چکیده مبسوط

عنوان: واکاوی استعمار داده: از تبیین سلطه‌گری نوین تا ضرورت حکمرانی ملی بر داده

نام نویسندگان: مهدیه لطیف زاده؛ استادیار حقوق خصوصی، گروه پژوهشی فقه و حقوق اسلامی، پژوهشکده مطالعات اسلامی در علوم انسانی دانشگاه فردوسی مشهد، مشهد، ایران ؛ پست الکترونیکی: latifzadeh@um.ac.ir

مقدمه: در عصر حاضر که داده به‌عنوان سرمایه راهبردی کشورها شناخته می‌شود، شرکت‌های بزرگ فناوری با بهره‌گیری از ابزارهای پیشرفته به‌جای تسخیر سرزمین‌ها و منابع طبیعی به تصاحب داده‌های کاربران (استعمار داده) اقدام می‌کنند. پدیده استعمار داده به معنای تسلط نظام‌مند بر داده‌های کاربران و بهره‌برداری یک‌جانبه از آن‌ها توسط قدرت‌های فراملیتی فناوری است که با ارائه خدمات به ظاهر رایگان به استخراج و کنترل این منبع راهبردی می‌پردازند. آمارها نشان می‌دهد ایران با بیش از ۴۸ میلیون کاربر فعال در شبکه‌های اجتماعی، یکی از بزرگترین تولیدکنندگان داده در منطقه است که به دلیل فقدان چارچوب حقوقی الزام‌آور، ارزش این داده ها به خارج از مرزهای حاکمیتی کشور منتقل می‌گردد. پژوهش حاضر با رویکردی تحلیلی به بررسی ابعاد حقوقی استعمار داده و راهکارهای مقابله با آن در چارچوب نظام حقوقی ایران می‌پردازد. در این خصوص مسائل اصلی شامل شناسایی خلأهای نظام حقوقی ایران در مواجهه با استعمار داده، ارائه راهکارهای ملی مقابله و تقویت حاکمیت داده همچنین بررسی تجارب موفق کشورهای پیشرو برای تدوین الگوی بومی و استحکام حکمرانی بر داده است.

روش‌شناسی: پژوهش حاضر با بهره‌گیری از روش تحلیل محتوای کیفی به واکاوی چندجانبه پدیده استعمار داده پرداخته است. این پژوهش از نظر هدف، بنیادی بوده و با اتخاذ رویکردی توصیفی-تحلیلی، امکان شناسایی لایه‌های پنهان پدیده استعمار داده و تحلیل عمیق آن را فراهم آورد. روش گردآوری اطلاعات، اسنادی و کتابخانه‌ای بود که شامل بررسی آثار علمی معتبر از پایگاه‌های داده موثق شد. جستجوی منابع با کلیدواژه‌های فارسی و انگلیسی مرتبط از جمله «استعمار داده»، «حاکمیت داده» و "Data Colonialism" و "Data Sovereignty" در پایگاه‌های Web of Science، ScienceDirect، SID (پایگاه مرکز اطلاعات علمی جهاد دانشگاهی) و Magiran (بانک اطلاعات نشریات کشور) انجام گرفته است. در فرایند تحلیل کیفی، مراحل کدگذاری اولیه (۸۷ کد)، کدگذاری محوری (۱۸ مقوله فرعی) و کدگذاری انتخابی (۴ مقوله اصلی) طی شد. چارچوب تحلیلی پژوهش در سه سطح مفهومی، ساختاری و راهبردی طراحی گردید. برای افزایش روایی پژوهش، از روش مثلث‌سازی منابع داده استفاده شد و برای تضمین پایایی، مستندسازی نظام‌مند تمامی مراحل پژوهش صورت گرفت. محدودیت‌های پژوهش نیز شامل نوظهور بودن موضوع، کمبود منابع فارسی و پیچیدگی‌های ذاتی موضوع به دلیل ماهیت میان‌رشته‌ای آن بوده است.

یافته‌های اصلی: پژوهش نشان داد چهار عامل اصلی به عنوان عناصر زمینه‌ساز استعمار داده شناسایی شده‌اند. نخست، خلأ قانونی و ضعف در الزامات حقوقی است که شامل فقدان قوانین جامع حفاظت از داده، عدم تعریف دقیق حقوق

مالکیت داده و نبود ضمانت اجرای مؤثر است. دوم، فقدان زیرساخت‌های فنی مانند کمبود مراکز داده داخلی با ظرفیت کافی، ضعف در فناوری‌های پردازش و تحلیل داده‌های بزرگ و وابستگی به پلتفرم‌های خارجی برای ذخیره‌سازی و پردازش داده‌ها است. سوم، ضعف سازوکار نظارتی است که شامل فقدان نهاد تنظیم‌گر مستقل در حوزه داده، عدم نظام پایش جریان داده‌های مرزی و ناکارآمدی سازوکارهای نظارت بر عملکرد پرداز شگران داده است. چهارم، پایین بودن سطح سواد داده در میان شهروندان، مدیران و تصمیم‌گیران است که منجر به عدم آگاهی از ارزش داده‌ها، ناآشنایی با حقوق دیجیتالی و بی‌توجهی به پیامدهای افشای داده‌های شخصی می شود. این عوامل در تعامل با یکدیگر به تضعیف حاکمیت داده و در نهایت تضعیف نظام حکمرانی بر داده می‌انجامند. همچنین، یافته‌ها نشان داد که استعمار داده از طریق سازوکارهایی مانند استخراج غیر شفاف داده‌های کاربران، الگوریتم‌های انحصاری و غیرقابل بررسی و ایجاد وابستگی فناورانه عمل می‌کند. بررسی تجارب نظام های حقوقی موید این است که برخی از این نظام ها مانند اتحادیه اروپا با مقررات عمومی حفاظت از داده؛ رویکرد مطلوبی را برای حفظ حاکمیت داده اتخاذ کرده‌اند که می‌تواند الگویی برای تدوین چارچوب بومی باشد.

بحث و نتیجه‌گیری: با توجه به یافته های پژوهش روشن است که در عصر حاضر که داده به‌مثابه منبع راهبردی و عنصر کلیدی قدرت ملی محسوب می‌گردد، مقابله با استعمار داده به ضرورتی حاکمیتی مبدل شده است. به موجب برآمد پژوهش برخلاف اَشکال سنتی استعمار، پدیده استعمار داده از طریق سازوکارهای پیچیده‌تر و کم‌هزینه‌تری عمل می‌کند و تأثیرات عمیق‌تری بر حاکمیت ملی کشورها بر جای می‌گذارد. راهکارهای مقابله با استعمار داده شامل ایجاد نظام حقوقی چند سطحی حفاظت از داده است که در سه سطح عمل می‌کند. نخست حمایت‌های بنیادین از طریق اصلاح قوانین موجود، دوم حمایت‌های عام با تدوین قانون جامع حفاظت از داده، و در نهایت حمایت‌های خاص با تمرکز بر داده‌های خاص است. این نظام حقوقی باید با استقرار نظام ملی حاکمیت داده تکمیل گردد که بر پایه ساختاری سه‌لایه‌ای شامل لایه راهبردی (سیاست‌گذاری)، لایه اقتصادی (خلق ارزش) و لایه حمایتی (تأمین امنیت و حفظ حقوق) استوار باشد. تقویت حاکمیت داده نیز مستلزم بازتعریف مفهوم قدرت در فضای سایبری است، به گونه‌ای که تسلط بر داده‌های ملی و توانمندی تحلیل و بهره‌برداری از آن‌ها، شاخص نوینی از قدرت محسوب می‌شود. در نهایت باید دانست که هدف از مقابله با استعمار داده، نه انزوای دیجیتالی، بلکه دستیابی به استقلال داده است که از طریق تقویت زیرساخت‌های ملی، ارتقای توانمندی‌های فنی داخلی و مشارکت فعال در شکل‌دهی به نظام حکمرانی جهانیِ داده محقق می‌گردد. نتیجه نهایی این امر، تحقق حاکمیت مؤثر بر داده‌های ملی و صیانت از حقوق دیجیتالی شهروندان خواهد بود.

کلیدواژه‌ها: استعمار داده، حکمرانی داده، سواد دیجیتالی، قدرت سایبری، مقررات عمومی حفاظت از داده اتحادیه اروپا

Extended Abstract

Title: **Data Colonialism Inquiry: From Explaining New Forms of Domination to the Necessity of National Data Governance**

Names of Authors: Mahdieh Latifzadeh, Assistant professor of private law, Department (The Research Group) of Islamic Jurisprudence and Law, Institute for Islamic Studies in Humanities, Ferdowsi University of Mashhad, Mashhad, Iran, Email: latifzadeh@um.ac.ir

Introduction: In the present era, where data is recognized as a strategic asset of nations, large technology companies employ advanced tools to capture user data (data colonialism) rather than conquering territories and natural resources. The phenomenon of data colonialism refers to the systematic control over user data and unilateral exploitation by transnational technology powers, which offer seemingly free services to extract and control this strategic resource. Statistics show that Iran, with more than 48 million active users on social networks, is one of the largest data producers in the region. However, due to the absence of a binding legal framework, the value of this data is transferred beyond the country's sovereign borders.

This research employs an analytical approach to examine the legal dimensions of data colonialism and countermeasures within Iran's legal framework. The main issues include identifying gaps in Iran's legal system regarding data colonialism, providing national countermeasures and strengthening data sovereignty, as well as examining successful experiences of leading countries to develop a localized model and strengthen data governance.

Methodology: The present research utilizes qualitative content analysis to examine the multifaceted phenomenon of data colonialism. In terms of purpose, it is fundamental research with a descriptive-analytical approach that enables identification of hidden layers of data colonialism and facilitates in-depth analysis. The information collection method was documentary and library-based, including reviewing credible scientific works from reliable databases.

Resource searches were conducted using relevant Persian and English keywords including "data colonialism," "data sovereignty," and others in databases such as Web of Science, ScienceDirect, SID (Academic Jihad Scientific Information Database), and Magiran (Country Publications Information Bank). The qualitative analysis process involved primary coding (87 codes), axial coding (18 subcategories), and selective coding (4 main categories). The analytical framework was designed across three levels: conceptual, structural, and strategic.

To enhance research validity, data source triangulation was employed, and for reliability, systematic documentation of all research stages was carried out. Research limitations included the emerging nature of the topic, scarcity of Persian resources, and inherent complexities due to its interdisciplinary nature.

Main Findings: The research identified four main factors facilitating data colonialism. First, legal gaps and weaknesses in regulatory requirements, including the absence of comprehensive data protection laws, lack of precise definitions for data ownership rights, and insufficient enforcement mechanisms. Second, inadequate technical infrastructure, such as insufficient domestic data centers, weakness in big data processing and analysis technologies, and dependence on foreign platforms for data storage and processing.

Third, weak oversight mechanisms, including the absence of an independent regulatory body in the data field, lack of a cross-border data flow monitoring system, and ineffective oversight of data processors' operations. Fourth, low levels of data literacy among citizens, managers, and decision-makers, leading to lack of awareness about data value, unfamiliarity with digital rights, and disregard for the consequences of disclosing personal data.

These factors interact to weaken data sovereignty and ultimately undermine the data governance system. The findings also revealed that data colonialism operates through mechanisms such as non-transparent extraction of user data, proprietary and unexaminable algorithms, and creation of technological dependency. A review of legal systems demonstrates that some jurisdictions, such as the European Union with its General Data Protection Regulation, have adopted favorable approaches to maintaining data sovereignty that could serve as models for developing localized frameworks.

Discussion and Conclusion: Given the research findings, it is evident that in the current era where data is considered a strategic resource and a key element of national power, countering data colonialism has become a sovereign imperative. According to the research outcomes, unlike traditional forms of colonialism, data colonialism operates through more complex and cost-effective mechanisms while producing deeper impacts on national sovereignty.

Strategies to counter data colonialism include establishing a multi-level legal system for data protection operating at three levels: first, fundamental protections through amending existing laws; second, general protections by developing comprehensive data protection legislation; and finally, specific protections focusing on particular data categories. This legal framework must be complemented by establishing a national data sovereignty system based on a three-layer structure: a strategic layer (policymaking), an economic layer (value creation), and a protective layer (ensuring security and preserving rights).

Strengthening data sovereignty also requires redefining the concept of power in cyberspace, such that mastery over national data and the ability to analyze and utilize it becomes a new indicator of power. Ultimately, it should be understood that the goal of countering data colonialism is not digital isolation but achieving data independence through strengthening national infrastructure, enhancing domestic technical capabilities, and active participation in shaping the global data governance system. The final outcome will be the realization of effective sovereignty over national data and protection of citizens' digital rights.

Keywords: Data Colonialism, Data Governance, Digital Literacy, Cyber Power, General Data Protection Regulation (GDPR)