقی بین‌المللی تحلیل شده‌اند. این چارچوب‌ها تلاش‌هایی برای پاسخ به پیچیدگی‌های فضای دیجیتال و مدیریت حقوقی آن ارائه می‌دهند. مقاله با استفاده از تحلیل برنامه اقامت الکترونیکی استونی، برنامه آدهار هند^۵ و رسوایی تحلیل داده کمبریج (۲۰۱۶) سازمان یافته است.

۴. یافته‌ها

در پرتو تحلیل‌های نظری و مطالعات موردی پیش‌گفته، این بخش به تبیین یافته‌های اصلی پژوهش می‌پردازد که ابعاد گوناگون شهروندی دیجیتال در جهان بدون مرز را از منظر جمعیت‌شناختی، حقوقی و حکمرانی روشن می‌سازد. نتایج حاصل از بررسی برنامه‌های اقامت الکترونیکی استونی و سیستم آدهار هند، همراه با تحلیل داده‌های جمعیتی و حقوق بین‌الملل، نشان می‌دهد که شهروندی دیجیتال فراتر از یک پدیده فناورانه، به‌منزله تحولی ساختاری در روابط اجتماعی، اقتصادی و سیاسی عمل می‌کند؛ تحولی که هم‌زمان فرصت‌ها و چالش‌های نوینی را در زمینه‌های عدالت دیجیتال، شمول اجتماعی، و حاکمیت داده‌ها پدید آورده است. بر این اساس، در ادامه، یافته‌ها در چهار محور اصلی بررسی می‌شوند: نخست، فرصت‌های برآمده از گسترش فضاهای دیجیتال و توانمندی‌های نوین شهروندان؛ دوم، چالش‌های نهادی، حقوقی و اخلاقی ناشی از فقدان مرزهای سنتی در حکمرانی دیجیتال؛ سوم، پیامدهای جمعیتی، از جمله مهاجرت مجازی و ظهور دیاسپوراهای دیجیتال؛ و در نهایت، راهکارها و توصیه‌هایی برای ایجاد چارچوب‌های تطبیقی و آینده‌نگر در جهت تحقق عدالت و حکمرانی مؤثر در عصر دیجیتال.

۴-۱. فرصت‌ها در دنیای دیجیتال بدون مرز

بررسی داده‌ها و مطالعات موردی نشان می‌دهد که شهروندی دیجیتال علاوه بر چالش‌ها، فرصت‌های گسترده‌ای نیز برای توسعه انسانی و اقتصادی فراهم کرده است. محیط دیجیتال بدون مرز، محدودیت‌های جغرافیایی و قضایی را حذف کرده و فرصت‌هایی بی‌سابقه برای رشد اقتصادی، مشارکت اجتماعی، و نوآوری جهانی

کارگران از راه دور ایجاد کرده است، که در یک فضای امن و کارآمد فعالیت‌های حرفه‌ای خود را مدیریت کنند. استونی، با جدا کردن حکمرانی از مرزهای سرزمینی، به توسعه عدالت اقتصادی و شمولیت جهانی کمک کرده است.

با وجود موفقیت‌ها، مسائل امنیتی، سوءاستفاده، و نبود چارچوب‌های حقوقی بین‌المللی از چالش‌های کلیدی این برنامه هستند. خطراتی چون کلاهبرداری و پولشویی، علی‌رغم استفاده از فناوری‌های پیشرفته مانند بلاکچین، همچنان وجود دارند (e-Estonia, 2024, April 9).^۱ همچنین، هماهنگی ناکافی قوانین بین‌المللی و مسائل مربوط به حریم خصوصی داده‌ها اعتماد کاربران را تهدید می‌کند. ایجاد تعادل میان نوآوری و مسئولیت‌پذیری، همان‌طور که چاندر (۲۰۱۳) تأکید می‌کند، برای موفقیت این برنامه ضروری است. از این رو، برای دستیابی به حکمرانی دیجیتالی جهانی یکپارچه، سیاست‌گذاری دقیق و هماهنگی بین‌المللی لازم است. به‌رغم کاستی‌ها و چالش‌های موجود، برنامه اقامت الکترونیکی استونی الگویی برای ارتقای شمولیت اقتصادی و تقویت تعاملات دیجیتال است که با همکاری‌های جهانی می‌تواند به الگویی پایدار برای آینده تبدیل شود.

۳. روش پژوهش

این مقاله با اتخاذ رویکردی میان‌رشته‌ای به بررسی پیامدهای شهروندی دیجیتال در دنیایی بدون مرز می‌پردازد. تحلیل ارائه‌شده بر دو حوزه مکمل تکیه دارد: مطالعات جمعیت‌شناسی و حقوق بین‌الملل. از طریق ادغام این دو دیدگاه، مقاله تلاش دارد تا درکی جامع از تأثیر محیط‌های دیجیتال بر تحولات جمعیتی و چالش‌های حقوقی و حکمرانی مرتبط ارائه دهد. در بخش مطالعات جمعیت‌شناسی، تحولات ناشی از مهاجرت دیجیتال، تغییرات جمعیتی و شکل‌گیری هویت در عصر دیجیتال مورد بررسی قرار گرفته است. این تحلیل بر مبنای گزارش‌های سازمان‌های بین‌المللی مانند اتحادیه بین‌المللی مخابرات^۲ و مطالعات موردی درباره دیاسپوراهای دیجیتال و اکوسیستم‌های کاری از راه دور استوار است که عمدتاً بازه زمانی سال‌های ۲۰۰۰ تا ۲۰۲۴ را در بر می‌گیرند.

در حوزه حقوق بین‌الملل نیز چالش‌های مرتبط با شهروندی دیجیتال

1. E-Estonia. (2024, April 9): Retrieved from <https://e-estonia.com/2023-estonia-advanced-cybersecurity-threats/>
2. International Telecommunication Union (ITU)
3. Budapest Convention on Cybercrime (Council of Europe, 2001)
4. The European Union's General Data Protection Regulation (GDPR, 2016)
5. Aadhaar System (India)

فناوری نگرانی‌هایی درباره عدالت و شمولیت ایجاد کرده است. برای رفع این نابرابری‌ها، وان‌دایک (۲۰۲۰) بر سرمایه‌گذاری در زیرساخت‌ها، تقویت ظرفیت‌ها، و سیاست‌گذاری‌های جامع تأکید می‌کند. اقدامات هدفمند در زیرساخت‌های مناطق محروم، همراه با آموزش سواد دیجیتال، می‌تواند توزیع عادلانه‌تر مزایا را تضمین کرده و عدالت اجتماعی را در فضای دیجیتال تقویت کند.

۴-۲. چالش‌ها در دنیای دیجیتال بدون مرز

با وجود فرصت‌های گسترده، محیط دیجیتال بدون مرز چالش‌های پیچیده‌ای در حوزه‌های حکمرانی، امنیت و عدالت به همراه دارد. نبود مرزهای فیزیکی در فضای سایبری، سازوکارهای سنتی کنترل و نظارت را مختل کرده و آسیب‌پذیری‌هایی ایجاد نموده است که تمامی افراد، کسب‌وکارها و دولت‌ها را تحت تأثیر قرار می‌دهد.

یکی از چالش‌های اساسی، حاکمیت دیجیتال است. با عبور آزادانه داده‌ها از مرزها، پرسش‌های جدی درباره کنترل و حفاظت از این داده‌ها مطرح می‌شود. دولت‌ها در مدیریت فعالیت‌های دیجیتالی فرامرزی که بر شهروندان یا زیرساخت‌های آن‌ها تأثیر می‌گذارد، با دشواری‌هایی مواجه‌اند. حملات سایبری و نقض‌های امنیتی اغلب از خلأهای قضایی سوءاستفاده می‌کنند و قربانیان را با گزینه‌های محدود برای جبران خسارت مواجه می‌سازند (Chander, 2013). کنوانسیون بوداپست در مورد جرایم سایبری (۲۰۰۱) کوشیده است از طریق همکاری بین‌المللی، این شکاف‌ها را پر کند. با این حال، ناهماهنگی در پذیرش این چارچوب، به‌ویژه از سوی بازیگران اصلی نظیر چین و روسیه، اثربخشی آن را محدود کرده است و چالشی جدی برای مدیریت جهانی جرایم سایبری و حفاظت از داده‌ها ایجاد کرده است.

تمرکز قدرت در شرکت‌های بزرگ فناوری^{۱۱} نظیر گوگل، متا، آمازون، و اپل، چالشی دیگر در عصر دیجیتال است. این شرکت‌ها نه تنها بر بازارهای دیجیتال تسلط دارند، بلکه بر گفتمان عمومی،

فراهم آورده است. این فضا با دموکراتیزه کردن دانش، از طریق پلتفرم‌هایی مانند «آکادمی خان»^۱، «کورسرا»^۲ و «اداکس»^۳ آموزش باکیفیت را در دسترس افراد در سراسر جهان قرار داده و طبق گزارش بانک جهانی^۴ (۲۰۱۸) شکاف‌های آموزشی و اقتصادی را کاهش داده است. همچنین، انتشار دسترسی آزاد به دانش علمی، پژوهش‌های بین‌رشته‌ای را تسریع کرده است. در حوزه اقتصادی، پلتفرم‌های تجارت الکترونیک مانند آمازون،^۵ علی‌بابا،^۶ و شاپیفای^۷ امکان دسترسی کسب‌وکارها، فارغ از اندازه و سرمایه آن‌ها، به بازارهای بین‌المللی را فراهم کرده و شمولیت اقتصادی را تقویت کرده‌اند. به‌ویژه، شرکت‌های کوچک در کشورهای در حال توسعه با کاهش موانع ورود به بازارهای جهانی رقابت می‌کنند. پلتفرم‌های اقتصاد گیگ^۸ مانند آپ‌ورک^۹ و فیور^{۱۰} نیز با از میان برداشتن موانع جغرافیایی، امکان مشارکت کارگران در بازارهای جهانی را فراهم ساخته‌اند. با این حال، این مزایا چالش‌هایی همچون دستمزد پایین و شرایط کاری ناپایدار را به‌همراه دارد (Graham et al., 2017) که سیاست‌گذاری‌های حمایتی برای رفع آن‌ها ضروری است.

از منظر اجتماعی، شبکه‌های اجتماعی نظیر توئیتر و فیسبوک ابزارهایی برای تقویت جنبش‌های جهانی نظیر جمع‌ها برای آینده (#FridaysForFuture)، من‌هم (#MeToo) و حذف جنسیت از زبان (#HeForShe) بوده‌اند. این پلتفرم‌ها صدای گروه‌های حاشیه‌نشین را توانمند کرده و امکان بسیج عمومی برای اصلاحات اجتماعی را فراهم آورده‌اند (Tufekci, 2017). ابزارهای دیجیتال، تعامل جهانی را تقویت کرده و شکاف‌های ناشی از محدودیت‌های جغرافیایی را کاهش داده‌اند، به طوری که فضای دیجیتال به بستری توانمندساز برای عدالت اجتماعی، رشد اقتصادی، و گسترش دانش تبدیل شده است.

با وجود این فرصت‌ها، شکاف‌های دیجیتال در زمینه دسترسی، زیرساخت، و سواد دیجیتال، بخش‌هایی از جمعیت جهانی را از مزایای این فضا محروم کرده است. تمرکز قدرت در دست شرکت‌های بزرگ

1. Khan Academy: <https://www.khanacademy.org/>

2. Coursera: <https://www.coursera.org/>

3. edEx: <https://www.edx.org/>

4. World Bank

5. Amazon

6. Alibaba

7. Shopify

9. Upwork

10. Fiverr

11. Big Tech

۸. اقتصاد گیگ مدلی از اقتصاد است که در آن، کارفرمایان و کارمندان به‌صورت موقت و پروژه‌ای با یکدیگر همکاری دارند: ymonoce gig

پلتفرم‌های دیجیتالی و فرصت‌های کار از راه دور، تعاملات فراملی را بازتعریف کرده‌اند.

مهاجرت مجازی تأثیرات شگرفی بر نیروی کار جهانی داشته و الگوهای سنتی اشتغال را تغییر داده است. **گراهام و همکاران (۲۰۱۷)** اشاره می‌کنند که پلتفرم‌هایی نظیر Upwork، Fiverr و Toptal به فریلنسرها امکان دسترسی به بازارهای بین‌المللی را می‌دهند، به طوری که افراد می‌توانند بدون نیاز به مهاجرت فیزیکی، در اقتصاد جهانی مشارکت کنند. این شکل از تحرک دیجیتال به‌ویژه برای کارگران در کشورهای در حال توسعه سودمند است، زیرا آن‌ها را قادر می‌سازد تا در عین حفظ ارتباط با جوامع محلی، درآمدهای خود را به اقتصاد مبدأ تزریق کنند. علاوه بر این، مهاجرت مجازی هویت ترکیبی جدیدی را میان کارگران دیجیتال ایجاد کرده که تلفیقی از سنت‌های فرهنگی محلی و تأثیرات جهانی است. با این حال، چالش‌هایی نیز وجود دارد، از جمله وابستگی به پلتفرم‌های دیجیتال که رقابت ناعادلانه یا آسیب‌پذیری در برابر نوسانات بازار را به همراه دارد. علی‌رغم این چالش‌ها، مهاجرت مجازی ظرفیت‌های زیادی برای کاهش نابرابری‌های جهانی و تقویت عدالت اقتصادی دارد.

دیاسپوراها دیجیتال به‌عنوان یکی دیگر از ابعاد تحولات جمعیتی، با استفاده از فناوری‌های دیجیتال، ارتباط خود را با سرزمین مادری حفظ کرده و نقش‌های سیاسی و فرهنگی مهمی ایفاء می‌کنند. **برینکرهوف^۲ (۲۰۰۹)** تأکید دارد که فناوری و پلتفرم‌های دیجیتال ابزارهای مؤثری برای ایجاد و حفظ شبکه‌های اجتماعی دیاسپوراها فراهم کرده‌اند. گروه‌های دیاسپورا از پلتفرم‌هایی مانند فیس‌بوک^۳، توئیتر^۴ و واتساپ^۵ برای ایجاد و حفظ شبکه‌های اجتماعی و فرهنگی استفاده می‌کنند. این پلتفرم‌ها جوامع پراکنده را قادر می‌سازند تا در کمپین‌های بشردوستانه، فعالیت‌های سیاسی، و تبادلات فرهنگی مشارکت کنند. نمونه‌هایی مانند بسیج دیاسپورای ایتوپی در جریان درگیری‌های تیگرای نشان می‌دهد که چگونه دیاسپوراها دیجیتال از ابزارهای آنلاین برای افزایش آگاهی جهانی، جلب حمایت بین‌المللی، و ارائه کمک‌های بشردوستانه استفاده می‌کنند (**Brinkerhoff, 2009**). این پلتفرم‌ها همچنین به حفظ هویت فرهنگی کمک می‌کنند، زیرا دیاسپوراها می‌توانند

دسترسی به اطلاعات، و شیوه‌های جمع‌آوری داده‌ها نیز تأثیر عمیقی می‌گذارند. چنین تمرکزی رقابت را کاهش داده و نگرانی‌های اخلاقی در زمینه حریم خصوصی و سوءاستفاده از داده‌های کاربران را تقویت کرده است. **زوبوف (۲۰۱۹)** با اشاره به وقایعی نظیر رسوایی کمبریج آنالیتیکا، این سوءاستفاده‌ها را نماد سوءمدیریت قدرت دیجیتال می‌داند. این رویداد نشان داد که چگونه داده‌های شخصی کاربران بدون رضایت آن‌ها برای تأثیرگذاری بر تصمیم‌گیری‌های سیاسی مورد استفاده قرار می‌گیرد. برای رفع این چالش‌ها، تدوین چارچوب‌های نظارتی قوی و تضمین‌کننده حفظ حقوق کاربران و رقابت سالم ضروری است.

با وجود افزایش نفوذ اینترنت در سطح جهانی، شکاف دیجیتال همچنان مانعی جدی برای شمولیت در دنیای دیجیتال باقی مانده است. نابرابری‌های پایدار در دسترسی، هزینه، و سواد دیجیتال، به‌ویژه در میان جوامع روستایی و کم‌درآمد در کشورهای در حال توسعه، مشارکت این گروه‌ها در اکوسیستم دیجیتال را محدود می‌کند (**Van Dijk, 2020**). برنامه‌هایی نظیر اتحاد برای اینترنت مقرون‌به‌صرفه (**A4AI, 2021**)^۱ برای کاهش این شکاف‌ها تلاش می‌کنند، اما محدودیت منابع و چالش‌های زیرساختی پیشرفت در این زمینه را کند کرده است. رفع این شکاف نیازمند سرمایه‌گذاری پایدار در زیرساخت‌ها، سیاست‌های حمایتی جامع، و آموزش سواد دیجیتال در جوامع حاشیه‌نشین است. برای این امر، این تنها دولت‌ها هستند که می‌توانند نابرابری‌های منابع و امکانات را کاهش داده و نقش کلیدی در تحقق عدالت دیجیتال ایفاء کند (**خلیلی, ۱۳۹۴**).

۳-۴. تحولات جمعیتی در عصر دیجیتال

۱-۳-۴. مهاجرت مجازی و دیاسپوراها دیجیتال

عصر دیجیتال مفاهیم سنتی مهاجرت و دیاسپورا را متحول کرده است. **لویت و جاورسکی (۲۰۰۷)** معتقدند که فناوری‌های نوین ارتباطات، تبادلات اقتصادی، اجتماعی و فرهنگی فراملی را تسهیل کرده‌اند و امکان ارتباطات قوی فرامرزی را بدون نیاز به جابه‌جایی فیزیکی فراهم آورده‌اند. در این راستا، پدیده‌هایی مانند مهاجرت مجازی و دیاسپورای دیجیتال^۲ به وجود آمده‌اند که به کمک

1. Alliance for Affordable Internet (A4AI)
2. Digital diaspora
3. Brinkerhoff
4. Facebook
5. Twitter
6. WhatsApp

کرده است. این تغییرات که در تفاوت‌های نسلی، شهرنشینی، و یکپارچگی جهانی فناوری مشهود است، نشان‌دهنده تأثیر عمیق فناوری دیجیتال بر ساختارهای جمعیتی و اجتماعی است. نسل‌های جوان‌تر، به دلیل آشنایی با فناوری از کودکی، تمایل بیشتری به استفاده از ابزارهای دیجیتال دارند، در حالی که نسل‌های قدیمی‌تر با چالش‌هایی مانند بی‌سوادی دیجیتال و مقاومت در برابر تغییر روبرو هستند. این شکاف دیجیتال میان نسل‌ها، به‌ویژه با افزایش شهرنشینی و دسترسی بیشتر به زیرساخت‌های فناوری در مناطق شهری، پررنگ‌تر شده است.

پرنسکی (۲۰۰۱) نسل‌های هزاره^۵ و نسل زد^۶ را به‌عنوان «بومیان دیجیتال»^۷ معرفی می‌کند، افرادی که رشد در محیط‌های دیجیتال ترجیحات آن‌ها را به سمت پلتفرم‌های نوآورانه‌ای نظیر تیک‌تاک و اینستاگرام سوق داده است. این نسل‌ها، از طریق تأکید بر خلاقیت و اصالت، صنایع مختلف را دگرگون کرده‌اند. در مقابل، ون‌دیورسن و هلسپر (۲۰۱۵) نسل‌های قدیمی‌تر را «مهاجران دیجیتال»^۸ می‌نامند که با موانعی چون بی‌سوادی دیجیتال و عدم تمایل به تغییر مواجه‌اند. برنامه‌های آموزشی بین‌نسلی و نوآوری‌هایی نظیر «پزشکی از راه دور»^۹ در کاهش این شکاف‌ها نقش مهمی ایفاء کرده‌اند و به نسل‌های قدیمی‌تر امکان دسترسی به خدمات نوین را داده‌اند که کیفیت زندگی آن‌ها را بهبود بخشیده است. روند شهرنشینی نیز به پذیرش سریع‌تر فناوری‌های دیجیتال کمک کرده است. شهرهای هوشمندی مانند سنگاپور، بارسلونا و اخیراً شهر آرکاداگ ترکمنستان نمونه‌هایی از ادغام ابزارهای دیجیتال برای بهبود زیرساخت‌ها و خدمات عمومی هستند. **بتی و همکاران^{۱۰} (۲۰۱۲)** تأکید می‌کنند که شهرنشینی فناوری‌های مبتنی بر داده را در سامانه‌های شهری ادغام کرده و محیط‌های پایدارتری ایجاد کرده است. با این حال، مناطق روستایی از دسترسی مشابه به این زیرساخت‌ها برخوردار نیستند، که این موضوع خطر افزایش شکاف دیجیتال را در این جوامع به همراه دارد.

در سطح جهانی، یکپارچگی فناوری به تسهیل همکاری‌های فرامرزی و مشارکت اقتصادی از طریق نوآوری‌هایی چون تجارت

از طریق رویدادهای مجازی و تبادل اطلاعات، سنت‌های خود را برای نسل‌های آینده نگه دارند و آن‌ها را با مخاطبان جهانی به اشتراک بگذارند. توجه ویژه به دیاسپورای دیجیتال، خصوصاً برای دولت‌هایی نظیر ایران، به‌عنوان یکی از مهاجرگسیل‌ترین کشورهای جهان، بسیار حیاتی است. همان‌طور که **حسین‌پور و همکاران^{۱۱} (۱۳۹۹)** بیان می‌دارند، اتباع ایرانی خصوصاً نخبگان ایرانی بخش قابل توجهی از جمعیت کشورهای میزبان را تشکیل می‌دهند. بنابراین ضرورت دارد دولت مبداء از طریق ابزارهای فناوری دیجیتال ارتباط با دیاسپورای خود را حفظ و ارتباط آن‌ها با سایر اتباع را تقویت نموده و در جهت توسعه کشور به‌کار برد.

با وجود فرصت‌های بی‌نظیر، مهاجرت مجازی و دیاسپوراهای دیجیتال با چالش‌هایی روبه‌رو هستند. شکاف دیجیتال یکی از مهم‌ترین موانع است؛ دسترسی محدود به زیرساخت‌های فناوری، هزینه بالای فناوری‌های مدرن، و نابرابری‌های اقتصادی مانع مشارکت کامل گروه‌های حاشیه‌نشین می‌شود (Van Dijk, 2020). همچنین، وابستگی بیش از حد به پلتفرم‌های دیجیتال، جوامع را در معرض خطراتی چون آزار سایبری^{۱۲}، نظارت دولتی^{۱۳} و استثمار اقتصادی^{۱۴} قرار می‌دهد. برای مقابله با این چالش‌ها، دولت‌ها باید سرمایه‌گذاری‌های گسترده‌ای در زیرساخت‌های ارتباطی انجام دهند، از جمله دسترسی به اینترنت پرسرعت و تجهیزات دیجیتال در مناطق محروم. همچنین، تدوین سیاست‌های حمایتی و ارتقای سوادی دیجیتال میان شهروندان ضروری است تا مشارکت فراگیر در فضای دیجیتال تضمین شود. این تحولات، نشان‌دهنده تأثیر عمیق فناوری بر مفاهیم جمعیتی و اجتماعی در سطح جهانی است و فرصت‌هایی را برای تقویت همبستگی میان جوامع پراکنده و تعامل بیشتر نیروی کار جهانی ایجاد می‌کند.

۲-۳-۴. تغییرات جمعیتی و پذیرش فناوری

پذیرش گسترده فناوری‌های دیجیتال تغییرات چشمگیری در ساختارهای جمعیتی و شیوه تعامل آن‌ها با فناوری و یکدیگر ایجاد

1. Huseynpur et al.
2. Cyberbullying
3. Surveillance
4. Exploitation
5. Millennials
6. Generation Z
7. Digital natives
8. Digital immigrants
9. Telemedicine
10. Batty et al.

محلی و جهانی، امنیت سایبری و مدیریت تهدیدات نوظهور، و مسائل اخلاقی مرتبط با توسعه و کاربرد هوش مصنوعی می‌پردازد.

۴-۱-۴. ابهام در صلاحیت قضایی

ماهیت بدون مرز فضای دیجیتال، نظام‌های حقوقی سنتی مبتنی بر حوزه‌های جغرافیایی را با چالش‌های جدی مواجه ساخته است. فعالیت‌هایی مانند تجارت الکترونیک، انتقال داده‌ها و تعاملات رسانه‌های اجتماعی که در چندین کشور به‌طور هم‌زمان رخ می‌دهند، اغلب منجر به ایجاد ابهامات قضایی پیچیده می‌شوند. در حقوق بین‌الملل، این ابهامات زمانی برجسته‌تر می‌شوند که قوانین کشورهای مختلف بر یک فعالیت واحد تأثیر می‌گذارند. برای مثال، شرکت‌های تجارت الکترونیک که کالاها یا خدمات خود را به مشتریانی در سراسر جهان عرضه می‌کنند، با مسائلی مانند تعیین صلاحیت قضایی و انتخاب قوانین قابل اجرا مواجه می‌شوند که پیچیدگی‌های حقوقی فراوانی را ایجاد می‌کند. این چالش‌ها به تفاوت‌های میان قوانین ملی و نبود چارچوب‌های بین‌المللی جامع بازمی‌گردند و ضرورت هماهنگی حقوقی را بیش از پیش آشکار می‌سازند.

در راستای رفع این چالش، اتحادیه اروپا با وضع «مقررات عمومی حفاظت از داده‌ها»^۲ تلاش کرده است هماهنگی در قوانین داده‌محور را تقویت کرده و اجرای فرامرزی این مقررات را ممکن سازد. با این حال، موفقیت این مقررات نیازمند چارچوب‌هایی جامع است که محدودیت‌های مرزهای ملی را پشت سر بگذارد. در نمونه‌ای دیگر، پرونده گوگل بر علیه اکواوستیک سولوشن^۳ تضاد میان حفاظت از حقوق مالکیت فکری و حاکمیت ملی را برجسته کرد. در این پرونده، حکم دیوان عالی مبنی بر حذف جهانی محتوای ناقص حقوق مالکیت فکری، پرسش‌هایی کلیدی درباره اجرای فرامرزی قوانین ملی و تأثیر آن بر اصول جهانی حقوقی به میان آورد. **اِزل و کوری^۴** (۲۰۱۹) بر لزوم اجماع بین‌المللی تأکید می‌کنند که می‌تواند تعادل میان حمایت از مالکیت فکری و احترام به حاکمیت ملی را فراهم آورد. همچنین، «کنوانسیون بوداپست درباره جرایم سایبری» (۲۰۰۱) گامی در جهت تقویت همکاری‌های بین‌المللی بوده است. با این وجود، محدودیت پذیرش این کنوانسیون توسط کشورهایمانند چین و هند، که ناشی از نگرانی‌های ژئوپلیتیکی است، مانعی اساسی بر

الکترونیک و آموزش مجازی کمک کرده است. با وجود این پیشرفت‌ها، جوامع حاشیه‌نشین همچنان با موانع ساختاری مانند فقر و کمبود زیرساخت‌های دیجیتال مواجه‌اند. گزارش بانک جهانی (۲۰۱۸) تأکید می‌کند که این نابرابری‌ها، به‌ویژه در مناطق کم‌درآمد، شدیدتر است. این امر ضرورت گسترش زیرساخت‌های دیجیتال و سیاست‌گذاری جامع برای تقویت عدالت دیجیتال را برجسته می‌کند. در ایران نیز، با وجود پیشرفت‌های فناوری در حوزه‌هایی مانند آموزش مجازی، دسترسی نامتوازن به اینترنت و کمبود زیرساخت‌های مناسب در مناطق روستایی و حاشیه‌ای همچنان از چالش‌های اساسی است. برنامه‌هایی نظیر «طرح توسعه ارتباطات روستایی»^۱ نشان‌دهنده تلاش‌های دولت برای کاهش این نابرابری‌هاست، اما نیاز به سیاست‌گذاری جامع‌تر و تخصیص منابع پایدار همچنان محسوس است.

۴-۴. چالش‌های حکمرانی در عصر دیجیتال

تحولات دیجیتال مرزهای جغرافیایی و اجتماعی را کم‌رنگ ساخته و مفاهیمی نظیر شهروندی دیجیتال و هویت‌های فراملی را مطرح کرده است. این دگرگونی‌ها، افزون بر فرصت‌هایی برای همکاری جهانی و گسترش شمولیت اجتماعی و اقتصادی، چالش‌هایی در حقوق و حکمرانی ایجاد کرده‌اند. در اکوسیستمی بدون مرز که تعاملات انسانی و تبادل اطلاعات در آن صورت می‌گیرد، قوانین سنتی اغلب ناکارآمد به نظر می‌رسند. نظام‌های حقوقی مبتنی بر مرزهای جغرافیایی، در مواجهه با مسائلی مانند ابهام صلاحیت قضایی، حاکمیت داده‌ها، امنیت سایبری، و حکمرانی اخلاقی بر هوش مصنوعی، کارآمدی کافی ندارند. برای نمونه، اختلافات مرتبط با جرایم سایبری، کپی‌رایت، و حریم خصوصی، به‌وضوح محدودیت‌های قوانین موجود را در برابر پیچیدگی‌های فضای دیجیتال آشکار می‌سازد. فناوری‌هایی نظیر هوش مصنوعی نیز مسائل بنیادی درباره شفافیت، عدالت، و مسئولیت‌پذیری مطرح کرده‌اند که نیازمند چارچوب‌های نوین و بین‌المللی است. به‌ویژه در موضوع حاکمیت داده‌ها، تعارض میان قوانین ملی و تقاضاهای جهانی برای تبادل آزاد داده‌ها، تدوین قوانین فراگیر را ضروری ساخته است. این مقاله به تحلیل دقیق این چالش‌ها، از جمله ابهام در صلاحیت قضایی در فضای دیجیتال، حاکمیت داده‌ها و تضادهای ناشی از قوانین

۱. سایت دولت: <https://dolat.ir/detail/452146>

2. GDPR

3. Google LLC v. Equustek Solutions Inc

4. Ezell & Cory

این اختلاف، ابطال توافقنامه «سپر حریم خصوصی اتحادیه اروپا و ایالات متحده»^۵ در سال ۲۰۲۰ بود که جریان داده‌های فراآتلانتیکی را در وضعیت مبهم حقوقی قرار داد.

قوانین محلی‌سازی داده‌ها، که ذخیره‌سازی داده‌ها در مرزهای ملی را الزامی می‌کند، نیز به پیچیدگی این چشم‌انداز افزوده است. مولر^۶ (۲۰۱۷) اشاره می‌کند که کشورهایمانند هند و روسیه با اتخاذ این رویکرد تلاش دارند نظارت خارجی را محدود کرده و اطلاعات حساس را محافظت کنند. هرچند این اقدامات به کنترل بیشتر دولت‌ها کمک می‌کند، اما هزینه‌های عملیاتی شرکت‌ها را افزایش داده، تجارت فرامرزی را محدود می‌کند و اینترنت را به اکوسیستم‌های منزوی ملی تقسیم می‌کند. این چالش‌ها بر نیاز به سیاست‌هایی تأکید دارند که میان حاکمیت داده و ماهیت فرامرزی اینترنت توازن برقرار کنند. مقررات سختگیرانه‌ای نظیر GDPR و قوانین محلی‌سازی داده‌ها، بیانگر تمایل دولت‌ها به کنترل داده‌ها هستند، اما همکاری‌های بین‌المللی و توافق‌نامه‌های چندجانبه برای حمایت از جریان آزاد اطلاعات و حفاظت از حریم خصوصی کاربران ضروری‌اند. این اقدامات می‌توانند به ایجاد چارچوب‌هایی متوازن و پایدار برای مدیریت داده‌های جهانی و تقویت حقوق و امنیت شهروندان در عصر دیجیتال منجر شوند.

۴-۳-۴. امنیت سایبری و تهدیدات علیه زیرساخت‌های دیجیتال

امنیت سایبری یکی از پیچیده‌ترین چالش‌های حقوقی و اخلاقی دوران دیجیتال به‌شمار می‌آید. وابستگی روزافزون به سامانه‌های دیجیتالی متصل، آسیب‌پذیری دولت‌ها، شرکت‌ها و افراد را در برابر حملات سایبری پیشرفته‌ای که زیرساخت‌های کلیدی را تهدید می‌کنند، افزایش داده است. لی و همکاران^۷ (۲۰۲۱) به حمله سایبری سولارویندز^۸ در ۲۰۲۰ اشاره می‌کند؛ حمله‌ای زنجیره‌ای که آژانس‌های دولتی ایالات متحده و شرکت‌های خصوصی را هدف قرار داد و ضعف چارچوب‌های موجود در مواجهه با ماهیت متغیر تهدیدات سایبری را آشکار ساخت. این حمله که گمان می‌رود از حمایت مالی دولتی برخوردار بوده است، از فرایندهای توسعه و توزیع

سر راه گسترش آن به‌عنوان یک چارچوب جهانی ایجاد کرده است. در این میان، تعارض میان قوانین محلی و عملکرد پلتفرم‌های جهانی نیز برجسته است. گیلسپی^۱ (۲۰۱۸) و برادفورد^۲ (۲۰۲۰) به مشکلاتی همچون استانداردهای متناقض در حوزه آزادی بیان و تعدیل محتوا اشاره کرده‌اند، مشکلاتی که به‌ویژه در اختلافات میان اتحادیه اروپا و ایالات متحده مشاهده می‌شود. این تناقضات اجرای مقررات ملی و ایجاد انسجام جهانی را برای پلتفرم‌ها به چالشی جدی تبدیل کرده است. در نهایت، جامعه جهانی باید توجه داشته باشد که در صورت عدم تدوین استانداردهای حقوقی هماهنگ در سطح بین‌المللی، که بتواند تعارض‌های قانونی را کاهش داده و امکان سازگاری پلتفرم‌های جهانی با مقررات ملی را فراهم کند، خطر افزایش سردرگمی حقوقی و کاهش اعتماد عمومی به سازوکارهای بین‌المللی به‌شدت افزایش خواهد یافت.

۴-۴-۲. حاکمیت بر داده‌ها و حریم خصوصی

حاکمیت داده‌ها در عصر دیجیتال، به‌عنوان مفهومی محوری مطرح شده که بر اساس آن داده‌های دیجیتال تابع قوانین کشوری است که در آن تولید یا ذخیره می‌شوند. دولت‌ها داده را به‌عنوان دارایی راهبردی مرتبط با امنیت ملی و حقوق شهروندان تلقی می‌کنند و با تدوین قوانینی مانند «مقررات عمومی حفاظت از داده‌ها»، به مدیریت آن پرداخته‌اند. وویگت و فون‌دم‌بوشه^۳ (۲۰۱۷) بیان می‌کنند که این مقررات، سازمان‌ها را ملزم به شفافیت در پردازش داده‌ها، اخذ رضایت صریح کاربران، و رعایت اصول حفاظت از داده‌ها کرده است. دامنه فراسرزمینی این قانون، شرکت‌های خارج از اتحادیه اروپا را نیز دربرمی‌گیرد، به‌گونه‌ای که شرکت‌هایی نظیر گوگل و فیس‌بوک با جریمه‌های سنگین مواجه شده‌اند. این مقررات به معیاری جهانی در حفاظت از داده‌ها تبدیل شده است، با این حال، به گفته چاندر و لی^۴ (۲۰۱۵)، مناقشاتی از جمله هزینه‌های بالای انطباق، به‌ویژه برای کسب‌وکارهای کوچک و متوسط،^۴ همچنان پابرجاست. علاوه بر این، تضاد آن با مقررات ملایم‌تر نظیر ایالات متحده، اختلافات قابل‌توجهی در انتقال بین‌المللی داده‌ها ایجاد کرده است. نمونه بارز

1. Gillespie

2. Bradford

3. Voigt & Von dem Bussche

4. Small and Midsize Enterprises (SMEs)

5. Privacy Shield

6. Mueller

7. Lee et al.

8. SolarWinds

سایبری، چارچوبی برای درک نحوه اعمال این حقوق در عملیات سایبری ارائه می‌دهد، با این حال، **اشمیت (۲۰۱۷)** بیان می‌کند که نبود الزام‌آوری و اجماع جهانی، اثرگذاری این چارچوب را محدود ساخته است. حملات باج‌افزایی نیز معضلات تازه‌ای برای اجرای قانون ایجاد کرده است. **کیشتری (۲۰۱۹)** تأکید دارد که شبکه‌های جنایی با سوءاستفاده از خلأهای حقوقی، تحقیقات را پیچیده کرده و مقابله با این حملات را دشوارتر ساخته‌اند. هرچند پروژه‌هایی نظیر «دیگر باج ندهید»^۶ که توسط یورویل^۷ ایجاد شده‌اند، ابزارهایی برای بازبایی داده‌ها فراهم کرده، اما مقیاس این جرایم همچنان از توانایی راهکارهای کنونی فراتر است و نیاز به همکاری‌های بین‌المللی را دوچندان می‌کند.

۴-۴-۴. حکمرانی اخلاقی هوش مصنوعی

هوش مصنوعی (AI) به‌عنوان یکی از فناوری‌های تحول‌آفرین، قابلیت‌های قابل‌توجهی در نوآوری، افزایش کارایی، و حل مسائل پیچیده دارد. با این حال، گسترش این فناوری، چالش‌های حقوقی و اخلاقی متعددی مانند پاسخگویی، سوگیری، و شفافیت را به همراه داشته است. **یونیکس^۸ (۲۰۱۸)** به خطاهای الگوریتم‌های تشخیص چهره در شناسایی افراد از گروه‌های اقلیت اشاره و نگرانی‌هایی درباره استفاده از این فناوری در اجرای قانون و امکان تداوم تبعیض مطرح کرده است. به‌طور مشابه، **نوبل^۹ (۲۰۱۸)** سوگیری‌های جنسیتی و نژادی در سیستم‌های استخدام خودکار را نقد و بر لزوم اصلاح این ابزارها برای تضمین عدالت تأکید کرده است. این نمونه‌ها، ضرورت تدوین چارچوب‌های حکمرانی اخلاقی برای هدایت کاربردهای هوش مصنوعی به سمت پاسخگویی، شمولیت، عدالت و انصاف را نشان می‌دهند. «قانون هوش مصنوعی اتحادیه اروپا»^{۱۰} یکی از جامع‌ترین تلاش‌ها در این راستا است. این قانون، سیستم‌های هوش مصنوعی را بر اساس سطوح ریسک دسته‌بندی کرده و برای کاربردهای پرریسک الزامات سخت‌گیرانه‌ای تعیین کرده است. اصول کلیدی این قانون شامل شفافیت، نظارت انسانی،

نرم‌افزار برای تزریق کدهای مخرب بهره‌برد و موجب دسترسی غیرمجاز به شبکه‌ها و اطلاعات حساس بدون شناسایی شد. پیچیدگی این حمله ضرورت توسعه معماری‌های امنیتی پیشرفته‌تر نظیر «معماری بدون اعتماد»^۱ را برجسته کرده است. این معماری بر اصل «هرگز اعتماد نکن، همیشه راستی‌آزمایی کن»^۲ تأکید دارد و با کنترل دقیق دسترسی، از نفوذهای پیچیده جلوگیری می‌کند. **ویلِت^۳ (۲۰۲۱)** همچنین بر اهمیت تقویت تاب‌آوری سیستم‌های دیجیتال به‌هم‌پیوسته تأکید کرده است. این حمله نشان‌دهنده شکاف‌های جدی در چارچوب‌های حقوقی و فنی موجود است و بر عدم کفایت نظام‌های فعلی در مدیریت خطرات زنجیره تأمین تأکید دارد. درواقع، حمله سولارویندز پرسش‌هایی اساسی درباره مسئولیت دولت‌ها در مقابله با این‌گونه حملات مطرح کرده است. **اشمیت^۴ (۲۰۱۷)** معتقد است که سیاست‌گذاران باید تعادلی میان حفاظت از زیرساخت‌های حیاتی و حفظ حقوق حریم خصوصی برقرار کنند. افزون بر این، این حادثه اهمیت تدوین استانداردهای امنیتی جدید برای زنجیره تأمین دیجیتال و همکاری‌های بین‌المللی را برجسته ساخته است. **ویلِت (۲۰۲۱)**، بر اهمیت اجرای راهبردهای پیش‌دستانه برای بهبود امنیت سایبری، به ویژه در برابر تهدیدات از طریق زنجیره تأمین نرم‌افزاری تأکید دارد. ویلت اشاره می‌کند که نظارت مستمر بر نرم‌افزارها و ارتقای استانداردهای امنیتی می‌تواند از حملات پیچیده‌ای مانند هک سولارویندز جلوگیری کند. این حملات نشان داده‌اند که آسیب‌پذیری‌ها در زنجیره تأمین نرم‌افزاری می‌توانند به‌طور گسترده‌ای به شبکه‌های مختلف سرایت کنند. بنابراین، اتخاذ رویکردهای پیش‌دستانه از جمله تقویت نظارت و سخت‌گیری در استانداردها، می‌تواند به کاهش ریسک سوءاستفاده از این زنجیره‌ها و کاهش آسیب‌پذیری‌های امنیتی کمک کند. با وجود تلاش‌ها برای تدوین هنجارهای بین‌المللی، فقدان توافقات الزام‌آور و نبود هم‌سویی جهانی همچنان توانایی جامعه بین‌المللی را در مقابله با تهدیدات فزاینده محدود کرده است. برای نمونه، «راهنمای تالین»^۵ در حقوق بین‌الملل مرتبط با جنگ‌های

1. Zero-Trust Architectures
2. Never Trust, Always Verify
3. Willet
4. Schmitt
5. Tallinn Manual
6. No More Ransom
7. EuroPol: The European Union Agency for Law Enforcement Cooperation
8. Eubanks
9. Noble
10. The European Union Artificial Intelligence Act

می‌دانند، اما این اقدامات می‌توانند حقوق حریم خصوصی و آزادی‌های مدنی را تضعیف کنند. سیاست‌های نظارتی دولت‌ها، اگرچه برای حفظ امنیت ملی طراحی شده‌اند، می‌توانند اعتماد عمومی را کاهش داده و فضای بیان آزادانه را محدود کنند.

گرینوالد^۴ (۲۰۱۴) با اشاره به برنامه‌های نظارتی گسترده‌ای مانند پروژه PRISM از سوی آژانس امنیت ملی ایالات متحده،^۵ بیان می‌کند که چنین برنامه‌هایی، بدون آگاهی و رضایت کاربران، داده‌های گسترده‌ای را جمع‌آوری کرده و حقوق بشر را نقض می‌کنند. این وضعیت، ضرورت ایجاد چارچوب‌هایی شفاف و پاسخگو را برجسته می‌کند که بتوانند تعادلی میان امنیت و آزادی‌های بنیادین برقرار سازند. رمزگذاری سرتاسری نیز به‌عنوان یکی از ابزارهای کلیدی در حفاظت از حریم خصوصی دیجیتال، در مرکز این بحث‌ها قرار دارد. رمزگذاری سرتاسری به کاربران اجازه می‌دهد ارتباطات خود را از دسترسی غیرمجاز محافظت کنند، اما نهادهای مجری قانون معتقدند که این فناوری توانایی آن‌ها را برای مقابله با جرایم پیچیده محدود می‌کند. آن‌ها درخواست ایجاد «درهای پشتی»^۶ در سیستم‌های رمزگذاری شده دارند، اما کارشناسان امنیت دیجیتال مانند **آپلسون و همکاران^۷ (۲۰۱۵)** هشدار می‌دهند که چنین اقداماتی امنیت کل اکوسیستم دیجیتال را به خطر می‌اندازد. زیرا این آسیب‌پذیری‌ها می‌توانند نه تنها توسط دولت‌ها، بلکه توسط بازیگران مخرب مانند هکرها، مجرمان سایبری، و حتی دولت‌های متخاصم مورد سوءاستفاده قرار گیرند. در نتیجه، چنین اقداماتی نه تنها حریم خصوصی فردی را به خطر می‌اندازد، بلکه امنیت کلی در فضای دیجیتال را نیز تضعیف می‌کند.

تعادل میان امنیت و آزادی نیازمند رویکردی است که تنها به حفاظت از حریم خصوصی محدود نشود، بلکه به پیامدهای گسترده‌تر دسته‌بندی و طبقه‌بندی داده‌ها نیز توجه کند. **دورک و مولیگان^۸ (۲۰۱۳)** استدلال می‌کنند که فرآیندهای تحلیل داده و طبقه‌بندی، نه تنها به ظاهر بی‌طرف نیستند، بلکه در بسیاری از موارد، بازتولیدکننده سوگیری‌های نهفته در داده‌ها و تصمیم‌گیری‌های انسانی هستند. آن‌ها معتقدند که شفافیت و نظارت، هرچند ابزارهای

و پاسخگویی هستند که توسعه‌دهندگان و کاربران را ملزم به ارائه اطلاعات شفاف درباره عملکرد سیستم‌ها و تضمین نظارت انسانی بر کاربردهای حساس می‌کنند.

با وجود جامعیت، برخی منتقدان معتقدند که دامنه گسترده این قانون ممکن است نوآوری را محدود کرده و هزینه‌های اجرایی سنگینی بر کسب‌وکارهای کوچک‌تر تحمیل کند. **فلوریدی و همکاران^۱ (۲۰۱۸)** تأکید دارند که اصولی مانند شفافیت و پاسخگویی می‌توانند استفاده مسئولانه از این فناوری را تسهیل کنند. قانون اتحادیه اروپا تلاشی برای ایجاد تعادل میان استفاده نوآورانه از هوش مصنوعی و مسئولیت‌پذیری اخلاقی است که هدف آن کاهش خطرات و حفظ حقوق افراد است. همچنین، **فلوریدی و همکاران^۲ (۲۰۲۰)** از اصولی نظیر قابلیت توضیح‌پذیری و حق اعتراض حمایت می‌کنند. این اصول به افراد امکان می‌دهند تصمیمات سیستم‌های هوش مصنوعی را درک کرده و در صورت لزوم به چالش بکشند، که می‌تواند اعتماد به فناوری و پاسخگویی را تقویت کند. با این حال، استفاده جهانی از هوش مصنوعی، اجرای اصول اخلاقی را دشوار کرده است. تفاوت‌های قانونی و نظارتی میان کشورها، نبود استانداردهای جهانی، و چالش‌های همکاری بین‌المللی، موانع تحقق حکمرانی اخلاقی محسوب می‌شوند. در این زمینه، همکاری‌های جهانی و تدوین استانداردهای هماهنگ برای تنظیم این فناوری ضروری است. حکمرانی اخلاقی موفق باید تعادلی میان نوآوری فناورانه و حفاظت از حقوق افراد ایجاد کند و با پیامدهای ناعادلانه مقابله نماید.

۴-۴-۵. ایجاد تعادل میان امنیت و آزادی

در عصر دیجیتال، تنش میان امنیت و آزادی‌های فردی یکی از چالش‌های محوری جوامع مدرن به شمار می‌آید. دولت‌ها که انتظار می‌رود در روند دیجیتالی‌سازی کردن در راستای تأمین حقوق و منافع شهروندان قرار دهند، «گاه به موجب گزارش‌های منطقه‌ای بین‌المللی بیشترین سوءاستفاده را در این عرصه مرتکب می‌شوند» (**معتدزآباد^۳، ۱۳۹۷، ص ۹**). دولت‌ها اغلب نظارت‌های گسترده را برای مقابله با تهدیداتی نظیر تروریسم و جرایم سایبری ضروری

1. Floridi et al. (2018)
2. Floridi et al. (2020)
3. Motamednejad (2018)
4. Greenwald
5. U.S. National Security Agency's (NSA)
6. Backdoors
7. Abelson et al.
8. Dwork & Mulligan

گیلسپی (۲۰۱۸) بیان می‌کند که پلتفرم‌هایی نظیر فیسبوک و توئیتر از ترکیبی از ابزارهای خودکار و مدیران انسانی برای مدیریت محتوا استفاده می‌کنند. ابزارهای خودکار گرچه سریع هستند، اغلب محتوای مشروع را اشتباه حذف کرده یا از شناسایی اشکال ظریف نفرت‌پراکنی بازمی‌مانند. افزون بر این، این فناوری‌ها به دلیل وابستگی به داده‌های محدود و پیش‌فرض‌های فرهنگی ممکن است ناکارآمد باشند. تفاوت‌های فرهنگی و قانونی در حوزه‌های قضایی مختلف، اجرای سیاست‌های محتوایی را دشوارتر می‌کند. آنچه در یک کشور نفرت‌پراکنی تلقی می‌شود، ممکن است در کشوری دیگر سخنی مجاز باشد و این امر چالش‌های قابل توجهی را برای پلتفرم‌های جهانی به وجود آورده است.

در اتحادیه اروپا، «قانون خدمات دیجیتال»^۱ پلتفرم‌ها را ملزم به حذف محتوای غیرقانونی و افزایش شفافیت در مدیریت محتوا می‌کند. این قانون مسئولیت‌پذیری پلتفرم‌ها را تقویت کرده و تلاش می‌کند میان امنیت کاربران و آزادی بیان تعادل ایجاد کند. در مقابل، ایالات متحده بر اساس بخش ۲۳۰ «قانون نجابت ارتباطات»^۲ پلتفرم‌ها را از مسئولیت محتوای کاربران معاف کرده و به آن‌ها آزادی قابل توجهی در مدیریت محتوا می‌دهد. این چارچوب، اگرچه نوآوری و آزادی بیان را تقویت کرده است، اما هم‌زمان به کاهش مسئولیت اجتماعی شرکت‌های فناوری نیز منجر شده است (Citron & Wittes, 2018). این تفاوت‌های قانونی، نشان‌دهنده پیچیدگی مدیریت محتوا در سطح جهانی است و بر ضرورت تدوین چارچوب‌های حقوقی هماهنگ‌تر تأکید دارد. همکاری بین‌المللی برای ایجاد استانداردهایی که حقوق بنیادین کاربران را حفظ کرده و تنوع فرهنگی را در نظر بگیرند، ضروری است.

چالش ایجاد تعادل میان مدیریت محتوا و آزادی بیان نیاز به همکاری جهانی را برجسته می‌کند. استانداردهای هماهنگ که هم‌زمان تنوع فرهنگی را در نظر بگیرند و حقوق بنیادین را حفظ کنند، برای مدیریت این مسئله پیچیده ضروری هستند. از این رو، **کلونیک^۳** (۲۰۱۸) بر اهمیت توانمندسازی کاربران تأکید دارد و بیان می‌کند که ابزارهایی نظیر گزارش‌دهی، فرآیندهای اعتراض به تصمیمات، و فیلترگذاری محتوا می‌توانند به شفافیت و اعتماد در مدیریت محتوا کمک کنند. این ابزارها با افزایش شفافیت و مشارکت کاربران، به ایجاد حس اعتماد در تعاملات آنلاین کمک می‌کنند. برای مواجهه

مهمی در کاهش اثرات منفی این سیستم‌ها هستند، اما به‌تنهایی کافی نیستند و نمی‌توانند از ایجاد نابرابری‌ها و تبعیض‌های ناشی از داده‌های بزرگ جلوگیری کنند. از این رو، آن‌ها پیشنهاد می‌کنند که علاوه بر شفاف‌سازی الگوریتم‌ها، باید مدل‌هایی برای ارزیابی و کاهش سوگیری‌های نهادینه‌شده در سیستم‌های داده‌محور توسعه یابد. همچنین، آن‌ها بر این نکته تأکید دارند که اتکا به راهکارهای سنتی حفظ حریم خصوصی، مانند شفافیت و کنترل فردی بر داده‌ها، نمی‌تواند به‌تنهایی چالش‌های مرتبط با عدالت و عدم تبعیض در سیستم‌های مبتنی بر داده‌های کلان را حل کند. در واقع، می‌توان استنتاج نمود که برای ایجاد تعادل میان امنیت، آزادی و عدالت، باید داده‌ها و سیستم‌های تصمیم‌گیری به‌گونه‌ای طراحی شوند که اثرات اجتماعی و اخلاقی آن‌ها نیز مورد بررسی و تنظیم قرار گیرد. برای رسیدن به این هدف، ایجاد مکانیسم‌های نظارتی مستقل و شفافیت در عملکرد نهادهای امنیتی اهمیت دارد. این سازوکارها تضمین می‌کنند که اقدامات امنیتی، علاوه بر محافظت از جامعه در برابر تهدیدها، به حقوق و آزادی‌های کاربران احترام بگذارند. همچنین الزامات شفافیت برای سازمان‌های دولتی و خصوصی می‌تواند به آگاهی بیشتر کاربران درباره نحوه استفاده از داده‌های آن‌ها کمک کند. ترکیب فناوری‌های پیشرفته، همراه با نظارت شفاف و پاسخ‌گویی، تضمین می‌کند که اقدامات امنیتی، علاوه بر حفاظت از جامعه در برابر تهدیدها، حقوق و آزادی‌های اساسی کاربران را نیز محترم بشمارند. این رویکرد می‌تواند راه‌حلی برای چالش‌های پیچیده‌ای باشد که میان امنیت و آزادی در عصر دیجیتال وجود دارد.

۴-۴-۶. مدیریت محتوا و آزادی بیان

مدیریت محتوا در پلتفرم‌های دیجیتال یکی از مسائل پیچیده عصر دیجیتال است. شرکت‌های شبکه‌های اجتماعی وظیفه دارند محتوای مضر نظیر نفرت‌پراکنی و اطلاعات نادرست را حذف کنند، در عین حال آزادی بیان را نیز حفظ کنند. با این حال، سیاست‌های ناهماهنگ مدیریت محتوا و استفاده از الگوریتم‌های خودکار باعث اتهاماتی نظیر سانسور و سوگیری شده است. این چالش‌ها نشان‌دهنده تضاد ذاتی میان حفاظت از آزادی بیان و نیاز به کنترل محتوای مخرب هستند، که مدیریت آن نیازمند رویکردهای چندجانبه است.

1. Services Act (DSA) (European Parliament & Council, 2022)
2. Section 230 of the Communications Decency Act
3. Klönick

مخابرات^۱ (۲۰۲۴) حدود ۳۰ درصد از جمعیت روستایی در کشورهای کم‌درآمد و در حال توسعه هنوز به اینترنت دسترسی ندارند، که این آمار بیانگر نابرابری شدید در زیرساخت‌های دیجیتال است. در این زمینه، پروژه‌هایی نظیر بال‌های گوگل لون^۲ و ماهواره‌های مدار پایین استارلینک^۳، راه‌حل‌های نوآورانه و امیدوارکننده‌ای برای اتصال مناطق دورافتاده ارائه کرده‌اند و افق‌های جدیدی را برای کاهش شکاف دیجیتال گشوده‌اند.

هزینه‌های بالای اینترنت نیز مانعی برای گروه‌های کم‌درآمد محسوب می‌شود. طرح‌هایی مانند «هند دیجیتال» با یارانه‌ها و ارائه اینترنت عمومی، نرخ نفوذ اینترنت را افزایش می‌دهند. با اتخاذ چنین رویکردهایی، دولت‌ها می‌توانند عدالت دیجیتال را ارتقاء دهند. علاوه بر این، سواد دیجیتال شهروندان اهمیت حیاتی دارد. توانایی استفاده مؤثر از فناوری و درک ایمنی آنلاین، مشارکت معنادار در جهان دیجیتال را تضمین می‌کند. به‌ویژه، گنجاندن سواد دیجیتال در برنامه‌های درسی و ارائه آموزش‌های هدفمند برای گروه‌های حاشیه‌نشین، مانند زنان، سالمندان و افراد دارای معلولیت، از اقدامات کلیدی در این زمینه است. **یونسکو^۴ (۲۰۱۸، ۲۰۲۱)** در چارچوب سواد دیجیتال خود بر راهبردهای متناسب فرهنگی و نسلی تأکید دارد. ارتقای طراحی فراگیر برای دسترسی همگانی، به‌ویژه برای افراد دارای معلولیت، ضروری است. **مایکروسافت^۵ (۲۰۲۰)** در برنامه «هوش مصنوعی برای دسترسی»^۶ از فناوری‌هایی نظیر صفحه‌خوان‌ها و نرم‌افزارهای تشخیص صدا استفاده می‌کند تا مشارکت گسترده‌تر را ممکن سازد. اگرچه این ابتکارات نویدبخش هستند، کاهش شکاف دیجیتال نیازمند هماهنگی پایدار میان دولت‌ها، بخش خصوصی و نهادهای بین‌المللی است. پیشنهادات موجود بر همکاری جامع و رویکردی چندبعدی تأکید دارند تا اکوسیستم دیجیتالی فراگیر و معنادار ایجاد شود. این هدف را می‌توان از طریق اقداماتی همچون اولویت‌بندی نیازهای فناوری مناطق، فراهم‌سازی بسترهای فرهنگی و اجتماعی موردنیاز برای بهره‌گیری از فناوری اطلاعات و ارتباطات، تدوین برنامه‌های جامع که آموزش استفاده از سخت‌افزارها و نرم‌افزارها، آموزش اصول اخلاقی، و راهبردهای دیگر را شامل

با این چالش، ایجاد چارچوب‌هایی ضروری است که حقوق کاربران را در اولویت قرار داده و در عین حال از سوءاستفاده‌های احتمالی جلوگیری کنند. این رویکرد می‌تواند به تقویت اعتماد عمومی و ایجاد فضای دیجیتالی سالم‌تر منجر شود.

۵. راهکارها و توصیه‌ها برای آینده دیجیتال

تحولات سریع در عصر دیجیتال چالش‌ها و فرصت‌های متعددی را برای جوامع انسانی به همراه داشته است. از نابرابری در دسترسی به فناوری گرفته تا ضرورت تنظیم چارچوب‌های حکمرانی و ارتقای شهروندی دیجیتال اخلاق‌محور، جوامع امروز به دنبال یافتن راهکارهایی برای کاهش شکاف‌های موجود و دستیابی به پایداری و شمول دیجیتال هستند. در این مسیر، سیاست‌گذاری‌های جامع، نوآوری‌های فناورانه، و همکاری‌های بین‌المللی از اهمیت ویژه‌ای برخوردارند. هدف نهایی، ایجاد اکوسیستمی دیجیتال است که با تأکید بر عدالت، مسئولیت‌پذیری، و شمول‌پذیری، پیشرفت برابر برای همگان را ممکن سازد. در همین راستا، این بخش به بررسی و ارائه راهکارهایی برای کاهش شکاف دیجیتال، تقویت همکاری‌های جهانی، انطباق چارچوب‌های حکمرانی با فناوری‌های نوظهور، و ترویج شهروندی دیجیتال اخلاق‌محور می‌پردازد.

۵-۱. کاهش شکاف دیجیتال

شکاف دیجیتال میان جوامع مختلف یکی از چالش‌های اساسی در دوران دیجیتال است و ناشی از دسترسی نابرابر به فناوری اطلاعات و ارتباطات می‌باشد. این شکاف مانعی جدی برای دستیابی به شهروندی دیجیتال برابر است و میلیون‌ها نفر را از فرصت‌های اقتصادی، آموزشی و اجتماعی عصر دیجیتال محروم کرده است. رفع این چالش مستلزم سرمایه‌گذاری در زیرساخت‌ها، تسهیل دسترسی مالی، و گسترش برنامه‌های سواد دیجیتال است. دسترسی پایدار به اینترنت پرسرعت، پیش‌شرطی برای شمول دیجیتال محسوب می‌شود، اما همچنان مناطق روستایی و کم‌برخوردار دچار کمبودهای اساسی هستند. براساس گزارش اتحادیه بین‌المللی

1. The International Telecommunication Union (ITU)
2. Google's Loon
3. Starlink
4. UNESCO (2018)
5. Global Media and Information Literacy Assessment Framework: Country Readiness and Competencies, UNESCO (2021)
6. Microsoft (2020)
7. Empowering People with Disabilities Through AI

دیجیتال و امنیت سایبری فراهم کرده است. هرچند غیرالزام‌آور، این مجمع با ایجاد اجماع و تدوین بهترین رویه‌ها، به حکمرانی دیجیتال کمک می‌کند (DeNardis, 2014). افزایش نمایندگی عادلانه، به‌ویژه از سوی کشورهای در حال توسعه، می‌تواند به وارد کردن دیدگاه‌های متنوع به این گفت‌وگوها کمک کرده و حکمرانی جهانی را تقویت نماید.

جرایم سایبری نیز تهدیدی جدی برای امنیت جهانی محسوب می‌شوند. همکاری بین‌المللی، از جمله از طریق سازمان‌هایی نظیر یورپول و اینترپل، برای مقابله مؤثر با این تهدیدها حیاتی است. پروژه‌هایی نظیر «دیگر باج ندهید»^۲ توسط یورپول منابعی برای قربانیان حملات باج‌افزایی ارائه کرده‌اند تا بدون پرداخت باج، اطلاعات خود را بازیابی کنند (Kshetri, 2019). به عنوان مثال، مجمع جهانی تخصص‌های سایبری،^۳ آموزش و تبادل دانش در زمینه‌هایی مانند واکنش به حوادث و حفاظت از زیرساخت‌های حیاتی را ترویج می‌دهد (GFCE, 2020). همچنین، اقدامات پیشگیرانه نظیر ظرفیت‌سازی و تبادل اطلاعات می‌تواند توانایی کشورها را در پیشگیری از تهدیدات افزایش دهد. با این حال، تنش‌های ژئوپلیتیک مانند تضاد میان رویکرد دولتی چین و رویکرد بازارمحور ایالات متحده، مانع اجماع جهانی می‌شود (Mueller, 2017). ابتکاراتی مانند «فراخوان پاریس برای اعتماد و امنیت در فضای سایبری»^۴ اصولی برای رفتار مسئولانه دولت‌ها ارائه می‌دهند و همکاری میان ذینفعان را تسهیل می‌کنند (Microsoft, 2020). در مجموع، هماهنگی چارچوب‌های قانونی، تقویت مدل‌های حکمرانی فراگیر، و اجرای اقدامات پیشگیرانه، عناصر کلیدی حکمرانی جهانی مؤثر در عصر دیجیتال هستند. موفقیت در این مسیر مستلزم تعهد مستمر، اعتماد متقابل، و اولویت‌بخشی به منافع جمعی است.

۳-۵. تطبیق چارچوب‌های حکمرانی

پیشرفت‌های سریع فناوری، نقایص مدل‌های سنتی حکمرانی را آشکارتر ساخته و ضرورت رویکردهای نوآورانه برای حکمرانی در عصر دیجیتال را برجسته کرده است. سیستم‌های متمرکز غالباً در مواجهه با چالش‌های اکوسیستم جهانی ناکارآمدند، امری که نیاز به غیرمتمرکزسازی، رویکردهای تطبیقی، و سیاست‌گذاری فراگیر را

می‌شوند، محقق ساخت (کاظم پوریان و عبدلی، ۱۳۹۵). این اقدامات، در کنار نظارت مداوم و ارزیابی تأثیرات، می‌توانند راه را برای کاهش شکاف دیجیتال و تحقق عدالت دیجیتال هموار سازند.

۲-۵. تقویت همکاری‌های بین‌المللی

در دنیای به‌هم‌پیوسته دیجیتال، همکاری‌های بین‌المللی برای مقابله با چالش‌هایی همچون جرایم سایبری، حفاظت از داده‌ها، و حکمرانی ضروری است. با این حال، تعارض قوانین ملی، منافع متضاد، و تنش‌های ژئوپلیتیک این تلاش‌ها را پیچیده‌تر می‌کنند و موانع جدی در مسیر دستیابی به هماهنگی جهانی ایجاد می‌نمایند. هماهنگ‌سازی چارچوب‌های قانونی، نخستین گام در این مسیر است. پراکنندگی مقررات امنیت سایبری و حفاظت از داده‌ها، اجرای قوانین را در پرونده‌های فرامرزی دشوار کرده است. معاهداتی مانند کنوانسیون بوداپست درباره جرایم سایبری (کنوانسیون بوداپست، ۲۰۰۱)، الگوی مناسبی برای تبادل اطلاعات و هماهنگی اقدامات فراهم می‌کنند، اما پذیرش محدود آن، به‌ویژه از سوی کشورهای تأثیرگذاری مانند چین، هند، و روسیه، نیاز به تدوین توافقات جامع‌تر و فراگیرتر را بیش از پیش نمایان می‌سازد.

سازگاری رژیم‌های حفاظت از داده‌ها نیز به همان اندازه حیاتی است. مقررات عمومی حفاظت از داده‌های اتحادیه اروپا (GDPR)، به‌عنوان استاندارد جهانی، حقوق فردی را با سخت‌گیری حفظ می‌کند. این استاندارد، هرچند پیشرو، دامنه فراسرزمینی گسترده‌ای دارد که باعث ایجاد تنش‌هایی با کشورهایمانند ایالات متحده شده است، جایی که قوانین حفاظت از داده‌ها کمتر محدودکننده هستند. لغو توافق سپر امنیتی اتحادیه اروپا و ایالات متحده^۱ در سال ۲۰۲۰ نشان‌دهنده پیچیدگی ایجاد تعادل میان نظام‌های حقوقی متفاوت و تضمین امنیت داده‌هاست (Chander & Le, 2015). این چالش‌ها بر ضرورت اتخاذ رویکردهای جامع‌نگر و انعطاف‌پذیر برای انتقال امن داده‌های فرامرزی تأکید می‌کنند.

مدل‌های حکمرانی چندذینفعی، راه‌حلی فراگیر ارائه می‌دهند و ذینفعان مختلف نظیر دولت‌ها، شرکت‌ها، و جامعه مدنی را در سیاست‌گذاری دخیل می‌کنند. مجمع حکمرانی اینترنت سازمان ملل بستر مهمی برای بحث درباره موضوعاتی مانند شمول

1. EU-U.S. Privacy Shield

2. No More Ransom

3. The Global Forum on Cyber Expertise (GFCE)

4. The Paris Call on Trust and Security in Cyberspace

مصنوعی،^۴ می‌تواند با گردآوری دیدگاه‌های متنوع از سوی دولت‌ها، بخش خصوصی، و جامعه مدنی، به افزایش مشروعیت و اعتماد عمومی کمک کند (Floridi et al., 2018). در نتیجه، انطباق حکمرانی دیجیتال مستلزم استفاده از فناوری‌های پیشرفته، چارچوب‌های تنظیمی نوآورانه، و همکاری گسترده میان ذینفعان در سطوح ملی و بین‌المللی است.

۴-۵. ترویج شهروندی دیجیتال اخلاق‌مدار

شهروندی دیجیتال اخلاق‌محور زیربنای جامعه‌ای دیجیتال، پایدار و فراگیر است. با ادغام فناوری‌های دیجیتال در زندگی روزمره، پرورش ارزش‌هایی مانند مسئولیت‌پذیری، عدالت، و احترام در فضای آنلاین به یکی از ضرورت‌های عصر دیجیتال تبدیل شده است. دستیابی به این هدف مستلزم رویکردی جامع است که آموزش، شمول‌پذیری، و مشارکت اجتماعی را در بر گیرد.

آموزش نقشی محوری در تقویت شهروندی دیجیتال اخلاق‌محور ایفاء می‌کند. چارچوب سواد رسانه‌ای و اطلاعاتی یونسکو، با ادغام تفکر انتقادی و تعامل اخلاقی، فراگیران را برای مواجهه آگاهانه با پیچیدگی‌های دنیای دیجیتال آماده می‌کند (یونسکو، ۲۰۲۱).^۵ این چارچوب بر مهارت‌هایی چون ارزیابی اطلاعات، آگاهی از پیامدهای اخلاقی رفتارهای آنلاین، و تصمیم‌گیری مسئولانه تأکید دارد. علاوه بر این، مباحث مهمی مانند حریم خصوصی داده‌ها و حقوق مالکیت فکری به دانش‌آموزان کمک می‌کنند تا پیامدهای اجتماعی و اخلاقی رفتارهای خود را بهتر درک کنند. به‌طور مثال، کمپین‌هایی مانند «روز اینترنت امن‌تر» کمیسیون اروپا،^۶ با تأکید بر صحت اطلاعات و احترام به مرزهای آنلاین، مسئولیت‌پذیری دیجیتال را میان کاربران ترویج می‌دهند (کمیسیون اروپا، ۲۰۲۰).^۷ شمول‌پذیری و تنوع اصول بنیادین شهروندی دیجیتال اخلاق‌مدار محسوب می‌شوند. رفع نابرابری‌ها، به‌ویژه تفاوت ۲۰ درصدی در استفاده از اینترنت موبایلی میان زنان و مردان در کشورهای با درآمد متوسط و پایین، نیازمند اقدامات هدفمند است (GSMA, 2020).^۷ از جمله این اقدامات می‌توان به یارانه برای خانوارهای زن‌سرپرست و ایجاد فضاهای امن آنلاین اشاره کرد. طراحی فراگیر نیز نقش

بیشتر برجسته می‌سازد.

یکی از ابزارهای کلیدی در این زمینه، فناوری بلاکچین است که برای حل مسائل مرتبط با مدیریت هویت دیجیتال، تراکنش‌های امن، و شفافیت داده‌ها مورد توجه قرار گرفته است. برنامه اقامت الکترونیکی استونی، نمونه‌ای موفق از کاربرد این فناوری در ارائه خدمات دولتی امن به شمار می‌رود. همچنین، سیستم‌های رأی‌گیری مبتنی بر بلاکچین امکان برگزاری انتخابات شفاف و مطمئن را فراهم می‌کنند. تاپسکات و تاپسکات (۲۰۱۸) ظرفیت این فناوری برای تضمین یکپارچگی انتخابات را برجسته کرده‌اند. پروژه‌های رأی‌گیری بلاکچینی در سوئیس و ویرجینیای غربی نمونه‌هایی عملی از این قابلیت هستند، هرچند چالش‌هایی نظیر مقیاس‌پذیری، پیچیدگی فنی، و مصرف انرژی همچنان باقی مانده‌اند.

مدل‌های نوآورانه نظارتی، همچون آزمایشگاه‌های تنظیمی^۱ سازمان پولی سنگاپور^۲ در بخش فین‌تک، بستر مناسبی برای آزمون فناوری‌های نوظهور در محیط‌های کنترل‌شده و نظارت شده فراهم کرده‌اند (MAS, 2020). این مدل می‌تواند به حوزه‌هایی نظیر هوش مصنوعی، امنیت سایبری و حریم خصوصی گسترش یابد و با تطبیق تدریجی مقررات، هم‌راستایی آن‌ها با ارزش‌های اخلاقی و اجتماعی را تضمین کند. در همین راستا، پاسخگویی پلتفرم‌ها، به‌ویژه در مورد الگوریتم‌های گوگل، فیسبوک و توئیتر، برای رفع نگرانی‌های مرتبط با سوگیری، اطلاعات نادرست و قطب‌بندی اجتماعی ضروری است. چارچوب‌های نظارتی نظیر قانون خدمات دیجیتال اتحادیه اروپا^۳ (DSA) الزاماتی چون شفافیت در تعدیل محتوا و انجام ممیزی مستقل را به اجرا درآورده‌اند (Bradford, 2020). افزون بر این، اقدامات داخلی پلتفرم‌ها مانند هیئت نظارت فیسبوک (Klonick, 2018). به‌عنوان مکانیزمی برای نظارت بر تصمیمات مناقشه‌برانگیز، مورد توجه قرار گرفته‌اند. این ابزارها می‌توانند در راستای تقویت پاسخگویی و اعتماد عمومی نقش بسزایی ایفاء کنند. برای همگام‌سازی مقررات با تحولات سریع فناوری، رویکردهای تطبیقی و چابک ضروری هستند. سیاست‌گذاری فراگیر، همراه با همکاری بین‌بخشی، در قالب ابتکاراتی نظیر مشارکت در هوش

1. Regulatory Sandboxes

2. The Monetary Authority of Singapore (MAS)

3. European Union's Digital Services Act (DSA)

4. Partnership on AI

5. UNESCO (2021, 2023)

6. European Commission

۷. گزارش «شکاف جنسیتی در استفاده از موبایل ۲۰۲۰» (The Mobile Gender Gap Report 2020) منتشرشده توسط انجمن سیستم جهانی برای ارتباطات موبایل برگرفته از: https://www.gsma.com/r/gender-gap-2020/?utm_source=chatgpt.com

را منعکس کرده و به جوامع این امکان را می‌دهند که ضمن تعامل جهانی، هویت‌های بومی و فرهنگی خود را حفظ کنند. با این وجود، نابرابری در دسترسی به زیرساخت‌ها، آموزش و منابع دیجیتال، بخش‌هایی از جامعه را از این فرصت‌ها محروم کرده است و این واقعیت، ضرورت تلاش برای کاهش شکاف دیجیتال و فراهم‌سازی فرصت‌های برابر را آشکارتر می‌سازد.

سرعت تحول فناوری‌های دیجیتال، چارچوب‌های حکمرانی سنتی را با چالش‌های جدی روبه‌رو کرده و کاستی‌های آنها در مسائلی مانند حاکمیت داده‌ها، ابهام‌های قضایی، و امنیت سایبری را نمایان کرده است. برای مثال، برنامه اقامت الکترونیکی استونی با تکیه بر فناوری بلاک‌چین، ظرفیت‌های تحول‌آفرین هویت دیجیتال را به نمایش گذاشته، اما همزمان نگرانی‌هایی در مورد امنیت سایبری و مسائل حقوقی ایجاد کرده است. همچنین، سیستم آدهار هند با ارائه پایگاه داده بیومتریک گسترده، شمول مالی و کارآمدی خدمات عمومی را تسهیل کرده، اما نگرانی‌هایی در خصوص نقض حریم خصوصی و حذف گروه‌های آسیب‌پذیر به همراه داشته است. افزون بر این، حملاتی سایبری نظیر سولارویندز، آسیب‌پذیری سیستم‌های دیجیتال را نشان داده و بر نیاز به همکاری بین‌المللی برای تقویت امنیت زنجیره تأمین دیجیتال تأکید کرده است. این نمونه‌ها، بر ضرورت طراحی چارچوب‌های حکمرانی حقوقی شفاف، پاسخگو، و منطبق با اصول حقوق بشر تأکید دارند.

رفع شکاف دیجیتال، به‌ویژه در مناطق کمتر توسعه‌یافته، پیش‌شرط دستیابی به شهروندی دیجیتال فراگیر و عادلانه است. این هدف نیازمند سرمایه‌گذاری‌های پایدار در زیرساخت‌های فناوری و ارائه راهکارهایی نوآورانه برای بهبود دسترسی به فناوری‌های دیجیتال است. طرح‌هایی مانند دیجیتال و پروژه استارلینک، با گسترش دسترسی به اینترنت، می‌توانند تأثیر بسزایی در کاهش شکاف دیجیتال داشته باشند. علاوه بر این، ارتقاء سواد دیجیتال از طریق آموزش مهارت‌های آنلاین و برنامه‌های آگاهی‌بخشی عمومی نقشی کلیدی در این راستا ایفا می‌کند. طراحی فراگیر نیز با تضمین مشارکت برابر افراد دارای معلولیت، اهمیت بسیاری دارد. به‌علاوه، برنامه‌هایی نظیر «هوش مصنوعی برای دسترسی» مایکروسافت، قابلیت فناوری در توانمندسازی گروه‌های حاشیه‌نشین و تقویت شمول‌پذیری اجتماعی را به نمایش گذاشته‌اند. پرورش رفتار مسئولانه در فضای آنلاین از طریق آموزش و

مهمی در مشارکت افراد دارای معلولیت ایفا می‌کند. ابزارهایی نظیر صفحه‌خوان‌ها و فناوری‌های جایگزین، مشارکت این گروه‌ها را تضمین می‌کنند. ابتکاراتی مانند «هوش مصنوعی برای دسترسی» مایکروسافت نشان‌دهنده قدرت فناوری در توانمندسازی جوامع حاشیه‌نشین و کم‌برخوردار است (Microsoft, 2021).

مشارکت اجتماعی نیز با تقویت اعتماد و پاسخگویی در محیط‌های دیجیتال، نقش مهمی در توسعه شهروندی اخلاق‌مدار دارد. مدل‌های حکمرانی مشارکتی، مانند اتکای ردیت به ناظران داوطلب، کاربران را در تدوین استانداردها و سیاست‌های محتوا دخیل می‌کنند (Ostrom, 1990). علاوه بر این، ابزارهایی چون فیلترهای محتوای قابل تنظیم و مکانیزم‌های گزارش‌دهی، تاب‌آوری دیجیتال را افزایش داده و به مقابله با قلدری سایبری و اطلاعات نادرست کمک می‌کنند. ابتکاراتی مانند «حقوق مدنی سایبری»^۱ نیز منابع حمایتی برای قربانیان سوءاستفاده آنلاین ارائه کرده و حضور دیجیتالی آن‌ها را بازسازی می‌کنند (۲۰۲۱). ترویج مشارکت مثبت در جوامع آنلاین یکی دیگر از ابعاد مهم شهروندی دیجیتال اخلاق‌مدار است. پلتفرم‌ها می‌توانند با شناسایی و پاداش دادن به کاربران سازنده، رفتارهای مثبت را تقویت کنند. به‌عنوان نمونه، جوایز خالق یوتیوب با قدردانی از تولیدکنندگان محتوای آموزنده و انگیزشی، به ایجاد فرهنگی مثبت و سازنده در فضای دیجیتال کمک کرده است. ادغام چارچوب‌های حکمرانی تطبیقی با ترویج شهروندی دیجیتال اخلاق‌محور می‌تواند تضمین کند که جوامع در اکوسیستم دیجیتال به‌طور مسئولانه و عادلانه پیشرفت کنند. پذیرش فناوری‌های غیرمتمرکز، ارتقای شمول‌پذیری، و تقویت مسئولیت‌پذیری، پایه‌ای برای ساخت آینده‌ای پایدار و نوآورانه خواهد بود.

۶. بحث و نتیجه‌گیری

عصر دیجیتال با ایجاد تغییرات گسترده در مفاهیم شهروندی و حکمرانی، دریچه‌های جدیدی از مشارکت، نوآوری و ارتباطات فراملی را گشوده است. فناوری‌های دیجیتال امکان تعاملات فراتر از مرزهای جغرافیایی را فراهم آورده و شهروندی دیجیتال را به نماد قابلیت‌های ارتباطی این دوران تبدیل کرده‌اند. این پیشرفت‌ها، علاوه بر تسهیل گفت‌وگوهای فراملی و تقویت فرصت‌های اقتصادی، نقشی کلیدی در حفظ و بازآفرینی هویت‌های فرهنگی ایفاء کرده‌اند. پدیده‌هایی مانند مهاجرت مجازی و دیاسپوراها دیجیتال ماهیت پویای هویت

یزدانی بروجنی، فرشید (۱۳۸۴). نگاهی به جهانی شدن و نابرابری با تأکید بر ایران. رفاه اجتماعی، ۵(۱۸)، ۲۰۱-۲۲۲. http://refahj.uswr.ac.ir/index.php?slc_lang=fa&sid=1

Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., ... Schneier, B. (2015). *Keys under doormats: Mandating insecurity by requiring government access to all data and communications*. Retrieved from <https://doi.org/10.1093/cybsec/tyv009>

Alliance for Affordable Internet. (2021). *The affordability report 2021*. <https://a4ai.org>

Batty, M., Axhausen, K. W., Giannotti, F., Pozdnoukhov, A., Bazzani, A., Wachowicz, M., ... & Portugali, Y. (2012). Smart cities of the future. *European Physical Journal Special Topics*, 214(1), 481-518. <https://doi.org/10.1140/epjst/e2012-01703-3>

Baym, N. K. (2015). *Personal connections in the digital age* (2nd ed.). Polity Press.

Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Oxford University Press.

Brinkerhoff, J. M. (2009). *Digital diasporas: Identity and transnational engagement*. Cambridge University Press.

Brubaker, R. (1992). *Citizenship and nationhood in France and Germany*. Harvard University Press.

Castles, S., & Davidson, A. (2000). *Citizenship and migration: Globalization and the politics of belonging*. Routledge.

Chander, A. (2013). *The electronic silk road: How the web binds the world in commerce*. Yale University Press.

Chander, A., & Le, U. P. (2015). Data nationalism. *Emory Law Journal*, 64(3), 677-739. URL: <https://scholarlycommons.law.emory.edu/elj/vol64/iss3/2/>

Citron, D. K., & Wittes, B. (2018). The Problem Isn't Just Backpage: Revising Section 230 Immunity. *Georgetown Law Technology Review*, 2(2), 453-473. <https://georgetownlawtechreview.org/the-problem-isnt-just-backpage-revising-section-230-immunity/GLTR-07-2018/>

Council of Europe. (2001). *Convention on Cybercrime*. Budapest: Council of Europe. <https://www.coe.int/en/web/cybercrime>

Cyber Civil Rights Initiative (CCRI). (2021). *Resources for victims of online abuse*. <https://www.cybercivilrights.org>

Dehghani Firozabadi, J., & Chehrzad, S. (2023). Artificial intelligence and the problematization of national security topics. *Political Strategic Studies*, 12(46), 207-242. <https://doi.org/10.22054/QPSS.2022.70690.3130>

DeNardis, L. (2014). *The global war for internet governance*. Yale University Press.

کمپین‌های عمومی مانند روز اینترنت امن‌تر، به تقویت شهروندی دیجیتال اخلاق‌مدار کمک می‌کند. چارچوب‌هایی نظیر سواد رسانه‌ای و اطلاعاتی یونسکو، با تأکید بر تفکر انتقادی و مسئولیت‌پذیری در تعاملات دیجیتال، بستری برای ارتقاء آگاهی کاربران ایجاد می‌کنند. نگاه به آینده نشان می‌دهد که دستیابی به عدالت دیجیتال تنها از طریق همکاری گسترده میان دولت‌ها، بخش خصوصی، و جامعه مدنی ممکن است. سرمایه‌گذاری در زیرساخت‌های پایدار، اولویت‌بندی شفافیت و اخلاق‌مداری توسط شرکت‌ها و تقویت صدای جوامع حاشیه‌نشین، اقداماتی حیاتی برای این منظور هستند. در نهایت، اگرچه فناوری دیجیتال چالش‌هایی را به همراه دارد، اما با تمرکز بر همکاری، پاسخگویی، و بهره‌گیری از ظرفیت‌های جمعی، می‌توان از این فناوری برای ایجاد جامعه‌ای عادلانه‌تر و پیشرفته‌تر بهره برد.

منابع

حسین‌پور، بابک، حسین صادق‌اوغلی و افسر روحی (۱۳۹۹). مهاجرت و موتیونیا: نقش بهزیستی و بهخواستی در تمایل زبان‌آموزان به مهاجرت از کشور. *مطالعات جمعیتی*، ۶(۲)، ۱۴۷-۱۸۱. <https://doi.org/10.22034/jips.2021.254325.1085>

خلیلی، محسن (۱۳۹۴). کشاکش دولت الکترونیک با دموکراسی الکترونیک. *دولت پژوهی*، ۱۱(۳)، ۱-۳۲. <https://doi.org/10.22054/tssq.2016.2451>

دهقانی فیروزآبادی، سید جلال و سعید چهارآزاد (۱۴۰۲). هوش مصنوعی و مسئله‌دار کردن درون‌مایه‌های امنیت ملی. *پژوهش‌های راهبردی سیاست*، ۱۲(۴۶)، ۲۰۷-۲۴۲. <https://doi.org/10.22054/QPSS.2022.70690.3130>

شهریاری، حیدر و سجاد رهبر (۱۴۰۲). شهروند دیجیتال و مناسبات آن با دولت در عصر دیجیتال: با نگاهی به مصداق‌های عینی. *رهیافت‌های سیاسی و بین‌المللی*، ۱۴(۴)، ۲۲۹-۲۵۳. <https://doi.org/10.48308/piaj.2023.229679.1317>

کاظم پوریان، سعید و سمانه عبدلی (۱۳۹۵). سواد دیجیتال: راهکاری برای پوشش شکاف دیجیتال و پرورش شهروند دیجیتال. *سیاست‌نامه علم و فناوری*، ۶(۴)، ۵۳-۶۴. https://stpl.ristip.sharif.ir/article_4480.html?lang=en

معمدنژاد، رویا (۱۳۹۷). وظایف دولت‌ها در عرصه تکنولوژی‌های دیجیتال: از دولت انحصارطلب تا دولت رگولاتور. *علوم خبری*، ۷(۴)، ۳۶-۹. https://www.mjourcom.ir/article_114311.html

- University Press.
- International Telecommunication Union. (2024). *Measuring digital development: Facts and figures 2024*. https://www.itu.int/hub/publication/D-IND-ICT_MDD-2024-4/
- Isin, E. F. (2002). *Being political: Genealogies of citizenship*. University of Minnesota Press.
- Kazem Pourian, S., & Abdoli, S. (2017). Digital literacy: A solution for covering the digital divide and training digital citizens. *Science and Technology Policy Letters*, 6(4), 53-64. [In Persian] URL: https://stpl.ristip.sharif.ir/article_4480.html?lang=en
- Kerr, I. (2019). *The legal and ethical challenges of artificial intelligence*. Cambridge University Press.
- Klonick, K. (2018). The new governors: The people, rules, and processes governing online speech. *Harvard Law Review*, 131(6), 1598-1670. URL: <https://harvardlawreview.org/print/vol-131/the-new-governors-the-people-rules-and-processes-governing-online-speech/>
- Kotka, T., Vargas, C., & Korjus, K. (2015). Estonian e-Residency: Redefining the nation-state in the digital era. *University of Oxford Cyber Studies Programme working paper*, 3. URL: <https://www.ctga.ox.ac.uk/article/estonian-e-residency-redefining-nation-state-digital-era>
- Kshetri, N. (2019). *The global cybercrime industry: Economic, institutional, and strategic perspectives*. Springer.
- Lee, R. D., Mancusi, M. A., Hay, A. A., & Raglani, A. (2021). Lessons learned from the SolarWinds cyberattack, and the future for the New York Department of Financial Services' cybersecurity regulation. Arnold & Porter.
- Livingstone, S. (2004). Media literacy and the challenge of new information and communication technologies. *The Communication Review*, 7(1), 3-14. <https://doi.org/10.1080/10714420490280152>
- Marshall, T. H. (1950). *Citizenship and social class*. Cambridge University Press.
- Microsoft. (2020). *Empowering people with disabilities through AI*. Microsoft. https://futureofwork.wbcd.org/wp-content/uploads/2020/02/WBCSD-FoW-Case-Study-Microsoft_2020_final.pdf
- Microsoft. (2021). AI for Accessibility. URL: <https://www.microsoft.com>
- Mossberger, K., Tolbert, C. J., & McNeal, R. S. (2007). *Digital citizenship: The Internet, society, and participation*. MIT Press. <https://doi.org/10.7551/mitpress/7428.001.0001>
- Mueller, M. L. (2017). *Will the internet fragment? Sovereignty*, Dwork, C., & Mulligan, D. K. (2013). It's not privacy, and it's not fair. *Stanford Law Review Online*, 66, 35-40.
- e-Estonia. (2024, April 9). A year of advanced threats and global tensions: Estonia's cyber security scene in 2023. *e-Estonia*. <https://e-estonia.com/2023-estonia-advanced-cybersecurity-threats/>
- Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor*. St. Martin's Press.
- European Commission. (2020). *Safer Internet Day*. <https://ec.europa.eu>
- European Parliament and Council. (2022). *Digital Services Act*. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065>
- The way forward for intellectual property internationally. *Information Technology and Innovation Foundation*, 2019 April, 1-61.
- Ezell, S., & Cory, N. (2019). *The way forward for intellectual property internationally*. Information Technology and Innovation Foundation. <https://itif.org/publications/2019/04/25/way-forward-intellectual-property-internationally/>
- Floridi, L., Cows, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., ... Schafer, B. (2018). AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. *Minds and Machines*, 28(4), 689-707. <https://doi.org/10.1007/s11023-018-9482-5>
- Floridi, L., Cows, J., King, T. C., & Taddeo, M. (2020). How to design AI for social good: Seven essential factors. *Science and Engineering Ethics*, 26, 1771-1796. <https://doi.org/10.1007/s11948-020-00213-5>
- Gillespie, T. (2018). *Custodians of the internet: Platforms, content moderation, and the hidden decisions that shape social media*. Yale University Press.
- Global Forum on Cyber Expertise. (2020). *Annual report 2020: Advancing cyber capacity-building globally*. GFCE. <https://www.thegfce.org>
- Graham, M., Hjorth, I., & Lehdonvirta, V. (2017). Digital labour and development: Impacts of global digital labour platforms. *Development in Practice*, 27(1), 102-112. <https://doi.org/10.1177/1024258916687250>
- Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state*. Metropolitan Books.
- GSMA. (2020). *The mobile gender gap report 2020*. Global System for Mobile Communications Association (GSMA). <https://www.gsma.com/r/gender-gap-2020/>
- Heater, D. (2004). *A brief history of citizenship*. Edinburgh

- <https://www.un.org/en/about-us/universal-declaration-of-human-rights>
- Van Deursen, A. J., & Helsper, E. J. (2015). The third-level digital divide: Who benefits most from being online? *Communication and Information Technologies Annual: Digital Distinctions and Inequalities*, 10, 29-52. <https://doi.org/10.1108/S2050-206020150000010002>
- Van Dijk, J. (2020). *The deepening divide: Inequality in the information society*. Sage Publications.
- Voigt, P., & Von dem Bussche, A. (2017). *The EU general data protection regulation (GDPR): A practical guide*. Springer. <https://doi.org/10.1007/978-3-319-57959-7>
- Wardle, C., & Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policy making*. Council of Europe.
- Willett, M. (2021). Lessons of the SolarWinds Hack. *Survival*, 63(2), 7-26. <https://doi.org/10.1080/00396338.2021.1906001>
- World Bank. (2018). *World development report 2018: Learning to realize education's promise*. Washington, DC: World Bank. <https://doi.org/10.1596/978-1-4648-1096-1>
- Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.
- globalization, and cyberspace*. Polity Press.
- Noble, S. U. (2018). *Algorithms of oppression: How search engines reinforce racism*. NYU Press.
- Ostrom, E. (1990). *Governing the commons: The evolution of institutions for collective action*. Cambridge University Press.
- Prensky, M. (2001). Digital natives, digital immigrants. *On the Horizon*, 9(5), 1-6. <https://doi.org/10.1108/10748120110424816>
- Rao, U., & Nair, V. (2019). Aadhaar: governing with biometrics. *South Asia: Journal of South Asian Studies*, 42(3), 469-481. <https://doi.org/10.1080/00856401.2019.1595343>
- Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press.
- Solove, D. J. (2010). *Understanding privacy*. Harvard University Press.
- Tufekci, Z. (2017). *Twitter and tear gas: The power and fragility of networked protest*. Yale University Press.
- UNESCO. (2018). *Digital literacy framework*. UNESCO Publishing. <https://unesdoc.unesco.org>
- UNESCO. (2021). *Media and information literacy: A model for digital education*. UNESCO. <https://unesdoc.unesco.org>
- UNESCO. (2023). *Media and Information Literacy*. <https://doi.org/10.54676/UYKM6672>
- United Nations. (1948). *Universal Declaration of Human Rights*.