extended abstract

Title: Scope and Effects of Confidentiality Obligations in Protecting Trade Secrets in the Age of Artificial Intelligence: A Comparative Study of the Legal Systems of Iran, the European Union, and the United States

Names of Authors: Ali Saatchi

Ph.D. in Private Law, Associate Professor, Faculty of Law and Political Science, Ferdowsi University of Mashhad

Email: alisaatchi@um.ac.ir

Javad FahimiTabar

Ph.D. Candidate in Private Law, Ferdowsi University of Mashhad

Email: fahimitabar.javad@gmail.com

Introduction: Today, data have become among the most valuable assets of commercial, scientific, and research organizations, while confidentiality obligations play a fundamental role in protecting such assets. The emergence of generative artificial intelligence and large language models has created new challenges concerning the disclosure, processing, storage, reproduction, and secondary use of confidential information. Sensitive research data, trade secrets, algorithms, training datasets, metadata, and other economically valuable information may enter artificial intelligence systems and subsequently be stored, recombined, inferred, or reproduced without any conventional direct disclosure to a third party. Therefore, the traditional understanding of disclosure appears insufficient to address algorithmic leakage and the loss of effective control over confidential information. This study aims to explain the scope and effects of confidentiality obligations in protecting trade secrets in the age of artificial intelligence and to assess the capacity of Iranian law in comparison with the legal frameworks of the European Union and the United States. The central question is how traditional concepts of confidentiality, disclosure, and liability can be adapted to the technological characteristics of artificial intelligence systems.

Methodology: This fundamental study employed a descriptive-analytical method with a comparative legal approach. Data were collected through library and documentary research and included legislation and regulations, official documents, judicial decisions, regulatory authorities' measures, reports issued by معتبر international organizations, and relevant scholarly literature. The sources were selected according to their legal authority, direct relevance to the research question, currency, and evaluability. The comparative analysis was organized around several predetermined dimensions, including the concept and conditions

for identifying confidential information and trade secrets, the standard of reasonable protective measures, the scope of disclosure and unauthorized processing, the nature of confidentiality obligations, the grounds of liability, the burden of proof, remedies, and sanctions concerning the deletion or restriction of the use of data and algorithms. In the United States, federal and state legal frameworks, judicial practice, and the measures adopted by the Federal Trade Commission were examined. In the European Union, the Trade Secrets Directive, the General Data Protection Regulation, and the Artificial Intelligence Act were analyzed. In Iran, the capacities of contractual rules, civil liability principles, electronic commerce regulations, and relevant legal and jurisprudential concepts, including trust, abuse, negligence, and causation, were assessed. The collected materials were first analyzed separately within each legal system and were subsequently compared to identify common approaches, differences, and solutions applicable to Iranian law.

Main findings: The findings showed that the United States maintains trade secret protection through the requirements of economic value, non-publicity, and reasonable protective measures. The inclusion of confidential information in uncontrolled artificial intelligence platforms may undermine the requirement of reasonable protection and consequently weaken or eliminate legal protection. The study also found that American regulatory approaches have gradually moved beyond the mere deletion of unlawfully obtained data toward the deletion, restriction, or cessation of use of artificial intelligence models and algorithms developed on the basis of such data. In the European Union, confidentiality protection operates through a multidimensional framework combining trade secret protection with data protection, transparency, fundamental rights, cybersecurity, and regulatory requirements for artificial intelligence systems. By contrast, Iranian law lacks a comprehensive and independent legal framework specifically governing trade secrets and data governance. Nevertheless, Articles 10, 219, 220, 221, and 230 of the Civil Code, together with the rules concerning trust, abuse, negligence, causation, unjust enrichment, civil liability, and the Electronic Commerce Law, provide a basis for protecting confidential information within contractual and professional relationships. The findings further demonstrated that disclosure in artificial intelligence environments should be interpreted functionally and technologically. Accordingly, disclosure should not be limited to direct publication or transfer but should encompass conduct that removes information from the holder’s effective control and materially increases the possibility of access, inference, secondary use, or reproduction.

Discussion and conclusions: The findings indicate that the traditional model of confidentiality protection requires significant reconstruction in the age of

artificial intelligence. The most important theoretical development proposed by this study is the transformation of confidentiality from a purely negative obligation of non-disclosure into a strengthened and context-sensitive digital duty of care. Under this approach, the obligated party must not only refrain from intentionally disclosing confidential information but must also adopt contractual, technical, and organizational measures proportionate to the nature and economic value of the information, the severity of potential harm, the possibility of re-identification, the type of artificial intelligence system, and the reasonable cost of prevention. The obligation should neither be regarded as an absolute obligation to achieve a particular result nor reduced to a merely formal obligation of means. After the injured party establishes the existence of a confidentiality relationship, access or entrustment of the information, and an incident occurring outside the authorized processing framework, the burden should be partially shifted to the obligated party to demonstrate that proportionate protective measures were adopted. This approach preserves fairness without creating strict liability. The study further suggests that reasonable protective measures should include information classification, access limitation, multi-factor authentication, encryption, logging, secure deletion, supplier assessment, restriction of public artificial intelligence systems for classified information, periodic security auditing, employee training, and continuous risk assessment. Confidentiality agreements alone should not be considered sufficient to establish reasonable protection. Remedies should also extend beyond monetary damages and may include suspension of processing, restriction of access, prohibition of transfer, targeted deletion, model modification, dataset separation, retraining, and independent auditing, subject to technical feasibility and proportionality. Accordingly, Iranian law has sufficient normative capacity to develop a coherent system for protecting trade secrets in artificial intelligence environments, but this requires a functional reinterpretation of disclosure, recognition of a digital duty of care, risk-based protection standards, a limited adjustment of the burden of proof, and remedies adapted to the reproducible and algorithmic nature of data.

Keywords: Confidentiality Obligation; Non-Disclosure; Trade Secrets; Artificial Intelligence; Digital Duty of Care; Confidential Data; Algorithmic Disclosure; Reasonable Protective Measures