

Global Governance of Genomic and Algorithmic Data; A Comparative Study of Iran's and the European Union's Commitments and Capacities within a Cyber Biosecurity Framework

Mojtaba Savadkoochi

Department of Law, Qas, C., Islamic Azad University, Qaemshahr, Iran.

Email: Mojtaba.savadkoochi@iau.ac.ir

 0009-0001-2385-1698

Fatemeh Mahdavi

Department of Theology, Qas, C., Islamic Azad University, Qaemshahr, Iran.

(Corresponding Author)

Email: Fa.mahdavy@iau.ac.ir

 0000-0002-6508-6795

Javad Habibi

Department of Law, Qas, C., Islamic Azad University, Qaemshahr, Iran.

Email: Dr.javad.habibi@iau.ac.ir

 0000-0002-1654-6660

Abstract

This study analyzes genomic and algorithmic data governance in Iran and the European Union, focusing on its implications for cyber-biosecurity and risks associated with emerging technologies. The research question is how differences in legal frameworks, institutional quality, and data governance patterns produce varying levels of cyber-biosecurity and control over intelligent biotechnology threats. The study hypothesizes that the European Union, due to strong regulatory institutions and stringent legal regimes, achieves higher cyber-biosecurity, whereas Iran, lacking a coherent data governance architecture and integration between biological and cyber policymaking, faces greater limitations in risk control. Using a descriptive-analytical method and comparative approach, the research draws on global governance, international technology regimes, and relational biosecurity theories. Findings show that the European Union benefits from coordinated multilevel regulation, comprehensive data protection rules, and greater resilience against cyber-biological threats, while serving as an international standard-setting actor. In contrast, Iran's data governance remains fragmented and institution-centered, with limitations in integrated regulation, secure data infrastructure, and participation in transnational regulatory networks. The study concludes that genomic data governance requires coherent institutional architecture, binding rules, standardized protection mechanisms, stronger integration of biological and cyber policymaking, enhanced regulatory capacity, and engagement with international technology regimes.

Keywords: Genomic Data Governance, Cyber-Biosecurity, Technology Regimes, Artificial Intelligence, Data Protection.

Extended Abstract

Introduction: The rapid convergence of biotechnology, artificial intelligence, and big data has created a new category of strategic resources known as genomic and algorithmic data. These resources include human genetic information and the algorithms and computational models used to process and interpret it. Their applications in precision medicine, drug development, public health, biosecurity, and socioeconomic policymaking have made their protection and governance major concerns of contemporary technology governance. The increasing use of artificial intelligence in biological data analysis has also contributed to the emergence of cyber-biosecurity, a field characterized by the growing interdependence of digital infrastructures, data systems, and biological technologies. Consequently, threats may take hybrid forms, including cyberattacks against genomic databases, manipulation of biological information, and malicious exploitation of biological algorithms. Governments and international organizations have therefore sought to regulate biological and algorithmic data through legislation, regulatory institutions, and technical standards. The European Union has become a leading actor in this field through the General Data Protection Regulation (GDPR), cybersecurity policies, and artificial intelligence governance. Iran, despite scientific progress in biotechnology and artificial intelligence, continues to face challenges involving institutional coordination, comprehensive data protection, and integration of biological and cyber policies. This study therefore compares genomic and algorithmic data governance in Iran and the European Union to determine how differences in legal frameworks, institutional capacities, and governance models affect cyber-biosecurity and technological risk management.

Research Question: How do differences in institutional architecture, legal frameworks, technical infrastructures, and international engagement shape genomic and algorithmic data governance and cyber-biosecurity in Iran and the European Union?

Research Hypothesis: The study hypothesizes that stronger institutional coordination, comprehensive legal protection, secure data infrastructures, and deeper international engagement produce more coherent genomic and algorithmic data governance and consequently higher levels of cyber-biosecurity. Therefore, the European Union is expected to demonstrate greater regulatory coherence and technological resilience than Iran.

Methodology and Theoretical Framework: This study employs a descriptive-analytical approach and a comparative research method. Data were collected through qualitative analysis of national laws and regulations, policy documents, reports issued by international organizations, academic articles, and other scholarly sources. Iran and the European Union were compared across four dimensions: institutional architecture, legal frameworks, data infrastructures, and international interaction. The theoretical framework is based on technology governance and cyber-biosecurity perspectives, which view security as an interconnected outcome of legal, institutional, technical, and transnational arrangements. This framework makes it possible to assess how governance capacity affects the protection of sensitive biological and algorithmic information and the management of risks created by technological convergence.

Research Findings: The findings reveal substantial differences between Iran and the European Union across institutional, legal, infrastructural, and international dimensions. Institutionally, the EU has developed a multilayered and coordinated governance system involving national regulatory authorities and supranational bodies such as the European Data Protection Board. This structure promotes



harmonized policymaking, oversight, and enforcement. Iran, by contrast, relies on fragmented institutional arrangements in which health, information technology, and security organizations share responsibilities, while coordination remains limited. Such fragmentation can obstruct unified standards and comprehensive risk management.

Legally, the EU benefits from a relatively comprehensive and stringent data protection regime. The GDPR establishes clear requirements for collecting, processing, and transferring personal data, including genomic information, while strengthening privacy, accountability, and organizational responsibility. Iran lacks an equally integrated legal framework; relevant provisions remain dispersed across sectoral laws, regulations, and guidelines. This fragmentation creates difficulties in protecting sensitive information and regulating genomic and algorithmic analysis. Technically, the EU has invested substantially in secure data infrastructures, including biobanks, advanced data centers, high-performance computing systems, and collaborative research platforms. These infrastructures support secure storage, processing, and analysis while incorporating stronger cybersecurity standards. Iran possesses significant scientific capabilities in biotechnology and genomics, but its infrastructures remain comparatively less mature, particularly regarding security standards, computational capacity, and system integration. These limitations can increase vulnerabilities and constrain the effective use of genomic and algorithmic resources.

Internationally, the EU plays an active role in shaping global data governance and emerging technology standards. Its policies have influenced international approaches to data protection and ethical technology use, strengthening its position as a standard-setting actor. Iran has more limited participation in transnational regulatory networks and international technology regimes, potentially reducing opportunities for scientific cooperation, regulatory learning, knowledge transfer, and access to collaborative mechanisms. Overall, the findings support the hypothesis that institutional coherence, legal comprehensiveness, infrastructural capacity, and international engagement significantly influence cyber-biosecurity and technological resilience.

Conclusion: The comparative analysis demonstrates that effective governance of genomic and algorithmic data requires the simultaneous coordination of institutional, legal, technical, and international dimensions. The European Union has developed a relatively coherent governance system because of its comprehensive legal framework, independent regulatory institutions, advanced data infrastructures, and active international engagement. This system supports privacy and security while facilitating scientific research and technological innovation. Iran, despite considerable scientific capabilities in biotechnology and artificial intelligence, faces persistent governance challenges arising from institutional fragmentation, incomplete data protection legislation, and limitations in secure data infrastructure. To strengthen cyber-biosecurity, Iran should improve coordination among relevant institutions, establish comprehensive and transparent data protection regulations, develop secure and interoperable data infrastructures, and strengthen mechanisms for accountability and oversight. Greater participation in international scientific and regulatory networks could additionally support knowledge transfer, technical standardization, and institutional learning. More broadly, the governance of biological data cannot be addressed solely through national policies because technological risks increasingly cross institutional and territorial boundaries. Effective cyber-biosecurity therefore requires closer integration of biological and cyber policies, coherent institutional architecture, transparent legal rules, resilient



infrastructures, and constructive international cooperation. Such measures can reduce vulnerabilities, improve technological resilience, and enable responsible innovation while protecting sensitive genomic and algorithmic resources. These reforms should also prioritize ethical principles, including informed consent, proportionality, purpose limitation, transparency, and equitable access to technological benefits. Clear standards for data ownership, cross-border transfer, algorithmic accountability, and incident reporting would further strengthen trust among citizens, researchers, institutions, and international partners. Consequently, integrated governance can transform genomic and algorithmic data from security vulnerabilities into responsibly managed strategic assets.

Keywords: Genomic Data Governance, Cyber-Biosecurity, Technology Regimes, Artificial Intelligence, Data Protection.

E-ISSN: 2717-0551 / University of Mazandaran / Quarterly of Strategic Studies of International Politics

Quarterly of Strategic Studies of International Politics is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.



doi 10.22080/jpir.2026.31587.1570

حکمرانی جهانی داده‌های ژنومی و الگوریتمی؛ مطالعه تطبیقی تعهدات و ظرفیت‌های ایران و اتحادیه اروپا در چارچوب امنیت سایبری - زیستی

مجتبی سوادکوهی

گروه حقوق، واحد قائم‌شهر، دانشگاه آزاد اسلامی، قائم‌شهر، ایران.

Email: Mojtaba.savadkahi@iau.ac.ir

 0009-0001-2385-1698

فاطمه مهدوی

گروه الهیات، واحد قائم‌شهر، دانشگاه آزاد اسلامی، قائم‌شهر، ایران. (نویسنده مسئول)

Email: Fa.mahdavy@iau.ac.ir

 0000-0002-6508-6795

جواد حبیبی

گروه حقوق، واحد قائم‌شهر، دانشگاه آزاد اسلامی، قائم‌شهر، ایران.

Email: Dr.javad.habibi@iau.ac.ir

 0000-0002-1654-6660

چکیده

پژوهش حاضر با هدف تحلیل تطبیقی حکمرانی داده‌های ژنومی و الگوریتمی در ایران و اتحادیه اروپا و پیامدهای آن بر امنیت سایبری - زیستی انجام شده است. پرسش پژوهش آن است که تفاوت در چارچوب‌های حقوقی، کیفیت نهادی و الگوهای حکمرانی داده در ایران و اتحادیه اروپا چگونه به امنیت سایبری - زیستی و کنترل تهدیدات زیست‌فناوری منجر می‌شود. فرضیه پژوهش این است که اتحادیه اروپا به دلیل نهادهای تنظیم‌گر و رژیم‌های حقوقی سخت‌گیرانه، سطح بالاتری از امنیت سایبری - زیستی را فراهم می‌کند؛ درحالی‌که ایران به دلیل فقدان معماری منسجم داده‌ای و پیوند ناکافی میان سیاست‌گذاری زیستی و سایبری، با محدودیت‌هایی در کنترل ریسک‌ها مواجه است. روش پژوهش توصیفی - تحلیلی و مبتنی بر نظریه‌های حکمرانی جهانی و رژیم‌های بین‌المللی فناوری است. یافته‌ها نشان می‌دهد اتحادیه اروپا از تنظیم‌گری چندسطحی، مقررات حفاظت از داده و تاب‌آوری در برابر تهدیدات سایبری - زیستی برخوردار است؛ حکمرانی داده در ایران پراکنده و نهادمحور بوده و در مقررات یکپارچه، زیرساخت‌های داده و مشارکت در شبکه‌های تنظیم‌گری با محدودیت مواجه است. بنابراین، معماری نهادی منسجم، قواعد الزام‌آور، استانداردسازی حفاظت از داده، تقویت پیوند سیاست‌گذاری زیستی و سایبری برای کاهش ریسک‌ها و تقویت امنیت سایبری - زیستی ایران است.

کلیدواژه‌ها: حکمرانی داده‌های ژنومی، امنیت سایبری - زیستی، رژیم‌های فناوری، هوش مصنوعی، حفاظت از داده.

۱. مقدمه

تحولات شتابان در حوزه‌های ژنومیک، زیست‌فناوری، کلان‌داده و هوش مصنوعی، ماهیت قدرت، امنیت و حکمرانی را در عصر دیجیتال دستخوش تغییرات بنیادین کرده است. در این میان، داده‌های ژنومی و الگوریتمی به‌عنوان یکی از مهم‌ترین دارایی‌های راهبردی قرن بیست‌ویکم، جایگاه ویژه‌ای در رقابت‌های علمی، اقتصادی و امنیتی دولت‌ها یافته‌اند. داده‌های ژنومی، به دلیل دربرداشتن اطلاعات حساس زیستی و هویتی افراد و جوامع و داده‌های الگوریتمی، به سبب نقش تعیین‌کننده در پردازش، تحلیل و تصمیم‌سازی هوشمند، به منابعی تبدیل شده‌اند که کنترل، حفاظت و بهره‌برداری از آن‌ها پیامدهایی فراتر از حوزه فناوری داشته و به ابعاد امنیت ملی، سلامت عمومی، اقتصاد دانش‌بنیان و سیاست‌گذاری عمومی گسترش یافته است. از این‌رو، حکمرانی این داده‌ها به یکی از مهم‌ترین موضوعات مورد توجه دولت‌ها، سازمان‌های بین‌المللی و نهادهای تنظیم‌گر تبدیل شده است.

هم‌زمان با افزایش ظرفیت‌های فناورانه در حوزه زیست‌فناوری و هوش مصنوعی، مخاطرات جدیدی نیز در عرصه امنیت بین‌المللی پدیدار شده است. امکان دسترسی غیرمجاز به بانک‌های اطلاعات ژنومی، سوءاستفاده از داده‌های زیستی برای اهداف تجاری یا امنیتی، حملات سایبری علیه زیرساخت‌های سلامت و پژوهش‌های زیستی و همچنین بهره‌گیری از الگوریتم‌های هوشمند در توسعه فناوری‌های زیستی حساس، نمونه‌هایی از تهدیدات نوظهوری هستند که ضرورت بازاندیشی را در الگوهای سنتی امنیت آشکار ساخته‌اند. در چنین شرایطی، مفهوم «امنیت سایبری - زیستی»^۱ به‌عنوان یکی از حوزه‌های نوین مطالعات امنیتی مطرح شده است؛ مفهومی که بر تلاقی میان زیست‌فناوری، فناوری اطلاعات، داده‌های زیستی و سامانه‌های هوش مصنوعی تأکید دارد و تلاش می‌کند راهکارهایی برای مدیریت ریسک‌های ناشی از همگرایی این فناوری‌ها ارائه دهد. در پاسخ به این چالش‌ها، نظام‌های حقوقی و نهادهای حکمرانی در سطوح ملی و بین‌المللی به سمت تدوین چارچوب‌های جدید تنظیم‌گری داده حرکت کرده‌اند. در ادبیات حکمرانی جهانی، مدیریت داده‌های حساس نه صرفاً یک مسأله فنی، بلکه بخشی از سازوکارهای توزیع قدرت، تنظیم روابط فراملی و کنترل فناوری‌های راهبردی تلقی می‌شود. بر اساس این، کیفیت نهادهای تنظیم‌گر، میزان انسجام قوانین حفاظت از داده، ظرفیت‌های نظارتی و سطح مشارکت کشورها



در رژیم‌های بین‌المللی فناوری، نقش تعیین‌کننده‌ای در شکل‌دهی به امنیت سایبری - زیستی و مدیریت تهدیدات ناشی از فناوری‌های نوظهور ایفا می‌کند.

در این میان، اتحادیه اروپا به‌عنوان یکی از پیشروترین بازیگران عرصه حکمرانی داده، توانسته است از طریق ایجاد نظامی چندسطحی از مقررات و نهادهای نظارتی، الگویی نسبتاً منسجم برای حفاظت از داده‌های حساس و تنظیم فناوری‌های نوین ارائه کند. مقررات عمومی حفاظت از داده‌ها^۱ قانون هوش مصنوعی اتحادیه اروپا^۲ و راهبردهای امنیت سایبری این اتحادیه، نمونه‌هایی از تلاش برای ایجاد تعادل میان نوآوری فناوریانه، حقوق بنیادین شهروندان و ملاحظات امنیتی محسوب می‌شوند. همین امر موجب شده است که اتحادیه اروپا به یکی از مهم‌ترین استانداردگذاران جهانی در حوزه حکمرانی داده و فناوری تبدیل شود. در مقابل، ایران طی سال‌های اخیر پیشرفت‌های قابل توجهی در حوزه‌های زیست‌فناوری، پزشکی ژنومیک و توسعه سامانه‌های مبتنی بر هوش مصنوعی تجربه کرده است؛ باین‌حال، چارچوب حکمرانی داده‌های ژنومی و الگوریتمی همچنان با چالش‌هایی نظیر پراکندگی نهادی، فقدان مقررات جامع حفاظت از داده، ضعف هماهنگی میان نهادهای متولی و محدودیت در تعامل با شبکه‌ها و رژیم‌های بین‌المللی تنظیم‌گری فناوری مواجه است. این وضعیت می‌تواند بر ظرفیت کشور در مدیریت ریسک‌های سایبری - زیستی، حفاظت از داده‌های حساس و بهره‌برداری ایمن از فناوری‌های نوظهور تأثیرگذار باشد.

با وجود اهمیت فزاینده موضوع، بخش قابل توجهی از پژوهش‌های موجود بر ابعاد فنی زیست‌فناوری، امنیت سایبری یا حفاظت از داده متمرکز بوده‌اند و مطالعاتی که به‌طور هم‌زمان رابطه میان حکمرانی داده‌های ژنومی و الگوریتمی، امنیت سایبری - زیستی و رژیم‌های بین‌المللی فناوری را در قالب یک چارچوب تطبیقی بررسی کنند، همچنان محدود هستند. به‌ویژه در مورد ایران، کمبود پژوهش‌های تطبیقی که بتوانند ظرفیت‌ها و چالش‌های حکمرانی داده را در مقایسه با الگوهای پیشرو جهانی تحلیل کنند، به‌وضوح مشاهده می‌شود. این خلأ پژوهشی ضرورت انجام مطالعاتی را برجسته می‌کند که بتوانند ارتباط میان ساختارهای حکمرانی داده و سطح تاب‌آوری سایبری - زیستی را تبیین کنند. بر اساس این، پژوهش حاضر به مطالعه تطبیقی حکمرانی داده‌های ژنومی و الگوریتمی در ایران و اتحادیه اروپا می‌پردازد. به بیانی دیگر، هدف اصلی پژوهش، تبیین تأثیر تفاوت‌های موجود در چارچوب‌های حقوقی، ظرفیت‌های

1. GDPR

2. EU AI Act

نهادی و الگوهای حکمرانی داده بر امنیت سایبری - زیستی و مدیریت ریسک فناوری‌های نوظهور است. در همین راستا، پرسش اصلی پژوهش عبارت است از اینکه: «تفاوت در چارچوب‌های حقوقی، ظرفیت‌های نهادی و الگوهای حکمرانی داده در ایران و اتحادیه اروپا چگونه بر سطح امنیت سایبری - زیستی و توانایی مدیریت ریسک‌های فناوری‌های نوظهور تأثیر می‌گذارد؟»

۲. ادبیات نظری و پیشینه پژوهش

۲-۱. نظریه حکمرانی جهانی

نظریه حکمرانی جهانی^۱ یکی از مهم‌ترین رویکردها برای فهم نظم سیاسی، نهادی و هنجاری در جهان معاصر است. این نظریه از این فرض آغاز می‌کند که تحولات جهانی، به‌ویژه در حوزه‌هایی مانند فناوری، سلامت، امنیت زیستی، اقتصاد دیجیتال و جریان داده، آن‌قدر پیچیده و فرامرزی شده‌اند که هیچ دولت واحدی به‌تنهایی قادر به مدیریت کامل آن‌ها نیست (Loginova & Cooper, 2024: 9). به همین دلیل، حکمرانی در سطح جهانی به‌عنوان فرآیندی چندسطحی و شبکه‌ای تعریف می‌شود که در آن بازیگران متعددی از جمله دولت‌ها، سازمان‌های بین‌المللی، نهادهای تنظیم‌گر، شرکت‌های چندملیتی، آزمایشگاه‌های تحقیقاتی، انجمن‌های علمی، جامعه مدنی و حتی زیرساخت‌های فناورانه در تولید قواعد و شکل‌دهی به رفتارها نقش دارند. در این چارچوب، حکمرانی نه صرفاً به معنای «حکومت»، بلکه به معنای «تنظیم، هماهنگی، هدایت و حل مسأله» است (Weiss & Wikinson, 2023: 71-72).

در حوزه داده‌های ژنومی و الگوریتمی، حکمرانی جهانی اهمیت ویژه‌ای پیدا می‌کند؛ زیرا این داده‌ها ذاتاً از مرزهای ملی عبور می‌کنند. یک نمونه ژنومی ممکن است در یک کشور تولید شود، در کشوری دیگر ذخیره گردد، توسط الگوریتمی در کشور سوم تحلیل شود و نتیجه آن در یک شبکه بین‌المللی به اشتراک گذاشته شود. چنین فرآیندی نشان می‌دهد که امنیت، مالکیت، حریم خصوصی و نظارت بر این داده‌ها صرفاً با قوانین داخلی قابل کنترل نیست؛ بنابراین حکمرانی جهانی بر ضرورت وجود قواعد مشترک، نهادهای هماهنگ‌کننده و چارچوب‌های همکاری فراملی تأکید می‌کند (Hofferberth, 2023: 153). در این رابطه، مسأله اصلی فقط وجود یا نبود قواعد نیست؛ بلکه چگونگی تولید مشروعیت برای آن قواعد نیز اهمیت دارد؛ یعنی باید مشخص شود چه نهادی حق قاعده‌گذاری دارد، این قواعد بر چه مبنایی پذیرفته



می‌شوند و چگونه می‌توان بین منافع متفاوت دولت‌ها و بازیگران خصوصی تعادل برقرار کرد (Studzinski et al., 2025: 119).

همچنین، حکمرانی جهانی بر اصل پاسخ‌گویی، شفافیت، مشارکت و عدالت در توزیع منافع و هزینه‌ها تأکید دارد. در موضوع داده‌های ژنومی و الگوریتمی، این مسأله بسیار حیاتی است؛ زیرا کشورهای دارای زیرساخت پیشرفته معمولاً توان بیشتری برای تولید، ذخیره‌سازی و بهره‌برداری از داده‌ها دارند؛ درحالی‌که کشورهایی با ظرفیت کمتر ممکن است در موقعیت وابستگی قرار بگیرند (Egan, 2023: 44-45). یکی از نقاط قوت این نظریه آن است که به‌جای نگاه صرفاً سلسله‌مراتبی به قدرت، به شبکه‌های چندمرکزی و روابط تعاملی میان بازیگران توجه می‌کند. به این ترتیب، روشن می‌شود که تنظیم‌گری مؤثر در حوزه‌های نوظهور فناوری‌ها نیازمند همکاری میان‌سطحی است؛ یعنی هم قواعد ملی باید وجود داشته باشند، هم استانداردهای منطقه‌ای و هم هنجارهای جهانی (Leeds et al., 2025: 58)؛ بنابراین، نظریه حکمرانی جهانی برای تبیین سازوکارهای اداره داده‌های حساس، تحلیل نقش نهادهای بین‌المللی، و فهم تعامل میان قدرت، مشروعیت و همکاری، چارچوبی بسیار کارآمد فراهم می‌کند.

۲-۲. نظریه رژیم‌های بین‌المللی فناوری

نظریه رژیم‌های بین‌المللی فناوری^۱ به مجموعه‌ای از اصول، هنجارها، قواعد، رویه‌ها و نهادهایی اشاره دارد که رفتار بازیگران را در حوزه‌های فناوری‌ها راهبردی تنظیم می‌کند. در این نظریه، رژیم به معنای صرفاً یک سازمان رسمی نیست؛ بلکه یک نظم نهادی و هنجاری است که انتظارات بازیگران را شکل می‌دهد و حدود رفتار مجاز و غیرمجاز را مشخص می‌کند (Kuznetsov & Mishra, 2023: 1483). این رژیم‌ها معمولاً زمانی شکل می‌گیرند که وابستگی متقابل فناوری‌ها افزایش می‌یابد، خطرات ناشی از استفاده نادرست از فناوری بالا می‌رود یا رقابت میان بازیگران مختلف نیازمند تنظیم قواعد مشترک می‌شود (Finnemore & Farrell, 2022: 35). در حوزه فناوری‌های زیستی، داده‌های ژنومی، هوش مصنوعی و تحلیل‌های الگوریتمی، شکل‌گیری رژیم بین‌المللی فناوری اهمیت اساسی دارد. این داده‌ها و فناوری‌ها نه تنها از نظر اقتصادی ارزشمندند، بلکه از نظر امنیتی، ژئوپلیتیکی و اخلاقی نیز حساسیت بالایی دارند. برای مثال، اگر استاندارد مشخصی برای گردآوری، اشتراک‌گذاری، ذخیره‌سازی یا تحلیل داده‌های

ژنومی وجود نداشته باشد، امکان سوءاستفاده، دستکاری، نشت اطلاعات یا ایجاد نابرابری در دسترسی به منافع فناوری افزایش می‌یابد (Kica & Bowman, 2021: 473). از همین‌رو، رژیم‌های فناوری تلاش می‌کنند چنین شکاف‌هایی را با وضع هنجارها و مقررات مشترک کاهش دهند. یکی از ابعاد مهم این نظریه، توزیع قدرت میان بازیگران مختلف است. برخلاف تصور سنتی که فناوری را صرفاً در اختیار دولت‌ها می‌داند، این نظریه نشان می‌دهد که شرکت‌های بزرگ فناوری، کنسرسیوم‌های علمی، انجمن‌های استانداردگذاری، آزمایشگاه‌های تحقیقاتی و سازمان‌های بین‌المللی نیز در شکل‌دهی رژیم‌ها نقش تعیین‌کننده دارند. درواقع، تنظیم‌گری فناوری در جهان امروز نوعی حاکمیت شبکه‌ای است که در آن قدرت در میان بازیگران مختلف پراکنده شده است (Altenburg & Bhasin, 2022: 994).

از منظر تحلیلی، این نظریه به ما کمک می‌کند تا چگونگی درک تبدیل قواعد فنی به قواعد سیاسی و حقوقی بهتر صورت پذیرد. برای مثال، یک استاندارد فنی در زمینه رمزگذاری داده یا تبادل اطلاعات ممکن است در ابتدا یک تصمیم تخصصی به نظر برسد، اما در عمل به ابزاری برای کنترل جریان داده، تعریف مسؤولیت حقوقی و تعیین موقعیت رقابتی کشورها تبدیل می‌شود. به همین دلیل، رژیم‌های بین‌المللی فناوری تنها مجموعه‌ای از استانداردهای فنی نیستند؛ بلکه سازوکارهایی برای ادارهٔ منازعه، کاهش عدم قطعیت و ایجاد ثبات در محیطی متحول‌اند (Kim, 2023: 156-157). در پژوهش حاضر، این نظریه کمک می‌کند تا بفهمیم چگونه قواعد فراملی در حوزهٔ داده‌های ژنومی و الگوریتمی شکل می‌گیرند، چه بازیگرانی در آن نقش دارند، چگونه استانداردها تثبیت می‌شوند و چگونه این رژیم‌ها بر امنیت، دسترسی و کنترل داده اثر می‌گذارند؛ بنابراین، نظریهٔ رژیم‌های بین‌المللی فناوری برای تحلیل پیوند میان نوآوری، قدرت، تنظیم‌گری و امنیت بسیار مناسب است.

۳-۲- پیشینهٔ تجربی پژوهش

دوندا و شانکار^۱ (۲۰۲۴) در پژوهشی با هدف بررسی حکمرانی جهانی برای فناوری‌های زیستی و هوش مصنوعی: ضرورت ایجاد چارچوب‌های نظارتی مشترک نشان دادند که ادغام زیست‌فناوری با هوش مصنوعی باعث ایجاد توانمندی‌های قدرتمندی در طراحی مولکولی و ویرایش ژن شده است. نویسندگان تأکید می‌کنند که این پیشرفت‌ها هم فرصت‌ساز و هم تهدیدزا هستند. مقاله پیشنهاد می‌کند یک رژیم جهانی برای نظارت



بر طراحی مولکولی مبتنی بر هوش مصنوعی ایجاد شود. همچنین بر خطر سوءاستفاده از مدل‌های مولد برای ساخت توالی‌های ژنتیکی خطرناک تأکید می‌شود. نویسندگان در پایان نتیجه گرفتند که همکاری جهانی میان دولت‌ها، صنعت و آکادمی برای تنظیم استانداردهای مشترک ضروری است.

اسمیت و اسولت^۱ (۲۰۲۴) در پژوهشی با هدف بررسی تهدیدات زیستی نوظهور در عصر مدل‌های مولد: ارزیابی خطرات و پیشنهاد راهکارها نشان دادند که حتی مدل‌هایی که برای شیمی محاسباتی طراحی شده‌اند، می‌توانند به‌طور ناخواسته توالی‌های خطرناک تولید کنند. مقاله توصیه می‌کند که «غربالگری اجباری خروجی مدل» در سطح بین‌المللی اجرا شود. همچنین نقش شفافیت، انتشار محدود و کنترل دسترسی مطرح می‌شود. نویسندگان در پایان اذعان داشتند که بدون چارچوب حکمرانی بین‌المللی، مدل‌های مولد می‌توانند خطرات زیستی بی‌سابقه ایجاد کنند.

الریش و گیمرک^۲ (۲۰۲۴) در پژوهشی با هدف بررسی حفاظت از داده ژنومی در عصر هوش مصنوعی: تهدیدات جدید و راهکارها نشان دادند که با قدرت گرفتن مدل‌های هوش مصنوعی، امکان بازسازی هویت افراد از داده‌های ژنومی ناشناس افزایش یافته است. نویسندگان در پایان نتیجه گرفتند که استانداردهای امنیت داده ژنومی باید برای عصر هوش مصنوعی بازنگری شوند. خطر افشای هویت ژنتیکی افراد در سطح ملی و بین‌المللی مطرح است.

جاسانوف و پرلمن^۳ (۲۰۲۴) در پژوهشی با هدف بررسی تنظیم‌گری جهانی هوش مصنوعی در زیست‌فناوری: نقشه راه سیاست نشان دادند که فقدان مقررات جهانی، خطرات زیستی نوظهور را تشدید می‌کند. نویسندگان همچنین اذعان داشتند که مدل‌های هوش مصنوعی می‌توانند فرآیندهای زیستی حساس مانند طراحی پروتئین یا ویروس را تسهیل کنند. همچنین به «فاصله نظارتی» میان کشورها اشاره می‌شود. توصیه اصلی مقاله ایجاد چارچوب حکمرانی مشترک برای نظارت بر مدل‌های زیستی-مولد است. نتیجه تأکید می‌کند که جامعه علمی باید همراه با دولت‌ها و صنعت کار کند. خطر افشای هویت ژنتیکی افراد در سطح ملی و بین‌المللی مطرح است.

درنهایت لاکوف (۲۰۲۲) در پژوهشی با هدف بررسی زیرساخت‌ها و گردش در حکمرانی معاصر امنیت زیستی نشان داد که سیستم‌های نظارت بیماری، پایگاه‌های

1. Smith & Esvelt

2. Erlich & Gymrek

3. Jasanoff & Pearlman

داده ژنومی و شبکه‌های آزمایشگاهی بخش مهمی از امنیت زیستی مدرن هستند. مقاله تأکید می‌کند که جریان داده‌ها در این شبکه‌ها تعیین‌کننده سرعت واکنش به بحران‌های زیستی است. همچنین نقش فناوری‌های دیجیتال در مدیریت بیماری‌های نوظهور بررسی می‌شود. نویسنده در پایان نتیجه گرفت که حکمرانی مؤثر نیازمند هماهنگی میان نهادهای علمی و سیاسی است. نتیجه پژوهش نشان می‌دهد که زیرساخت‌های داده‌ای قلب امنیت زیستی جهانی هستند.

۳. روش‌شناسی پژوهش

پژوهش حاضر از نوع توصیفی - تحلیلی است و با رویکرد تطبیقی به بررسی حکمرانی داده‌های ژنومی و الگوریتمی در ایران و اتحادیه اروپا می‌پردازد. شیوه گردآوری داده‌ها کتابخانه‌ای - اسنادی بوده و داده‌های مورد نیاز از طریق بررسی منابع علمی، اسناد سیاستی، مقررات حقوقی، گزارش‌های نهادهای و متون مرتبط با حفاظت از داده، امنیت زیستی و حکمرانی فناوری گردآوری شده است. واحد تحلیل شامل چارچوب‌های قانونی، ظرفیت‌های نهادهای، زیرساخت‌های داده، الگوهای اشتراک‌گذاری داده و سازوکارهای مدیریت ریسک در دو مورد مطالعاتی است. در مرحله تحلیل، با استفاده از مقایسه تطبیقی کیفی، شباهت‌ها و تفاوت‌های ایران و اتحادیه اروپا در ابعاد مزبور شناسایی و تبیین شده است. هدف این روش، ارزیابی میزان تأثیر الگوهای حکمرانی داده بر تاب‌آوری فناوری و کنترل تهدیدات زیست‌فناوری هوشمند است.

۴. تجزیه و تحلیل داده‌ها و یافته‌های پژوهش

۴-۱. الگوی حکمرانی داده‌های ژنومی و الگوریتمی در ایران؛ چالش‌ها،

ظرفیت‌ها و سازوکارهای در حال شکل‌گیری

واقعیت این است که حکمرانی داده‌های ژنومی و الگوریتمی در ایران در مرحله گذار از ساختارهای پراکنده و بخشی به سوی یک نظام منسجم و هماهنگ قرار دارد. ظرفیت‌های علمی و آزمایشگاهی کشور قابل توجه است، اما تبدیل این ظرفیت‌ها به زیرساخت حکمرانی یکپارچه نیازمند برنامه‌ریزی کلان و استانداردهای مشترک است. بخش مهمی از داده‌های زیستی در مراکز درمانی، پژوهشی و دانشگاهی تولید می‌شود، اما نبود سازوکارهای ملی اشتراک داده، مانع بهره‌برداری نظام‌مند از این منابع می‌شود. در حوزه قانون‌گذاری، ایران فاقد چارچوب تخصصی و جامع برای داده‌های ژنومی است و مقررات موجود غالباً پراکنده و واکنشی‌اند. امنیت زیستی دیجیتال نیز هنوز به‌عنوان یک حوزه میان‌رشته‌ای مستقل تثبیت نشده است. به همین دلیل، مسیر ایران ترکیبی



از پیشرفت‌های علمی و چالش‌های نهادی، حقوقی و امنیتی است که باید هم‌زمان مدیریت شوند.

۱-۴. معماری نهادی و چارچوب‌های حقوقی حکمرانی داده‌های ژنومی و

الگوریتمی در ایران

حکمرانی داده‌های ژنومی و الگوریتمی در ایران هنوز در مرحله شکل‌گیری قرار دارد و از منظر انسجام نهادی و جامعیت حقوقی با چالش‌های بنیادین روبه‌روست. ساختارهای موجود عمدتاً برآمده از حوزه‌های سلامت، اخلاق زیستی، فناوری اطلاعات و سیاست‌های عمومی حریم خصوصی‌اند، اما این قواعد پراکنده قادر به پوشش چرخه کامل داده‌های ژنومی از تولید و ذخیره‌سازی تا تحلیل، اشتراک‌گذاری، حفاظت و نابودی نیستند. از این‌رو، نظام حقوقی ایران بیشتر ماهیت واکنشی دارد تا آینده‌نگر؛ وضعیتی که توان پیش‌بینی تهدیدات نوظهور سایبری - زیستی و مدیریت مخاطرات مرتبط با تحلیل‌های الگوریتمی پیشرفته را کاهش می‌دهد (البرزی، ۱۴۰۳: ۲۵-۲۴).

علاوه بر این، حکمرانی نهادی در این حوزه چندپارچه و فاقد هماهنگی ساختاری است. وزارت بهداشت، دانشگاه‌های علوم پزشکی، مراکز پژوهشی زیستی، نهادهای فناوری اطلاعات و برخی ساختارهای امنیت زیستی هرکدام بخشی از مسؤولیت‌ها را بر عهده دارند، اما نبود یک نهاد مرکزی هماهنگ‌کننده موجب تداخل مأموریت‌ها، کندی جریان داده و فقدان وحدت رویه در تصمیم‌گیری می‌شود. پیامد مستقیم این پراکندگی، شکل‌گیری سیاست‌هایی است که اگرچه در حوزه‌های جزئی مفیدند، اما فاقد انسجام و کارآمدی در مقیاس ملی‌اند (مولاپور، ۱۴۰۴: ۸۷).

چالش دیگر، فقدان استانداردهای ملی و الزام‌آور برای ذخیره‌سازی، رمزنگاری، ناشناس‌سازی، اشتراک‌گذاری و مدیریت چرخه عمر داده‌های زیستی است. در غیاب چنین استانداردهایی، هر نهاد روش خاص خود را اتخاذ می‌کند و این امر نه تنها تطبیق‌پذیری داده‌ها را دشوار می‌کند، بلکه احتمال نشت اطلاعات و آسیب‌پذیری زیرساخت‌های داده را افزایش می‌دهد. این وضعیت همچنین توان کشور برای تشکیل یک بانک ملی ژنوم و بهره‌برداری از تحلیل‌های هم‌پیوند در سطح ملی را محدود می‌سازد (طالعی، ۱۴۰۳: ۲۲۹-۲۲۸).

برآیند این عوامل نشان می‌دهد که معماری حکمرانی داده زیستی در ایران نیازمند بازطراحی ساختاری است. ایجاد یک چارچوب قانونی جامع، تأسیس نهاد ملی هماهنگ‌کننده، تدوین استانداردهای فنی و امنیتی الزام‌آور و تعریف دقیق

مسئولیت‌ها، پیش‌شرط‌های ضروری برای حرکت از وضعیت پراکنده به سمت حکمرانی یکپارچه و کارآمد در حوزه داده‌های ژنومی و الگوریتمی به‌شمار می‌روند.

۲-۱-۴. زیرساخت‌های فنی، ظرفیت‌های فناوری و شکاف‌های کلان‌محاسباتی در مدیریت داده‌های ژنومی

ایران در سال‌های اخیر پیشرفت‌های قابل توجهی در حوزه زیست‌فناوری و ابزارهای مرتبط با تولید و تحلیل داده‌های ژنومی تجربه کرده است، اما این پیشرفت‌ها هنوز در چارچوب یک اکوسیستم زیرساختی ملی یکپارچه قرار نگرفته‌اند. آزمایشگاه‌های توالی‌یابی نسل جدید، پلتفرم‌های بایوانفورماتیک و مراکز تحقیقاتی فعال در کشور توان علمی و پژوهشی ارزشمندی ایجاد کرده‌اند، ولی فعالیت آن‌ها عمدتاً در قالب پروژه‌های محدود، دانشگاهی یا سازمانی تعریف شده است. نبود یک شبکه ملی زیرساختی باعث می‌شود این ظرفیت‌ها در مقیاس بزرگ قابل بهره‌برداری نباشند (صنّعی، ۱۴۰۳: ۵۵).

چالش اساسی، فقدان مراکز داده تخصصی و امن در حوزه داده‌های زیستی است. بسیاری از داده‌های ژنومی در مراکز درمانی و پژوهشی به‌صورت محلی ذخیره می‌شوند؛ رویکردی که امکان رمزنگاری استاندارد، کنترل دسترسی، رصد تهدیدات و جمعیت داده‌ها را دشوار می‌کند. نبود چنین مراکز تخصصی، عملاً ظرفیت تشکیل بانک ملی ژنوم و اجرای پروژه‌های مقیاس ملی را محدود می‌سازد (آساد، ۱۴۰۴: ۳۶۲-۳۶۱). از سوی دیگر، شکاف جدی میان نیازهای پردازشی تحلیل‌های ژنومی و توان محاسباتی موجود در کشور مشاهده می‌شود. تحلیل داده‌های ژنومی، به‌ویژه در مقیاس جمعیتی، نیازمند ابررایانه‌ها، ذخیره‌سازهای پیشرفته و الگوریتم‌های بهینه است. بسیاری از مراکز علمی ایران همچنان با محدودیت‌های پهنای باند، فضای ذخیره‌سازی و پردازش سریع مواجه‌اند. این محدودیت‌ها موجب کاهش سرعت پژوهش‌ها و کاستن از توان کشور برای مشارکت در پروژه‌های فراملی می‌شود (شهسواری، ۱۴۰۴: ۳۲۳).

مشکل دیگر، نبود استانداردهای ملی برای مدیریت چرخه عمر داده، پروتکل‌های امنیتی، رمزنگاری و انتقال امن داده است. در نبود این استانداردها، مراکز پژوهشی روش‌های متفاوتی به کار می‌گیرند که ضمن ایجاد ناهمگونی فنی، ریسک رخنه و نشت داده را افزایش می‌دهد (میرهاشمی، ۱۴۰۴: ۱۷۰-۱۶۹). سرانجام، شکاف میان ظرفیت علمی دانشگاه‌ها و توان نهادی کشور نیز قابل توجه است. مراکز دانشگاهی توانایی تولید تحلیل‌های پیشرفته را دارند، اما ارتباط آن‌ها با ساختارهای حکمرانی



داده ضعیف است. این جدایی سبب می‌شود توان علمی بالقوه به سیاست‌گذاری ملی تبدیل نشود (مولاپور، ۱۴۰۴: ۹۰). در مجموع، ایران برای ارتقاء حکمرانی داده ژنومی، نیازمند توسعه مراکز داده امن، تقویت زیرساخت‌های ملی پردازش، استانداردسازی پروتکل‌های فنی و ایجاد شبکه‌های یکپارچه داده‌ای است.

۳-۱-۴. الگوهای اشتراک‌گذاری داده، همکاری بین‌نهادی و ریسک‌های

امنیت زیستی دیجیتال

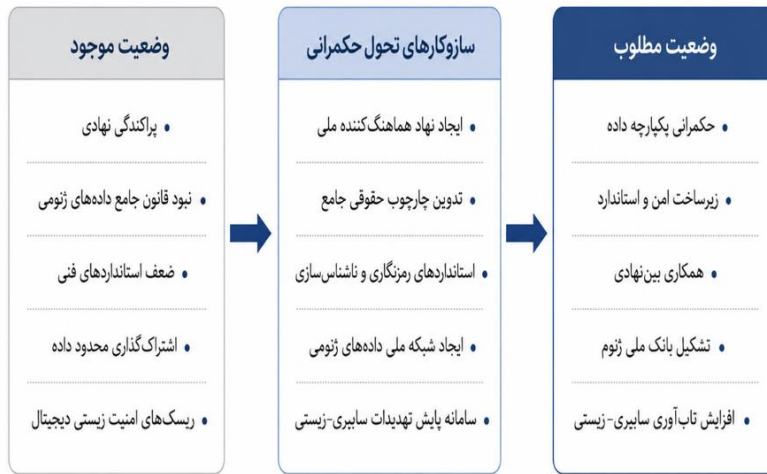
نظام اشتراک‌گذاری داده‌های ژنومی و زیستی در ایران هنوز در مرحله ابتدایی و فاقد ساختار ملی هماهنگ است. هر نهاد یا مرکز پژوهشی بنا به نیاز و ظرفیت خود، سازوکارهای داخلی برای گردآوری، ذخیره‌سازی و تحلیل داده‌ها طراحی می‌کند؛ وضعیتی که نوآوری‌های محلی را ممکن می‌سازد، اما مانع شکل‌گیری یک اکوسیستم داده‌ای یکپارچه در سطح کشور می‌شود (مولاپور، ۱۴۰۴: ۲۴). نبود استانداردهای مشترک برای قالب داده‌ها، پروتکل‌های ذخیره‌سازی، روش‌های ناشناس‌سازی و مدیریت دسترسی، تبادل داده میان مراکز را دشوار و گاه ناممکن می‌کند. این ناهمگونی، یکی از اصلی‌ترین عوامل ناکامی در ایجاد پروژه‌های چندمرکزی و بانک‌های داده ژنومی بزرگ است (محمدی، ۱۴۰۲: ۴۴۵-۴۴۴).

در سطح حقوقی و اخلاقی نیز خلأهای مهمی وجود دارد. نبود چارچوب رسمی برای توافق‌نامه‌های اشتراک داده و عدم وضوح مسؤولیت‌ها باعث می‌شود بسیاری از نهادها در مشارکت داده‌ای تردید داشته باشند؛ نگرانی از نشت اطلاعات، سوءاستفاده از داده‌ها یا پیامدهای قانونی نامشخص، مانعی ساختاری برای همکاری میان بخش‌های درمانی، پژوهشی و امنیت زیستی است (آساد، ۱۴۰۴: ۳۷۱). در کنار این مسائل، امنیت زیستی دیجیتال یکی از چالش‌های راهبردی کشور به‌شمار می‌رود (میرهاشمی، ۱۴۰۴: ۴۸-۴۹).

تهدیدات نوظهور ترکیبی ازجمله نشت داده‌های ژنومی، حملات سایبری به زیرساخت‌های زیستی، دستکاری الگوریتم‌های تحلیل ژنومی و سوءاستفاده از داده‌های زیستی در طراحی حملات هدفمند، هنوز در سیاست‌ها و مقررات ایران بازتاب کافی نیافته‌اند. کمبود نیروی انسانی میان‌رشته‌ای که هم‌زمان با زیست‌شناسی مولکولی، علوم داده و امنیت سایبری آشنا باشد، این شکاف را تشدید می‌کند (زهرایی، ۱۴۰۳: ۱۱۴-۱۱۳). همچنین، فقدان استانداردهای امنیتی اختصاصی، سامانه‌های پایش هوشمند تهدیدات، پروتکل‌های واکنش سریع و سازوکارهای رمزنگاری پیشرفته ازجمله خلأهای مهم زیرساخت امنیت زیستی دیجیتال در کشور است (علیمردانی،

۴۰۳: ۶۱). در مجموع، الگوی فعلی اشتراک‌گذاری داده در ایران مانع شکل‌گیری همکاری مؤثر و تضمین امنیت داده‌های زیستی است. توسعه شبکه ملی اشتراک داده، تدوین استانداردهای رسمی، طراحی سازوکارهای اخلاقی و حقوقی شفاف و ایجاد سامانه‌های امنیت زیستی هوشمند، پیش‌شرط‌های ارتقاء حکمرانی داده ژنومی در ایران به‌شمار می‌روند.

شکل ۱. الگوی حکمرانی داده‌های ژنومی و الگوریتمی در ایران؛ چالش‌ها، ظرفیت‌ها و سازوکارهای در حال شکل‌گیری (طراحی: نویسندگان)



شکل ۱ نشان می‌دهد که مدیریت داده‌های زیستی در ایران از وضعیتی پراکنده و نهادی‌گریز به سوی ساختاری منسجم، هماهنگ و مبتنی بر استانداردهای امنیتی در حال گذار است. در بخش نخست مدل، وضعیت موجود با ویژگی‌هایی مانند پراکندگی نهادی، نبود چارچوب حقوقی جامع، ضعف زیرساخت‌های کلان‌محاسباتی و فقدان استانداردهای یکپارچه برای ذخیره‌سازی و پردازش داده‌های ژنومی ترسیم شده است. این شرایط موجب کاهش قابلیت هم‌افزایی میان نهادهای پژوهشی و درمانی، محدود شدن ظرفیت تحلیل داده‌های زیستی و افزایش آسیب‌پذیری در برابر تهدیدات نوظهور در حوزه امنیت زیستی دیجیتال می‌شود. در سطح میانی مدل، مجموعه‌ای از سازوکارهای تحول‌آفرین قرار گرفته است که نقش واسط میان وضعیت موجود و وضعیت مطلوب را ایفا می‌کنند. مهم‌ترین این سازوکارها شامل ایجاد نهاد هماهنگ‌کننده ملی برای مدیریت داده‌های زیستی، تدوین چارچوب حقوقی و مقرراتی



جامع، توسعه زیرساخت‌های امن ذخیره‌سازی و پردازش داده، استقرار استانداردهای فنی نظیر رمزنگاری، ناشناس‌سازی و کنترل دسترسی و طراحی پروتکل‌های ملی برای اشتراک‌گذاری داده است. این مؤلفه‌ها در کنار سامانه‌های پایش تهدیدات سایبری - زیستی، بستر لازم را برای کاهش ناهمگونی نهادی و ارتقاء قابلیت مدیریت ریسک فراهم می‌کنند. در بخش نهایی، وضعیت مطلوب به‌عنوان نتیجه استقرار این سازوکارها ترسیم شده است؛ وضعیتی که در آن حکمرانی داده‌های ژنومی و الگوریتمی بر پایه هماهنگی نهادی، زیرساخت‌های فنی پایدار و چارچوب‌های حقوقی استاندارد شکل می‌گیرد. در چنین ساختاری، اشتراک‌گذاری ایمن داده میان نهادهای علمی، درمانی و تنظیم‌گر تسهیل شده و ظرفیت تحلیل کلان‌داده‌های زیستی افزایش می‌یابد. پیامد نهایی این فرآیند، تقویت تاب‌آوری سایبری - زیستی، ارتقاء امنیت داده‌های ژنتیکی و کاهش ریسک‌های فناورانه و امنیتی در زیست‌بوم پژوهش و سلامت کشور است.

۲-۴. الگوی حکمرانی داده‌های ژنومی و الگوریتمی در اتحادیه اروپا؛

ساختارهای یکپارچه، استانداردهای پیشرفته و امنیت زیستی دیجیتال اتحادیه اروپا یکی از پیشرفته‌ترین الگوهای حکمرانی داده در جهان را توسعه داده و در حوزه داده‌های ژنومی و الگوریتمی نیز از ساختاری نسبتاً بالغ، چندسطحی و هماهنگ برخوردار است. در این نظام، چارچوب‌های حقوقی جامع، شبکه‌های گسترده زیرساختی و سازوکارهای دقیق اشتراک‌گذاری داده در کنار یکدیگر قرار گرفته‌اند و یک معماری منسجم برای مدیریت داده‌های زیستی ایجاد کرده‌اند. وجود مقررات فراگیری مانند «مقررات عمومی حفاظت از داده‌ها» موجب شده است که داده‌های حساس زیستی در چارچوب استانداردهای سخت‌گیرانه حفاظت شوند و چرخه کامل داده از تولید و ذخیره‌سازی تا تحلیل و انتقال فرامرزی به‌صورت قانونمند مدیریت شود (Sharon, 2023: 5).

در کنار این چارچوب حقوقی، اروپا از زیرساخت‌های داده‌ای قدرتمندی شامل بیوبانک‌های بزرگ، مراکز داده امن، شبکه‌های توالی‌یابی پیشرفته و ابررایانه‌های تخصصی بهره می‌برد که امکان تحلیل مجموعه‌های عظیم داده‌های ژنومی را فراهم می‌کنند. برنامه‌هایی مانند «بر اروپایی علم باز» و «زیرساخت داده‌های ژنومی اروپا» بستری یکپارچه برای ذخیره‌سازی و تبادل داده میان کشورهای عضو ایجاد کرده‌اند و ظرفیت پژوهش‌های چندملیتی را به‌طور قابل توجهی افزایش داده‌اند (Palmer & West, 2024: 612). از سوی دیگر، سازوکارهای اشتراک‌گذاری داده در اروپا بر پایه اعتماد نهادی، استانداردهای فنی مشترک و نظارت اخلاقی دقیق شکل گرفته است.

ابتکارهایی مانند «طرح یک میلیون ژنوم» نمونه‌ای از همکاری فراملی در حوزه داده‌های ژنومی است که امکان اتصال پایگاه‌های داده کشورهای مختلف را در چارچوب قواعد مشترک فراهم می‌کند (Organisciak & Milanovic, 2023: 2397).

در چنین ساختاری، امنیت زیستی دیجیتال نیز به‌عنوان بخشی از سیاست‌های امنیت سایبری و سلامت عمومی مورد توجه قرار گرفته و تهدیدات ترکیبی ناشی از همگرایی زیست‌فناوری، داده‌های کلان و الگوریتم‌های هوش مصنوعی به‌صورت پیشگیرانه مدیریت می‌شوند (Millett & Kuzma, 2023: 1208-1209). بر اساس این، اتحادیه اروپا نمونه‌ای از یک نظام حکمرانی داده‌های زیستی - الگوریتمی منسجم و آینده‌نگر محسوب می‌شود که تلاش می‌کند میان حمایت از نوآوری علمی و حفاظت از داده‌های حساس تعادل برقرار کند.

۱-۲-۴. معماری نهادی و چارچوب‌های حقوقی حکمرانی داده‌های ژنومی و الگوریتمی در اتحادیه اروپا

اتحادیه اروپا یکی از جامع‌ترین چارچوب‌های حقوقی جهان را برای تنظیم داده‌های زیستی و ژنومی ایجاد کرده است. محور اصلی این نظام حقوقی «مقررات عمومی حفاظت از داده‌ها» است که استانداردهای سخت‌گیرانه‌ای برای حفاظت از داده‌های حساس، از جمله داده‌های ژنتیکی، تعیین می‌کند. این مقررات چرخه کامل داده را از مرحله جمع‌آوری تا پردازش، اشتراک‌گذاری و انتقال فرامرزی در بر می‌گیرد و مجموعه‌ای از اصول بنیادین مانند رضایت آگاهانه، حداقل‌سازی داده، مسؤولیت‌پذیری نهادی و حق دسترسی افراد را به داده‌های شخصی تضمین می‌کند (Organisciak & Milanovic, 2023: 2401).

در کنار این مقررات، مجموعه‌ای از قوانین تکمیلی در حوزه سلامت دیجیتال، پژوهش زیستی و هوش مصنوعی نیز وجود دارد که هر یک ابعاد خاصی از مدیریت داده‌های زیستی را پوشش می‌دهند. مقررات هوش مصنوعی، چارچوب‌های اخلاق پژوهش زیستی و دستورالعمل‌های داده‌های سلامت اروپا از جمله ابزارهایی هستند که کاربرد الگوریتم‌ها را در تحلیل داده‌های ژنومی در چارچوب‌های قانونی و اخلاقی مشخص هدایت می‌کنند (Sterckx & Van Assche, 2024: 3-4). در این رابطه، نظام حکمرانی داده در اروپا بر ساختاری چندسطحی استوار است. در سطح ملی، هر کشور عضو دارای نهاد مستقل نظارت بر حفاظت از داده است که اجرای مقررات را تضمین می‌کند. در سطح فراملی نیز «هیأت اروپایی حفاظت از داده‌ها» هماهنگی میان



کشورها و تفسیر یکپارچه مقررات را بر عهده دارد. علاوه بر این، نهادهایی مانند «آژانس دارویی اروپا»، «مرکز اروپایی پیشگیری و کنترل بیماری‌ها» و «کمسیون اروپا» در تنظیم‌گری داده‌های سلامت و مدیریت ریسک‌های زیستی نقش مهمی ایفا می‌کنند (Phillips & Knoppers, 2024: 246-247). ترکیب این چارچوب حقوقی جامع با ساختار نهادهای چندسطحی موجب شده است که سیاست‌گذاری، نظارت و اجرای مقررات در حوزه داده‌های زیستی در اروپا از سطح بالایی از انسجام و قابلیت پیش‌بینی برخوردار باشد.

۲-۴. زیرساخت‌های فنی، ظرفیت‌های کلان‌محاسباتی و شبکه‌های

پژوهشی اروپا

اتحادیه اروپا زیرساختی پیشرفته و گسترده برای مدیریت داده‌های ژنومی ایجاد کرده است که شامل شبکه‌ای از بیوبانک‌ها، مراکز داده امن، سامانه‌های ذخیره‌سازی کلان‌داده و ابررایانه‌های قدرتمند است. این زیرساخت‌ها امکان پردازش حجم عظیمی از داده‌های ژنتیکی را فراهم کرده و پژوهش‌های ژنومیک را در مقیاس جمعیتی ممکن کرده‌اند (Palmer & West, 2024: 612). یکی از مهم‌ترین ابتکارهای اروپا در این زمینه «بر اروپایی علم باز» است که بستری مشترک برای ذخیره‌سازی، اشتراک‌گذاری و تحلیل داده‌های علمی فراهم می‌کند. این سامانه پژوهشگران کشورهای مختلف را قادر می‌سازد داده‌های زیستی را در قالب استانداردهای مشترک مبادله کنند و پروژه‌های پژوهشی مشترک در سطح قاره‌ای اجرا کنند (Veale & Borgesius, 2023: 374).

از نظر ظرفیت پردازشی نیز اروپا به مجموعه‌ای از ابررایانه‌های پیشرفته مانند «لومی»، «ماره‌نوستروم» و «لئوناردو» مجهز است که قادرند تحلیل‌های پیچیده ژنومی و الگوریتمی را با سرعت بسیار بالا انجام دهند. این زیرساخت‌ها به پژوهشگران امکان می‌دهد مدل‌های پیچیده بیماری‌ها را تحلیل کنند، الگوهای ژنتیکی جمعیتی را شناسایی کنند و کاربردهای نوین پزشکی شخصی‌سازی‌شده را توسعه دهند (Shabani & Borry, 2023: 485). علاوه بر این، اروپا مجموعه‌ای از استانداردهای فنی مشترک برای قالب داده‌های ژنومی، فراداده و پروتکل‌های تبادل داده تدوین کرده است. این استانداردها موجب می‌شوند داده‌های تولیدشده در کشورهای مختلف با یکدیگر سازگار باشند و بتوان آن‌ها را در شبکه‌های پژوهشی فراملی تحلیل کرد. چنین زیرساختی یکی از مهم‌ترین مزیت‌های اروپا در رقابت جهانی حوزه ژنومیک محسوب می‌شود.

۳-۲-۴. الگوهای اشتراک‌گذاری داده، همکاری فراملی و امنیت زیستی دیجیتال در اتحادیه اروپا

اتحادیه اروپا یکی از نظام‌های پیشرفته اشتراک‌گذاری داده در حوزه داده‌های ژنومی و سلامت را ایجاد کرده است. این نظام بر پایه ترکیبی از چارچوب‌های حقوقی، نظارت اخلاقی و استانداردهای فنی شکل گرفته و هدف آن تسهیل پژوهش در کنار حفاظت از داده‌های حساس زیستی است. ابتکار «یک میلیون ژنوم» نمونه‌ای شاخص از این رویکرد است که با هدف اتصال پایگاه‌های داده ژنومی کشورهای عضو طراحی شده و امکان تحلیل داده‌های گسترده جمعیتی را فراهم می‌کند (Organisciak & Milanovic, 2023: 2397).

در این نظام، دسترسی به داده‌های ژنومی از طریق سازوکارهای چندمرحله‌ای و شفاف انجام می‌شود. پژوهشگران باید فرآیندهایی مانند ارزیابی علمی، بررسی اخلاقی، تضمین رعایت استانداردهای امنیتی و امضای توافق‌نامه‌های استفاده از داده را طی کنند. مشارکت کمیته‌های اخلاق، نهادهای نظارتی و مراکز تخصصی زیستی در این روند موجب شده است تعادل مناسبی میان توسعه پژوهش و حفاظت از حریم خصوصی برقرار شود (Phillips & Knoppers, 2024: 249). در سطح فنی نیز اروپا از پروتکل‌های پیشرفته بی‌نام‌سازی، شبه‌بی‌نام‌سازی و رمزنگاری داده استفاده می‌کند که امکان تحلیل داده‌ها را بدون افشای هویت افراد فراهم می‌کند. افزون بر این، اتصال پایگاه‌های داده زیستی در کشورهای مختلف باعث شکل‌گیری شبکه‌ای گسترده از همکاری‌های پژوهشی فراملی شده است که نقش مهمی در پیشرفت علم ژنومیک ایفا می‌کند (Veale & Borgesius, 2023: 378-379).

امنیت زیستی دیجیتال نیز بخشی جدایی‌ناپذیر از این نظام حکمرانی محسوب می‌شود. اتحادیه اروپا تهدیداتی مانند نشت داده‌های ژنومی، حملات سایبری به زیرساخت‌های زیستی، دستکاری داده‌ها یا سوءاستفاده از الگوریتم‌های یادگیری ماشین را به‌عنوان ریسک‌های راهبردی شناسایی کرده و برای مدیریت آن‌ها از سامانه‌های پایش تهدید، تیم‌های واکنش سریع، رمزنگاری پیشرفته و معماری‌های دفاع چندلایه بهره می‌گیرد (Millett & Kuzma, 2023: 1212-1214). در مجموع، ترکیب سازوکارهای اشتراک داده استاندارد، همکاری فراملی گسترده و چارچوب‌های امنیتی پیشگیرانه موجب شده است اتحادیه اروپا یکی از منسجم‌ترین و کارآمدترین نظام‌های حکمرانی داده‌های ژنومی در جهان را شکل دهد.



شکل ۲. الگوی حکمرانی داده‌های ژنومی و الگوریتمی در اتحادیه اروپا؛ ساختارهای یکپارچه، استانداردهای پیشرفته و امنیت زیستی دیجیتال (طراحی: نویسندگان)



(طراحی: نویسندگان)

شکل ۲، مدل مفهومی ارائه شده برای حکمرانی داده‌های ژنومی و الگوریتمی در اتحادیه اروپا است که یک ساختار لایه‌ای، منسجم و به هم پیوسته از عناصر حقوقی، نهادی، فناورانه و امنیتی را نشان می‌دهد که در نهایت به تولید پیامدهای راهبردی در

سطح کلان منجر می‌شود. در این مدل، لایه نخست به «معماری حقوقی و نهادی یکپارچه» اختصاص دارد که شامل مقررات عمومی حفاظت از داده‌ها، قانون هوش مصنوعی، نهادهای تنظیم‌گر اروپایی و ساختارهای ملی حفاظت از داده است. این لایه چارچوب اصلی تنظیم رفتار بازیگران، حفاظت از داده‌های ژنومی و تضمین انطباق نهادی را فراهم می‌کند. در لایه دوم، «زیرساخت‌های داده‌ای و ظرفیت‌های کلان‌محاسباتی» قرار دارد که شامل بیوبانک‌های اروپایی، مراکز داده امن، ابررایانه‌ها و سامانه‌های یکپارچه داده‌های علمی است. این زیرساخت‌ها امکان ذخیره‌سازی، پردازش و تحلیل حجم عظیمی از داده‌های ژنومی را در سطح فراملی فراهم و بستر لازم را برای توسعه پژوهش‌های پیشرفته ایجاد می‌کنند. لایه سوم به «اشتراک‌گذاری داده و همکاری‌های فراملی» اختصاص دارد که بر اساس استانداردهای مشترک، توافق‌نامه‌های حقوقی و اخلاقی و سازوکارهای اعتماد نهادی شکل گرفته است و امکان تبادل ایمن داده‌های ژنومی میان کشورهای عضو را فراهم می‌کند. در لایه چهارم، «امنیت سایبری - زیستی و مدیریت ریسک» قرار دارد که شامل سازوکارهای پایش تهدیدات، رمزنگاری داده‌ها، دفاع چندلایه و مدیریت ریسک‌های ناشی از همگرایی زیست‌فناوری و هوش مصنوعی است. در نهایت، لایه پنجم «پیامدهای حکمرانی» را نشان می‌دهد که شامل ارتقاء تاب‌آوری سایبری - زیستی، افزایش امنیت داده‌های ژنومی، توسعه نوآوری علمی، تقویت همکاری‌های فراملی و تثبیت جایگاه اتحادیه اروپا به‌عنوان استانداردگذار جهانی در حوزه حکمرانی داده‌های حساس است.

۵. نتیجه‌گیری و پیشنهاد

تحولات شتابان در حوزه‌های زیست‌فناوری، هوش مصنوعی و کلان‌داده‌ها موجب شده است که داده‌های ژنومی و الگوریتمی به یکی از مهم‌ترین منابع راهبردی در نظام حکمرانی فناوری تبدیل شوند. این داده‌ها افزون بر ارزش علمی، درمانی و اقتصادی، پیامدهای عمیقی برای امنیت زیستی، امنیت سایبری و مدیریت ریسک فناوری‌های نوظهور به همراه دارند. از این‌رو، نحوه تنظیم‌گری، حفاظت، پردازش و اشتراک‌گذاری آن‌ها دیگر صرفاً یک مسئله فنی یا پژوهشی نیست؛ بلکه به موضوعی بنیادین در مطالعات امنیت فناوری، حکمرانی جهانی و تاب‌آوری ملی بدل شده است. در چنین چارچوبی، پژوهش حاضر با هدف تحلیل تطبیقی حکمرانی داده‌های ژنومی و الگوریتمی در ایران و اتحادیه اروپا و بررسی تأثیر این الگوهای حکمرانی بر سطح امنیت سایبری - زیستی، ظرفیت تنظیم‌گری و مدیریت ریسک‌های فناوری‌های نوظهور انجام شد.



یافته‌های پژوهش نشان داد که تفاوت میان ایران و اتحادیه اروپا صرفاً به سطح توسعه فناوری محدود نیست؛ بلکه ریشه در کیفیت معماری حکمرانی، میزان انسجام نهادی، جامعیت رژیم‌های حقوقی، بلوغ زیرساخت‌های داده و نوع مواجهه با ریسک‌های ناشی از همگرایی زیست‌فناوری و فناوری‌های دیجیتال دارد. در سطح نخست، مقایسه تطبیقی چارچوب‌های قانونی و سطح جامعیت مقررات آشکار کرد که اتحادیه اروپا از یک نظام حقوقی چندلایه، هماهنگ و نسبتاً سخت‌گیرانه در حوزه حفاظت از داده‌های شخصی و زیستی برخوردار است. وجود قواعد شفاف برای جمع‌آوری، ذخیره‌سازی، پردازش و اشتراک‌گذاری داده‌های ژنومی، همراه با سازوکارهای نظارتی و ضمانت‌های اجرایی مشخص، سبب شده است که حکمرانی داده در این منطقه در چارچوبی نسبتاً قابل پیش‌بینی و استاندارد صورت گیرد. در مقابل، در ایران اگرچه مقرراتی در حوزه‌های سلامت، اخلاق زیستی، پژوهش و امنیت سایبری وجود دارد، اما این مقررات هنوز به سطح یک نظام حقوقی یکپارچه، اختصاصی و جامع برای داده‌های ژنومی و الگوریتمی نرسیده‌اند. پراکندگی هنجاری و خلأ در پیوند حقوقی میان ساحت‌های زیستی، دیجیتال و امنیتی موجب شده است که تنظیم‌گری این حوزه در بسیاری از موارد نهادمحور، موردی و وابسته به ترتیبات سازمانی باقی بماند.

در سطح دوم، بررسی زیرساخت‌های داده و توان محاسباتی نشان داد که اتحادیه اروپا از ظرفیت‌های فنی و فناورانه بسیار گسترده‌تری برای حکمرانی داده‌های ژنومی برخوردار است. شبکه بیوبانک‌ها، پایگاه‌های داده استاندارد، مراکز داده امن، بسترهای پردازش پیشرفته و قابلیت همگام‌سازی فراملی داده‌ها، امکان مدیریت و بهره‌برداری از داده‌های زیستی را در مقیاسی وسیع و در محیطی نسبتاً ایمن فراهم کرده است. این سطح از توسعه زیرساختی نه تنها مزیت علمی و پژوهشی ایجاد می‌کند، بلکه در افزایش تاب‌آوری در برابر مخاطرات سایبری - زیستی نیز نقش اساسی دارد. در مقابل، اگرچه در ایران ظرفیت‌های علمی و پژوهشی ارزشمندی در دانشگاه‌ها و مراکز تخصصی شکل گرفته و تلاش‌هایی برای توسعه زیرساخت‌های داده‌ای صورت گرفته است، اما این ظرفیت‌ها هنوز از منظر یکپارچگی، استانداردسازی، هم‌پیوندی ملی و دسترسی به توان پردازشی پیشرفته با محدودیت‌هایی همراه‌اند. پراکندگی مخازن داده، وابستگی به مدیریت پروژه‌ای و ضعف در اتصال ساختاری میان پایگاه‌های داده موجب می‌شود که ظرفیت ملی برای بهره‌برداری راهبردی، امن و مقیاس‌پذیر از داده‌های ژنومی به‌طور کامل فعال نشود.

در سطح سوم، تحلیل مدل‌های اشتراک‌گذاری داده و سازوکارهای دسترسی نشان داد که اتحادیه اروپا توانسته است میان ضرورت حمایت از حریم خصوصی و نیاز به دسترسی علمی به داده‌ها نوعی تعادل نهادی و حقوقی برقرار کند. فرآیندهای چندمرحله‌ای ارزیابی علمی، بررسی اخلاقی، پذیرش مسئولیت حقوقی و استفاده از سازوکارهایی مانند ناشناس‌سازی و شبه‌ناشناس‌سازی، امکان اشتراک‌گذاری گسترده اما کنترل‌شده داده‌های حساس را فراهم کرده‌اند. این الگو تنها اعتماد نهادی را افزایش می‌دهد، بلکه موجب تسهیل همکاری‌های علمی در مقیاس بزرگ و فرامرزی نیز می‌شود. در ایران، در مقابل، اشتراک‌گذاری داده‌های ژنومی عمدتاً در سطح سازمانی یا پروژه‌ای صورت می‌گیرد و هنوز یک نظام ملی، هماهنگ و استاندارد برای اعطای دسترسی، تنظیم توافق‌نامه‌های استفاده از داده و تضمین حفاظت از داده‌های حساس شکل نگرفته است. در نتیجه، بهره‌برداری علمی از داده‌ها با محدودیت‌های ساختاری مواجه می‌شود و امکان هم‌افزایی داده‌ای در سطح ملی و بین‌نهادی کاهش می‌یابد.

در سطح چهارم، مقایسه بلوغ امنیت زیستی دیجیتال و سازوکارهای مدیریت ریسک نشان داد که اتحادیه اروپا در مواجهه با مخاطرات ناشی از همگرایی زیست‌فناوری و فناوری‌های دیجیتال رویکردی پیشگیرانه، چندلایه و نهادمند در پیش گرفته است. توسعه استانداردهای تخصصی حفاظت از داده، بهره‌گیری از رمزنگاری پیشرفته، طراحی نظام‌های رصد مستمر تهدیدات، ایجاد تیم‌های واکنش سریع و توجه به خطرات سوءاستفاده از داده‌های زیستی یا دستکاری الگوریتم‌های زیستی، همگی بیانگر آن است که امنیت زیستی دیجیتال در این منطقه به‌عنوان یک حوزه مستقل و نوظهور مورد شناسایی و تقویت قرار گرفته است. در ایران نیز گرچه توجه به امنیت سایبری و امنیت زیستی به‌طور جداگانه وجود دارد و برخی ظرفیت‌های علمی و نهادی قابل توجه در این دو حوزه شکل گرفته است، اما پیوند میان آن‌ها هنوز به یک چارچوب منسجم امنیت زیستی دیجیتال تبدیل نشده است. کمبود تخصص‌های میان‌رشته‌ای، فقدان استانداردهای اختصاصی برای حفاظت از داده‌های ژنومی و محدودیت در سامانه‌های پیشرفته پایش تهدید، از جمله عواملی هستند که سطح بلوغ این حوزه را محدود می‌کنند.

در مجموع، مقایسه تطبیقی ایران و اتحادیه اروپا نشان می‌دهد که امنیت سایبری - زیستی صرفاً محصول پیشرفت فناوریانه نیست؛ بلکه نتیجه مستقیم کیفیت حکمرانی داده، انسجام نهادی، شفافیت حقوقی، توسعه زیرساخت‌های امن و مشارکت فعال در



شبکه‌های فراملی تنظیم‌گری و همکاری علمی است. اتحادیه اروپا به دلیل برخورداری از چارچوب‌های قانونی جامع، زیرساخت‌های داده‌ای پیشرفته، سازوکارهای رسمی اشتراک‌گذاری و بلوغ بالاتر در امنیت زیستی دیجیتال، توانسته است الگوی منسجم‌تری از حکمرانی داده‌های ژنومی و الگوریتمی شکل دهد. در مقابل، ایران با وجود ظرفیت‌های علمی مهم، همچنان با چالش‌هایی در زمینه یکپارچگی نهادی، استانداردسازی مقررات، توسعه زیرساخت‌های امن داده و نهاده‌سازی مدیریت ریسک‌های زیستی - دیجیتال مواجه است.

بر اساس این، می‌توان نتیجه گرفت که ارتقاء حکمرانی داده‌های ژنومی و الگوریتمی در ایران مستلزم چند اقدام هم‌زمان و راهبردی است: نخست، تدوین یک چارچوب حقوقی جامع و اختصاصی برای داده‌های زیستی و الگوریتمی که چرخه کامل حیات داده را پوشش دهد؛ دوم، ایجاد سازوکار نهادی هماهنگ‌کننده میان بخش‌های سلامت، پژوهش، فناوری اطلاعات و امنیت؛ سوم، توسعه زیرساخت‌های ملی داده، مراکز امن ذخیره‌سازی و توان محاسباتی پیشرفته؛ چهارم، طراحی نظام ملی اشتراک‌گذاری داده با استانداردهای روشن فنی، اخلاقی و حقوقی؛ پنجم، تقویت حوزه امنیت زیستی دیجیتال از طریق تربیت نیروی انسانی میان‌رشته‌ای، ارتقاء نظام‌های پایش تهدید و توسعه پروتکل‌های تخصصی حفاظت از داده‌های ژنومی. افزون بر این، تعامل فعال‌تر با رژیم‌های بین‌المللی فناوری و شبکه‌های فراملی تنظیم‌گری نیز می‌تواند امکان بهره‌گیری از تجارب، استانداردها و سازوکارهای مشترک را فراهم کند.

درنهایت، تجربه اتحادیه اروپا نشان می‌دهد که حکمرانی مؤثر داده‌های ژنومی و الگوریتمی زمانی محقق می‌شود که سیاست‌گذاری زیستی و سیاست‌گذاری سایبری نه به صورت دو حوزه منفک، بلکه در قالب یک منظومه واحد و هماهنگ دیده شوند. از این منظر، پیوند مؤثر میان حکمرانی داده، امنیت زیستی، امنیت سایبری و تنظیم‌گری فناوری‌های نوظهور، شرط اساسی ارتقاء تاب‌آوری فناوری و صیانت از منافع ملی در عصر زیست‌داده‌ها و هوش مصنوعی به شمار می‌رود.

۱-۵. پیشنهادها

الف) ایجاد معماری نهادی منسجم برای حکمرانی داده‌های زیستی و الگوریتمی: یکی از مهم‌ترین اقدامات برای ارتقاء امنیت سایبری - زیستی، طراحی یک ساختار نهادی هماهنگ میان نهادهای مسؤول در حوزه زیست‌فناوری، امنیت سایبری و سیاست‌گذاری داده است. چنین ساختاری می‌تواند از پراکندگی نهادی در مدیریت

داده‌های ژنومی جلوگیری کرده و فرآیند تنظیم‌گری این حوزه را منسجم‌تر کند. همچنین ایجاد سازوکارهای هماهنگی میان نهادهای علمی، امنیتی و تنظیم‌گر می‌تواند به بهبود مدیریت ریسک‌های فناوری‌های نوظهور کمک کند.

ب) تدوین چارچوب حقوقی جامع برای حفاظت از داده‌های ژنومی و زیستی: تدوین قوانین جامع در حوزه حفاظت از داده‌های زیستی و ژنومی می‌تواند نقش مهمی در افزایش امنیت داده و حفاظت از حریم خصوصی ایفا نماید. این چارچوب حقوقی باید استانداردهای روشنی برای جمع‌آوری، ذخیره‌سازی، پردازش و تبادل داده‌های ژنومی تعیین کند. همچنین تقویت نظام نظارتی و ایجاد ضمانت‌های اجرایی مؤثر می‌تواند از سوءاستفاده‌های احتمالی از داده‌های حساس جلوگیری نماید.

ج) توسعه زیرساخت‌های امن داده و سامانه‌های مدیریت ریسک زیستی - سایبری: تقویت زیرساخت‌های فناوری اطلاعات و ایجاد بسترهای امن برای ذخیره‌سازی و پردازش داده‌های ژنومی از الزامات اساسی حکمرانی داده‌های زیستی است. توسعه سامانه‌های پیشرفته امنیت سایبری، ایجاد مراکز داده تخصصی و استفاده از فناوری‌های رمزنگاری پیشرفته می‌تواند سطح امنیت این داده‌ها را افزایش دهد. چنین اقداماتی همچنین ظرفیت کشور را برای مقابله با تهدیدات سایبری در حوزه زیست‌فناوری تقویت می‌کند.

د) گسترش همکاری‌های بین‌المللی در حوزه حکمرانی داده و زیست‌فناوری: مشارکت فعال در شبکه‌های علمی و تنظیم‌گری بین‌المللی می‌تواند به انتقال دانش، دسترسی به استانداردهای جهانی و ارتقاء ظرفیت‌های ملی در حوزه حکمرانی داده کمک کند. همکاری با نهادهای بین‌المللی در حوزه تنظیم‌گری داده و امنیت زیستی همچنین می‌تواند زمینه‌های لازم را برای تبادل تجربه و توسعه چارچوب‌های مشترک مدیریت ریسک فراهم کند. چنین تعاملاتی در نهایت به تقویت تاب‌آوری فناورانه و امنیت سایبری - زیستی در سطح ملی کمک خواهد کرد.



فهرست منابع

الف - فارسی

- آساد، محمدتقی. (۱۴۰۴). مبانی ژنتیک. تهران: جهاد دانشگاهی.
- البرزی، محمود. (۱۴۰۴). الگوریتم ژنتیک. تهران: صنعتی شریف.
- زهرایی، بنفشه. (۱۴۰۳). الگوریتم ژنتیک و بهینه‌سازی مهندسی. تهران: گوتنبرگ.
- شهسوار، ناصر. (۱۴۰۴). برنامه‌ریزی و زمان‌بندی تولید با رویکرد الگوریتم‌های فراابتکاری. تهران: کیان.
- صنیعی، محمد. (۱۴۰۳). الگوریتم‌های تکاملی و محاسبات زیستی. تهران: دانش.
- طالعی، علیرضا. (۱۴۰۳). مقدمه‌ای بر ژنتیک بیومتری. تهران: دانشگاه تهران.
- علیمردانی، آرش. (۱۴۰۳). ژنتیک و جرم. تهران: مجد.
- محمدی، امیر. (۱۴۰۴). الگوریتم ژنتیک پزشکی. تهران: اندیشه.
- مولاپور، جاوید. (۱۴۰۴). پروژه‌های کاربردی هوش مصنوعی در پایتون. تهران: دیباگران.
- میرهاشمی، زهرا. (۱۴۰۴). فناوری ژنتیک انسانی. تهران: مجد.

ب - انگلیسی

- Altenburg, T., & Bhasin, S. (2022). Governing digitalization: Global technology regimes and innovation systems. *Journal of Industrial and Corporate Change*, 31(4), 987-1005.
- Doudna, J. A., & Shankar, E. (2024). Global governance for biotechnology and artificial intelligence: The need for shared regulatory frameworks. *Journal of Nature*, (628), 29-48. <https://doi.org/10.1038/d41586-024-00922-6n>.
- M. (2023). *Contestation and Polarization in Global Governance*. New York: Edward Elgar Publishing.
- Erlich, Y., & Gymrek, M. (2024). Re-identification risks in genomic data sharing and artificial intelligence. *Journal of Cell Genomics*, 4(2), 217-235.
- Esvelt, K. M., & Smith, J. C. (2024). Emerging biosecurity risks from generative artificial intelligence. *Journal of Human Science*, (383), 846-848.
- Finnemore, M., & Farrell, H. (2022). The end of cyber-anarchy? How to build a new digital order? *Journal of Foreign Affairs*, 101(3), 30-41.
- Hofferberth, M. (2023). Global Policymaking: The Patchwork of Global Governance. *Journal of Global Policy*, 28(2), 147-169.
- Jasanoff, S., & Pearlman, A. (2024). Governing artificial intelligence in biotechnology: Policy pathways for global health security. *The Lancet Digital Health*, 6(2), 265-291.
- Kica, E., & Bowman, D. M. (2021). Governing emerging technologies through international regimes: The case of gene editing. *Technology in Society*, (66), 469-487.
- Kim, S. (2023). Standards as global technology regimes: The geopolitics of setting international technology standards. *Journal of International Business Policy*, 6(2), 153-170.



- Kuznetsov, D. A., & Mishra, V. (2023). Global technology governance in the age of AI: Challenges for international regimes. *Journal of AI & Society*, (38), 1479-1492.
- Leeds, B. A., Mosley, L., Rosendorff, B. P., & Zarakol, A. (2025). The Future of Global Governance and World Order. *Journal of Cambridge Core*, 79(1), 43- 68.
- Loginova, A., & Cooper, A. (2024). *Global Governance*. London: Routledge.
- Millett, P., & Kuzma, J. (2023). Synthetic biology, cyberbiosecurity, and regulatory challenges in the European Union. *Journal of Trends in Biotechnology*, 41(11), 1203-1221.
- Organisciak, P., & Milanovic, F. (2023). DNA data storage and cybersecurity: Regulatory perspectives in the European Union. *Journal of ACS Synthetic Biology*, 12(9), 2392-2410.
- Palmer, M. J., & West, R. (2024). AI-driven genomic design and emerging biosecurity risks: Implications for European governance. *Journal of Nature Biotechnology*, 42(5), 612-630.
- Phillips, M., & Knoppers, B. M. (2024). Securing genomic data infrastructures in Europe: Governance frameworks for trusted sharing. *Journal of Nature Medicine*, 30(2), 245-261.
- Raszkowski, A., & Wroblewski, P. (2023). Cyber-biosecurity challenges in European biotechnology governance. *Frontiers in Bioengineering and Biotechnology*, (11), 284-308.
- Shabani, M. (2025). European governance for AI-enabled genomic analysis: Ethical, legal, and cybersecurity considerations. *Journal of Regulation & Governance*, 19(1), 55-70.
- Shabani, M., & Borry, P. (2023). Genomic data governance in the European Union: Balancing data protection and data sharing under the GDPR. *European Journal of Human Genetics*, 31(4), 482-499.
- Sharon, T. (2023). Algorithmic governance in the European digital health ecosystem. *Journal of Big Data & Society*, 10(2), 1-20.
- Sterckx, S., & Van Assche, K. (2024). The European Health Data Space and the future of genomic data governance. *Journal of Law and the Biosciences*, 11(1), 1-22.
- Studzinski, N. G., Kent, R., & Korowicz, D. (2025). Towards the Governance of Global Systemic Risk. *Journal of Global Governance*, 31(2), 113-136.
- Veale, M., & Borgesius, F. Z. (2023). Demystifying the EU Artificial Intelligence Act. *Journal of Computer Law & Security Review*, 5(1), 370-395.
- Weiss, T. G., & Wikinson, R. (2023). *International Organization and Global Governance*. London: Routledge.