شاپا چاپی: ۱۸۴۱-۲۷۸۳
شاپای الکترونیکی: ۱۹۲۲-۲۷۸۳

تمدن حقوقی

دوره ۸ - شماره ۲۵ - پاییز ۱۴۰۴

Legal Civilization
Vol. 8, No. 25, Autumn 2025
Pages: 593-616
Article Type: Original Research
https://www.pzhfars.ir/article_234795.html
doi: 10.22034/LC.2025.559675.1710

تمدن حقوقی
دوره ۸، شماره ۲۵، پاییز ۱۴۰۴
صفحات ۶۱۶-۵۹۳
نوع مقاله: پژوهشی

حق فراموش شدن و آثار آن بر روابط قراردادی در بلاکچین‌های عمومی؛ تحلیل تطبیقی حریم خصوصی داده‌ها در حقوق ایران و اروپا

عارفه قاسم زاده ده آبادی
دانشجوی کارشناسی‌ارشد حقوق خصوصی، دانشگاه آزاد اسلامی واحد علوم و تحقیقات، تهران، ایران
arefeghasemzade@yahoo.com

چکیده

این پژوهش به بررسی تناقض ذاتی بین ویژگی‌های تغییرناپذیری و شفافیت در بلاکچین‌های عمومی با «حق فراموش شدن» مطابق ماده هفدهم مقررات عمومی حفاظت از داده‌های اتحادیه اروپا می‌پردازد. این تعارض به‌ویژه در زمینه روابط قراردادی مبتنی‌بر قراردادهای هوشمند نمایان می‌شود، چرا که ماهیت غیرمتمرکز و تغییرناپذیر بلاکچین، اجرای حق حذف داده‌های شخصی را با چالش مواجه می‌سازد. هدف اصلی پژوهش، تحلیل آثار این تعارض بر مراحل مختلف رابطه قراردادی (شامل تشکیل، اجرا و انحلال) و ارائه راهکارهای فنی و حقوقی برای کاهش آن است. روش تحقیق به‌کارگرفته شده، تحلیلی-توصیفی با رویکرد تطبیقی است که در آن نظام‌های حقوقی ایران و اروپا مورد مقایسه قرار گرفته‌اند. یافته‌های پژوهش نشان می‌دهند که راهکارهای فنی از جمله طراحی قراردادهای هوشمند خودتخریبگر، هش کردن داده‌ها و ذخیره‌سازی اطلاعات حساس خارج از زنجیره می‌توانند تا حدی این تعارض را کاهش دهند. از منظر حقوقی نیز راهبردهایی مانند تفکیک داده‌ها، گنجاندن شروط صریح در قراردادها و توسعه چهارچوب‌های نظارتی ویژه بلاکچین پیشنهاد شده‌اند. در نهایت، این پژوهش بر ضرورت همکاری میان رشته‌ای برای دستیابی به تعادل بین حریم خصوصی افراد و یکپارچگی فناوری بلاک‌چین تأکید می‌ورزد.

واژگان کلیدی: حق فراموش شدن، بلاکچین عمومی، حریم خصوصی داده‌ها، قرارداد هوشمند، مقررات عمومی حفاظت از داده‌های اتحادیه اروپا.

دریافت مقاله: ۱۴۰۴/۰۷/۰۱ -بازنگری مقاله: ۱۴۰۴/۰۸/۳۰ -پذیرش مقاله: ۱۴۰۴/۰۹/۲۵

The Right to be Forgotten and its Effects on Contractual Relationships in Public Blockchains; a Comparative Analysis of Data Privacy in Iranian and European Law

Arefeh Ghasem Zadeh Dehabadi
Master's student in Private Law, Islamic Azad University, Science and Research Branch, Tehran, Iran

Abstract

This research examines the inherent contradiction between the immutability and transparency features of public blockchains and the "right to be forgotten" in accordance with Article 17 of the EU General Data Protection Regulation. This conflict is particularly evident in the context of contractual relationships based on smart contracts, as the decentralized and immutable nature of blockchains makes it challenging to implement the right to delete personal data. The main objective of the research is to analyze the effects of this conflict on different stages of the contractual relationship including formation, execution, and dissolution and to provide technical and legal solutions to mitigate it. The research method used is analytical-descriptive with a comparative approach in which the legal systems of Iran and Europe are compared. The research findings show that technical solutions, including the design of self-destructing smart contracts, data hashing, and off-chain storage of sensitive information, can mitigate this conflict to some extent. From a legal perspective, strategies such as data segregation, including explicit terms in contracts, and developing blockchain-specific regulatory frameworks have been proposed. Finally, this research emphasizes the need for interdisciplinary collaboration to achieve a balance between individual privacy and the integrity of blockchain technology.

Keywords: Right to be Forgotten, Public Blockchain, Data Privacy, Immutability, EU General Data Protection Regulation.

Received: 2025/09/23 - Review: 2025/10/22 - Accepted: 2025/12/16

ارجاع:
قاسم زاده ده آبادی، عارفه؛ (۱۴۰۴)، حق فراموش شدن و آثار آن بر روابط قراردادی در بلاکچین‌های عمومی؛ تحلیل تطبیقی حریم خصوصی داده‌ها در حقوق ایران و اروپا، تمدن حقوقی، شماره ۲۵.

مقدمه

تضاد ذاتی بین «حق فراموش شدن» به‌عنوان یک حق بنیادین در حریم خصوصی داده‌ها و «جاودانگی دیجیتال» ناشی از تغییرناپذیری و شفافیت در بلاکچین‌های عمومی، یک چالش اساسی و پیچیده در عصر فناوری‌های غیرمتمرکز ایجاد کرده است. از یک سو، مقرراتی مانند مقررات عمومی حفاظت از داده‌ها در اتحادیه اروپا و قوانین نوپای حفاظت از داده در ایران، به افراد حق درخواست حذف داده‌های شخصی را می‌دهند و از سوی دیگر، بلاکچین‌های عمومی به‌عنوان یک دفتر کل توزیع شده، با ویژگی تغییرناپذیری ذاتی، امکان حذف یا اصلاح داده‌های ثبت شده را نمی‌دهند. این تعارض به‌ویژه در حوزه روابط قراردادی مبتنی‌بر قراردادهای هوشمند که داده‌های شخصی در مراحل مختلف قرارداد در بلاکچین ثبت می‌شوند، آثار عمیقی بر جای می‌گذارد و پرسش‌های حقوقی، فنی و اخلاقی متعددی را درباره صحت، اجرا و انحلال قراردادها، مسئولیت‌پذیری و حفاظت از حریم خصوصی ایجاد می‌کند.

در بررسی پیشینه پژوهش، مطالعات متعددی در حوزه حقوق فناوری اطلاعات، بلاکچین و حریم خصوصی در سطح جهان انجام شده است. در اتحادیه اروپا، با تصویب مقررات عمومی حفاظت از داده‌ها و رأی دیوان دادگستری اتحادیه اروپا در پرونده گونزالس علیه گوگل، حق فراموش شدن به رسمیت شناخته شد و چالش‌های اجرای آن در محیط‌های دیجیتال مورد بررسی قرار گرفت. در ایران، اگرچه

قانون مشخصی تحت عنوان «حق فراموش شدن» وجود ندارد، اما لایحه حمایت از داده‌های شخصی مصوب ۱۴۰۰ و قوانین پراکنده‌ای مانند قانون جرائم رایانه‌ای مصوب ۱۳۸۸، تا حدی به جنبه‌های مرتبط با حریم خصوصی داده‌ها پرداخته‌اند. همچنین، در حوزه فقه، قواعدی مانند لاضرر، لایبطل و نفی سبیل به‌عنوان مبانی احتمالی این حق مورد استناد قرار گرفته‌اند. تحقیقات تطبیقی نشان می‌دهند که اگرچه چهارچوب‌های حقوقی ایران و اروپا از نظر سطح بلوغ و صراحت متفاوت هستند، اما هر دو با چالش مشترک سازگاری فناوری‌های غیرمتمرکز با قوانین حفاظت از داده روبرو می‌باشند.

پرسش‌های اصلی این پژوهش حول چهار محور اصلی شکل می‌گیرد: نخست، ماهیت حق فراموش شدن در حقوق ایران و اروپا به‌ویژه در مقررات عمومی حفاظت از داده‌های اتحادیه اروپا و تفاوت‌ها و شباهت‌های آن؛ دوم، آثار تغییرناپذیری ذاتی بلاچین‌های عمومی بر اجرا، صحت و انحلال روابط قراردادی؛ سوم، چگونگی تحلیل تعارض بین حق فراموش شدن و تغییرناپذیری بلاکچین در چهارچوب حقوقی ایران و اروپا؛ و چهارم، راهکارهای فنی و حقوقی برای کاهش این تعارض. فرضیه‌های این پژوهش بر این پایه استوارند که حق فراموش شدن در حقوق اروپا به‌صورت صریح و مستقل تعریف شده، درحالی‌که در حقوق ایران این حق به‌طور غیرمستقیم و در چهارچوب قوانین پراکنده و اصول فقهی مورد اشاره قرار گرفته است. همچنین تغییرناپذیری بلاکچین‌های عمومی، اجرای کامل حق فراموش شدن را غیرممکن ساخته و بر صحت، اجرا و انحلال روابط قراردادی تأثیر منفی می‌گذارد. علاوه بر این، تحلیل تعارض بین حق فراموش شدن و تغییرناپذیری بلاکچین نیازمند اتخاذ رویکردی تطبیقی و بین رشته‌ای در هر دو نظام ایران و اروپا است و در نهایت راهکارهای فنی و حقوقی می‌توانند تا حدی این تعارض را کاهش دهند.

هدف اصلی این پژوهش، تحلیل تطبیقی تعارض بین حق فراموش شدن و تغییرناپذیری بلاکچین‌های عمومی و ارائه راهکارهای حقوقی و فنی برای کاهش این تعارض در چهارچوب حقوق ایران و اروپا است. اهداف فرعی شامل تبیین ماهیت و دامنه حق فراموش شدن در حقوق ایران و اروپا، بررسی آثار تغییرناپذیری بلاکچین بر مراحل مختلف رابطه قراردادی، تحلیل راهکارهای موجود و پیشنهاد راهکارهای نوین برای ایجاد تعادل بین حریم خصوصی و یکپارچگی داده‌ها و در نهایت ارائه پیشنهاداتی به قانونگذاران، توسعه‌دهندگان و محققان می‌شود.

این پژوهش با روش تحلیلی-توصیفی و با رویکرد تطبیقی انجام شده و داده‌ها با استفاده از مطالعه کتابخانه‌ای و تحلیل قوانین، مقررات، آرای قضایی، مقاله‌های علمی و منابع معتبر فارسی و لاتین گردآوری شده‌اند. بااین‌حال، این پژوهش با محدودیت‌هایی از جمله کمبود منابع فارسی و پژوهش‌های داخلی در حوزه تعامل بلاکچین و حق فراموش شدن، پیچیدگی و نوپایی فناوری بلاکچین و عدم شفافیت کامل در برخی از جنبه‌های فنی و همچنین عدم تصویب نهایی برخی قوانین مرتبط در ایران روبرو بوده است. این چهارچوب به‌صورت به هم پیوسته، اساس تحلیلی منسجم و جامعی برای بررسی یکی از چالش برانگیزترین تقابل‌های عصر دیجیتال را فراهم می‌کند.

۱- مفاهیم پایه

۱-۱- بلاکچین عمومی: تعریف، ویژگی‌ها

بلاکچین عمومی به‌عنوان یک فناوری ذخیره‌سازی و انتقال اطلاعات به‌صورت غیرمتمرکز و شفاف عمل می‌کند که بدون نیاز به یک دستگاه کنترل مرکزی، امکان انتقال داده از نقطه الف به نقطه ب را فراهم می‌آورد. این سیستم یک پایگاه داده توزیع شده است که تاریخچه تمام مبادلات بین کاربران خود را از زمان ایجادش ثبت می‌کند و توسط کاربران مختلف و بدون واسطه به اشتراک گذاشته می‌شود. در بلاکچین عمومی، هریک از شرکت کنندگان می‌توانند آن را بخوانند و برای انجام تراکنش‌ها استفاده کنند و همچنین همه می‌توانند در فرایند ایجاد اجماع [۱] مشارکت داشته باشند. در این سیستم هیچ ثبت مرکزی یا شخص ثالث معتمد وجود ندارد و حکمرانی آن بر اساس فلسفه قانون، شکل گرفته که از جنبش منبع باز سرچشمه می‌گیرد.

ویژگی کلیدی بلاکچین عمومی استفاده از مکانیزم اثبات کار [۲] است که در آن ماینرها با صرف توان محاسباتی و انرژی، صحت تراکنش‌ها را تأیید و بلوک‌های جدیدی به زنجیره اضافه می‌کنند و در ازای آن با ارزهای جدید [۳] و کارمزد تراکنش‌ها پاداش می‌گیرند. این سیستم بر پایه رمزاقتصاد [۴] کار می‌کند که

1- consensus
2- Proof-of-Work
۳- مثل بیت‌کوین
4- cryptoeconomics

ترکیبی از مشوق‌های اقتصادی و مکانیزم‌های تأیید مبتنی‌بر رمزنگاری است. همچنین، هر بلاکچین عمومی لزوماً با یک سکه یا توکن کار می‌کند. از نمونه‌های موفق بلاکچین عمومی می‌توان به بیت‌کوین و اتریوم اشاره کرد. در نهایت، بلاکچین عمومی به‌عنوان یک سیستم مقاوم و انعطاف پذیر شناخته می‌شود که امنیت آن وابسته به این است که هیچ نهاد متخاصمی بیش از نیمی از قدرت محاسباتی شبکه را در اختیار نداشته باشد.

بلاکچین عمومی به‌عنوان یک رسانه پخش عمومی تأیید شده [۵] عمل می‌کند که در آن همه گره‌ها می‌توانند پیام‌ها را ببینند و از یک سیستم کلید عمومی [۶] برای احراز هویت استفاده می‌کنند. علاوه بر این، بلاکچین عمومی به‌عنوان یک مکانیسم همگام‌سازی نیز عمل می‌کند که در آن همه گره‌ها از شماره بلاک جاری آگاه هستند و پیام‌های ارسالی در دور i حداکثر تا دور $i+\delta$ به همه می‌رسند (Benhamouda et al.2020,7).

ویژگی‌های اصلی بلاکچین عمومی شامل مقیاس‌پذیری، عمومی بودن، قابلیت اعتماد بدون نیاز به اعتماد به شخص ثالث و مقاومت در برابر حمله مهاجم متحرک است. در این معماری، برای دستیابی به مقیاس‌پذیری، کارها به کمیته‌های کوچک واگذار می‌شود تا حجم محاسبات و ارتباطات به جای آن که به تعداد کل گره ها[۷] وابسته باشد، تنها به اندازه ثابتی از پارامتر امنیتی[۸] وابسته باشد (Benhamouda et al.2020,2).

بلاکچین عمومی که با نام‌های بلاکچین بدون مجوز نیز شناخته می‌شود، نوعی از بلاکچین است که در آن هر فردی می‌تواند بدون نیاز به دریافت مجوز از نهاد مرکزی، در شبکه مشارکت کند. این مشارکت شامل فعالیت‌هایی مانند ایجاد و اعتبارسنجی بلوک‌ها، تغییر وضعیت زنجیره از طریق تراکنش‌ها و دسترسی به داده‌های ذخیره شده در بلاکچین است. به عبارت دیگر، وضعیت بلاکچین و تمام تراکنش‌های آن برای همگان شفاف و قابل مشاهده است. این ویژگی اگرچه باعث افزایش اعتماد می‌شود، اما در مواردی که حریم خصوصی داده‌ها باید حفظ شود، می‌تواند چالش بر انگیز باشد (Ferdous et al.2021,4).

5- authenticated broadcast channel
6- PKI
7- N
8- λ

۱-۲- قرارداد هوشمند؛ تعریف، نحوه اجرا و جایگاه آن در تشکیل و اجرای قراردادها

قرارداد هوشمند به‌عنوان یک پروتکل کامپیوتری تعریف می‌شود که شرایط یک توافق را به‌صورت خودکار و بدون نیاز به واسطه اجرا می‌کند. این ایده نخستین بار در دهه ۱۹۹۰ میلادی توسط نیک سابو مطرح شد و امروزه با بهره‌گیری از فناوری بلاکچین، امکان تحقق بازار همتا به همتا را فراهم کرده است. قراردادهای هوشمند در واقع به‌صورت کدهای کامپیوتری نوشته شده و در بستر بلاکچین ذخیره، تکثیر و به روزرسانی می‌شوند (Zheng et al.2020,12).

فرایند تشکیل و اجرای قراردادهای هوشمند در چهار مرحله اصلی صورت می‌پذیرد: ایجاد، استقرار، اجرا و تکمیل. در مرحله ایجاد، طرفین قرارداد پس از مذاکره و توافق، مفاد قرارداد را به کمک وکلاء یا مشاوران تهیه کرده و سپس برنامه نویسان، این توافقنامه را به یک قرارداد هوشمند مبتنی‌بر زبان‌های برنامه نویسی تبدیل می‌کنند. پس از آن، در مرحله استقرار، قرارداد تأیید شده در پلتفرم بلاکچین مستقر می‌شود و دارایی‌های دیجیتال طرفین در کیف پول‌های مربوطه مسدود می‌گردد. در مرحله اجرا، قرارداد به‌صورت خودکار و در پاسخ به تحقق شرایط از پیش تعریف شده، اجرا می‌شود. هر اجرا به‌صورت یک تراکنش در بلاکچین ثبت و توسط ماینرها تأیید می‌شود. در نهایت، با تکمیل قرارداد، وضعیت جدید طرفین به روزرسانی و دارایی‌ها انتقال می‌یابند (Zheng et al.2020,34).

جایگاه قراردادهای هوشمند در مقایسه با قراردادهای سنتی، با مزایایی همچون کاهش ریسک، کاهش هزینه‌های اداری و خدمات و بهبود کارایی فرایندهای کسب و کار همراه است. این امر ناشی از غیرمتمرکز بودن، تغییرناپذیری و شفافیت بلاکچین است. برای مثال، در یک فرایند زنجیره تأمین، پرداخت‌ها بلافاصله پس از دریافت کالا توسط خریدار به‌صورت خودکار انجام می‌شود (Zheng et al.2020,2).

بااین‌حال، قراردادهای هوشمند با چالش‌های متعددی در هریک از مراحل چرخه حیات خود روبرو هستند. برای نمونه، در مرحله ایجاد، مسائلی مانند خوانایی کد، مسائل عملکردی مانند آسیب‌پذیری بازفراخوانی و هزینه‌های اضافی مطرح است (Zheng et al.2020,6). در مرحله استقرار، صحت قرارداد و کنترل جریان پویا از جمله چالش‌های اصلی به شمار می‌روند (Zheng et al.2020,7). در مرحله اجرا نیز مسائلی مانند وابستگی به ترتیب تراکنش‌ها و کارایی اجرا نیاز به توجه دارند. در نهایت، در مرحله تکمیل، نگرانی‌های مربوط به حریم خصوصی، امنیت و کلاهبرداری مطرح می‌شوند (Zheng et al.2020,9).

برای غلبه بر این چالش‌ها، راهکارهای متعددی ارائه شده است؛ از جمله استفاده از ابزارهای تحلیل کد، روش‌های یادگیری ماشین برای تشخیص آسیب‌پذیری‌ها و معماری‌های حفظ حریم خصوصی، همچنین پلتفرم‌های مختلفی مانند اتریوم و... هریک با ویژگی‌های منحصر به فرد، به توسعه و اجرای قراردادهای هوشمند می‌پردازند. به‌طورکلی جایگاه قراردادهای هوشمند در تشکیل و اجرای قراردادها را می‌توان از دو منظر کلان بررسی کرد: از یک سو، این فناوری امکان ایجاد و اجرای توافقات قابل اتوماسیون و اجرا را بدون اتکاء به واسطه‌های سنتی فراهم می‌کند که این امر می‌تواند هزینه‌های معاملاتی را کاهش داده و سرعت و شفافیت را افزایش دهد. از سوی دیگر، توسعه و اجرای قراردادهای هوشمند در حال حاضر با چالش‌های متعددی روبرو است شد و دقیقاً جایگاه کنونی آن را تحت تأثیر قرار داده است.

۱-۳- حریم خصوصی داده‌ها؛ تعریف و سطوح مختلف آن

حریم خصوصی اطلاعات به‌عنوان حق کنترل چگونگی جمع‌آوری و استفاده از اطلاعات شخصی تعریف می‌شود. این مفهوم در طول چرخه حیات کلان داده‌ها از مرحله تولید و ذخیره‌سازی تا پردازش مطرح می‌شود. در مرحله تولید داده، حریم خصوصی به دو شکل فعال[۹] و غیرفعال[۱۰] ظهور می‌یابد. در این مرحله، با محدود کردن دسترسی یا تحریف داده‌ها، از افشای اطلاعات حساس جلوگیری می‌شود (Jain et al.2016,6).

در مرحله ذخیره سازی، حریم خصوصی عمدتاً از طریق مکانیزم‌های رمزنگاری مانند رمزنگاری مبتنی‌بر هویت، رمزنگاری مبتنی‌بر ویژگی و رمزنگاری مسیر ذخیره‌سازی تأمین می‌شود. همچنین با استفاده از ابرهای ترکیبی[۱۱]، داده‌های حساس در محیط خصوصی نگهداری می‌شوند. در این مرحله، ابعاد حریم خصوصی شامل محرمانگی، یکپارچگی و در دسترس بودن داده‌ها است (Jain et al.2016,6). در مرحله پردازش داده، حریم خصوصی از طریق روش‌هایی مانند «انتشار داده با حفظ حریم خصوصی» و تکنیک‌های ناشناس‌سازی پیگیری می‌شود. این روش‌ها با کاهش دقت نمایش داده‌ها، تعادلی بین حریم خصوصی و کارایی تحلیل‌ها ایجاد می‌کنند. برای مثال، k ناشناسی تضمین می‌کند که هر رکورد در بین حداقل k رکورد دیگر غیرقابل تشخیص باشد (Jain et al.2016,10).

۹- اراده مند

۱۰- ناخواسته

11- Hybrid Clouds

یکی از چالش‌های اصلی، حفظ حریم خصوصی در عین انجام تحلیل‌های پیچیده است. برای این منظور، روش‌های جدیدی مانند «حریم خصوصی تفاضلی» مطرح شده‌اند که از الگوریتم‌هایی مانند «پنهان کردن سوزن در انبار کاه» برای حفظ حریم در استخراج قواعد ارتباطی استفاده می‌شود (Jain et al.2016,15). به‌طورکلی، حریم خصوصی در کلان‌داده‌ها نه‌تنها به معنای محافظت از هویت افراد، بلکه شامل محافظت از محتوای داده‌ها، تراکنش‌ها و جلوگیری از افشای غیرمجاز در تمامی مراحل چرخه حیات داده است. این امر مستلزم به کارگیری ترکیبی از راهبردهای فنی، مدیریتی و قانونی است تا بین بهره‌وری داده و حریم خصوصی افراد تعادل برقرار شود.

۱-۴- حق فراموش شدن؛ تعریف، مبانی و دامنه شمول

حق فراموش شدن به‌عنوان حقی برای افراد تعریف می‌شود که طبق آن می‌توانند درخواست حذف یا توقف پردازش داده‌های شخصی خود را هنگامی که این داده‌ها دیگر برای اهداف مشروع ضرورتی ندارند، مطرح کنند. این حق در پاسخ به تغییر «پیش‌فرض فراموشی» به «پیش‌فرض به‌خاطرسپاری» در عصر دیجیتال مطرح شده است (Ausloos,2012,3).

مبانی این حق را می‌توان در چند محور اصلی جست‌وجو کرد: افزایش کنترل فرد بر داده هایش؛ در محیطی که داده‌های شخصی به «ارز رایج» تبدیل شده‌اند، این حق به فرد امکان می‌دهد تا کنترل مؤثرتری بر هویت و اطلاعات خود داشته باشد. نارسایی چهارچوب فعلی رضایت؛ نظام رضایت کنونی در عمل ناکارآمد است؛ سیاست‌های حریم خصوصی مبهم هستند و افراد اغلب به دلیل وابستگی به سرویس‌ها، انتخاب واقعی ندارند. پویایی مفهوم داده شخصی؛ داده‌ها در بسترهای مختلف و در طول زمان ممکن است معنای متفاوتی پیدا کنند. حق فراموش شدن امکان بازبینی و بازتعریف مداوم استفاده از داده‌ها را فراهم می‌کند. جبران قدرت نابرابر: این حق می‌تواند توازن قدرت بین «افراد» و «کنترل‌کنندگان داده» را تا حدی بازگرداند (Ausloos,2012,9).

بااین‌حال، این حق با چالش‌های متعددی روبرو است: محدودیت دامنه: تنها در مواردی قابل اعمال است که فرد به پردازش داده‌ها رضایت داده باشد و شامل مواردی که داده‌ها به‌طور قانونی بدون رضایت جمع‌آوری شده‌اند، نمی‌شود. سانسور پنهان: ممکن است به حذف اطلاعاتی بی‌انجامد که از منظرعمومی دارای اهمیت هستند و با آزادی بیان و حق دسترسی به اطلاعات در تعارض قرار گیرد. دشواری‌های فنی

و عملی: پیاده‌سازی این حق در محیطی که داده‌ها به سرعت تکثیر و گاه «ناشناس‌سازی» می‌شوند، بسیار پیچیده است. توهم انتخاب: ممکن است صرفاً بار مسئولیت را به دوش فرد گذاشته و او را با این تصور که کنترل کامل دارد، فریب دهد (Ausloos,2012,8).

پیشنهاد شده است که؛ حق فراموش شدن به مواردی محدود شود که فرد رضایت خود را به پردازش داده‌ها داده است. همچنین، باید «استثنای منافع عمومی» در نظر گرفته شود تا در مواردی که حفظ داده‌ها به نفع عموم است[۱۲]، امکان رد درخواست حذف وجود داشته باشد. به علاوه، این حق باید شامل داده‌های منتقل‌شده به اشخاص ثالث نیز بشود، مگر آن که شخص ثالث بدون اقدام فعال کنترل‌کننده اصلی، داده را کپی کرده باشد. حق فراموش شدن در صورت تعریف دقیق و محدود، می‌تواند ابزاری مؤثر برای افزایش کنترل افراد بر داده‌های شخصی در عصر دیجیتال باشد. بااین‌حال، باید بااحتیاط و در چهارچوبی متعادل با سایر حقوق اساسی مانند آزادی بیان و منافع عمومی پیاده‌سازی شود تا به ابزاری برای سانسور یا توهم کنترل تبدیل نشود (Ausloos,2012,17).

۲- تحلیل تطبیقی حق فراموش شدن در حقوق ایران و اروپا

۲-۱- حق فراموش شدن در حقوق اروپا

در اتحادیه اروپا، حق فراموش شدن، ابتدا در سخنرانی ویویان ردینگ در سال ۲۰۱۰ میلادی مطرح شد و پس از آن در ماده‌های ۱۷ و ۱۸ «پیشنهاد مقرره حفاظت از داده ها» در سال ۲۰۱۲ میلادی گنجانده شد. پس از رأی دیوان دادگستری اتحادیه اروپا در پرونده ماریو کاستخا گونزالس در سال ۲۰۱۴ میلادی، این حق به رسمیت شناخته شد و نهایتاً در ماده ۱۷ مقررات عمومی حفاظت از داده‌ها [۱۳] که در مه ۲۰۱۸ میلادی لازم الاجرا شد، تحت عنوان «حق پاکسازی» [۱۴] تثبیت گردید (Stainforth,2022,8).

بر اساس ماده ۱۷ مقررات عمومی حفاظت از داده‌های اتحادیه اروپا افراد می‌توانند درخواست پاکسازی داده‌های شخصی خود را از کنترل‌کننده داده ارائه دهند. شرایط اعمال این حق شامل مواردی است که داده‌ها دیگر برای هدف اولیه جمع‌آوری لازم نباشند، فرد رضایت خود را پس بگیرد، دوره

۱۲- مانند اطلاعات مرتبط با سلامت یا امنیت

13- GDPR

14- Right to Erasure – RE

نگهداری داده به پایان رسیده باشد، فرد به پردازش داده اعتراض کند، یا پردازش داده با مقررات دیگر مغایرت داشته باشد. همچنین در مورد داده‌هایی که در دوران کودکی فرد منتشر شده‌اند نیز این حق قابل اعمال است (Stainforth,2022,7).

بااین‌حال، این حق مطلق نیست و استثنائاتی دارد. بر اساس ماده ۱۷، حق پاکسازی در مواردی که داده‌ها برای اعمال آزادی بیان و اطلاعات، اجرای وظایف قانونی، تحقق اهداف منافع عمومی، اهداف پژوهشی یا آماری، یا برای اثبات، اجرا یا دفاع از ادعاهای حقوقی لازم باشند، قابل اعمال نیست. این استثنائات نشان می‌دهد که توازن بین حق فراموشی و سایر ارزش‌های عمومی مانند شفافیت و آزادی بیان در نظر گرفته شده است .مسئولیت اجرای این حق بر عهده «کنترل‌کننده داده» است که طبق دستورالعمل حفاظت از داده‌های ۱۹۹۵ میلادی، شخص یا نهادی است که هدف و وسایل پردازش داده‌های شخصی را تعیین می‌کند. در رأی کاستخا گونزالس، دیوان دادگستری اتحادیه اروپا گوگل را به‌عنوان کنترل‌کننده داده در نظر گرفت و آن را ملزم به حذف داده‌های مرتبط از فهرست نتایج جست‌وجو کرد. البته این حذف به معنای پاکسازی کامل از اینترنت نیست، بلکه به‌صورت «حذف از فهرست» است که دسترسی به اطلاعات را دشوار می‌سازد (Stainforth,2022,8).

بااین‌حال، این مقررات با چالش‌هایی در عمل روبرو بوده است؛ از جمله تفسیر محدود گوگل از این حق که تنها در دامنه‌های اروپایی اعمال شد و نه به‌صورت جهانی که منجر به جریمه‌هایی از سوی مقامات فرانسوی شد. همچنین، شک‌هایی وجود دارد که آیا چنین حقوقی واقعاً می‌توانند در برابر شیوه‌های گسترده جمع‌آوری داده توسط شرکت‌هایی مانند گوگل مؤثر باشند؟ به‌طورکلی، اگرچه حق فراموش شدن گامی مهم در جهت محافظت از حریم خصوصی در عصر دیجیتال است، اما هنوز در عمل با محدودیت‌هایی در مقابله با اکولوژی پیچیده حافظه بالقوه و پردازش داده‌ها روبرو است (Stainforth,2022,11).

ابهام در تعیین مرز بین حق فراموش شدن و آزادی بیان نیز از دیگر مشکلات جدی است. ماده ۸۵ این مقررات به کشورهای عضو اجازه می‌دهد تا با وضع مقررات داخلی، موازنه بین این دو حق را برقرار کنند، اما این امر منجر به ناهمگونی در سطح اروپا شده و وحدت رویه را مخدوش کرده است. مسئولیت اجرای این حق بر عهده کنترل‌کننده داده‌ها است. کنترل‌کننده موظف است با در نظر گرفتن فناوری‌های موجود و

هزینه‌های اجرایی، اقدامات معقولی را برای حذف داده‌ها انجام دهد. این شامل اطلاع‌رسانی به سایر کنترل‌کننده‌هایی که داده‌های شخصی را پردازش می‌کنند نیز می‌شود. در زمینه یادگیری ماشین، اجرای این حق پیچیده‌تر است، زیرا مدل‌های یادگیری ماشین ممکن است به‌طور عمدی یا غیرعمدی داده‌های شخصی را در خود حفظ کنند[۱۵]، حتی پس از حذف از مجموعه داده آموزشی (Juliussen et al.2023,9).

در نهایت، اگر مدل یادگیری ماشین به گونه‌ای باشد که بتوان از طریق آن به داده‌های شخصی دست یافت[۱۶]، بازآموزی کامل مدل برای رعایت ماده ۱۷ ضروری خواهد بود. در غیر این صورت، در صورت عدم شواهد مبنی برشناسایی‌پذیری از طریق مدل، روش‌های تقریبی می‌توانند کافی باشند. این رویکرد انعطاف پذیر، هم‌زمان با حفظ حقوق اساسی افراد، به پیشرفت فناوری‌های نوین مانند یادگیری ماشین نیز کمک می‌کند (Juliussen et al.2023,11).

مسئولیت کنترل‌کننده داده‌ها[۱۷] در قبال این حق، انجام یک «تست موازنه» دقیق بین حقوق متعارض است. کنترل‌کننده باید مواردی مانند نقش داده‌ها در یک بحث عمومی، میزان شهرت فرد، روش جمع‌آوری داده‌ها و پیامدهای افشای داده‌ها را بسنجد. برای نمونه، آرشیوهای دولتی که حاوی داده‌های حساس شخصی[۱۸] هستند، موظفند ضمن رعایت حریم خصوصی، به‌ویژه برای افراد درگذشته[۱۹]، امکان دسترسی برای اهداف پژوهشی و تاریخی را نیز فراهم کنند. در عمل، این به معنای آن است که کنترل‌کننده باید درخواست حذف را بر اساس معیارهای عینی و با در نظر گرفتن منافع عمومی ارزیابی کند و صرف درخواست فرد برای حذف داده‌ها به معنای اجرای فوری آن نیست (Čtvrtník,2023,129).

۲-۲- جایگاه حق فراموش شدن در حقوق ایران

حق بر فراموش شدن به‌عنوان حقی که به افراد اجازه می‌دهد داده‌های شخصی مرتبط با گذشته خود را که ممکن است منجر به قضاوت ناعادلانه یا ممانعت از بازسازی اجتماعی شود، از فضای مجازی حذف

۱۵- حفظ ناخواسته

۱۶- نشت داده

۱۷- مانند آرشیوها

۱۸- مانند سوابق پزشکی یا پرونده‌های قضایی

۱۹- حفاظت پس از مرگ

کنند، در سال‌های اخیر به‌ویژه در اتحادیه اروپا از طریق «مقررات عمومی حفاظت از داده» به رسمیت شناخته شده است. بااین‌حال، در حقوق ایران، اگرچه قوانین پراکنده‌ای وجود دارد که به جنبه‌هایی از این حق اشاره می‌کند، اما هیچ متن قانونی صریح و مستقلی تحت عنوان «حق بر فراموش شدن» به تصویب نرسیده است (خوبیاری، ۱۴۰۳، ۶).

در حقوق ایران، نزدیک‌ترین متن قانونی به حق بر فراموش شدن، لایحه حمایت از داده‌های شخصی مصوب ۱۴۰۰ است. این قانون در ماده ۱۵ به «حق حذف داده ها» اشاره کرده و شرایطی را برای درخواست حذف داده‌های شخصی مقرر می‌دارد. بر این اساس، افراد می‌توانند در مواردی مانند عدم رضایت، تحقق هدف پردازش، یا نقض قانون درخواست حذف داده‌های خود را ارائه دهند. این ماده تا حدی با ماده ۱۷ مقررات عمومی حفاظت از داده‌های اتحادیه اروپا که به صراحت به «حق بر فراموش شدن» می‌پردازد، همسو است. بااین‌حال، تفاوت ماهوی در این است که در مقررات اخیرالذکر این حق به‌عنوان یک حق مستقل و گسترده شناخته شده، درحالی‌که در قانون ایران بیشتر در چهارچوب حق حذف داده و با شرایط محدودکننده‌تر مطرح شده است.

در غیاب قانون خاص، می‌توان به اصل بیست و دوم قانون اساسی جمهوری اسلامی ایران که حریم خصوصی را محترم شمرده و اصل بیست و پنجم که آزادی بیان را به رسمیت می‌شناسد، استناد کرد. این اصول می‌توانند مبنایی برای تعادل بخشی بین حق بر فراموش شدن و آزادی بیان باشند. همچنین، قانون جرائم رایانه‌ای مصوب ۱۳۸۸ با جرم انگاری افشای غیرقانونی داده‌های شخصی، تا حدی از حریم خصوصی در فضای مجازی حمایت کرده است. بااین‌حال، این قوانین عمدتاً در جهت جلوگیری از نشر غیرقانونی حرکت می‌کنند و نه الزاماً «حذف داده‌های قبلی» به درخواست فرد.

از منظر فقهی، قاعده لاضرر می‌تواند به‌عنوان یکی از مبانی احتمالی حق بر فراموش شدن مطرح شود؛ به این استدلال که باقی ماندن داده‌های قدیمی ممکن است موجب ضرر معنوی یا اجتماعی شود. بااین‌حال، ممکن است؛ جریان این قاعده در موارد تعارض با اصول دیگر مانند آزادی بیان محدود شود. وجوب تضمین حق فراموشی بر اساس قاعده «لایبطل دم امرء مسلم»[۲۰] نیز این گونه تحلیل می‌شود که این

۲۰- هدر نرفتن خون مسلمان

قاعده به‌عنوان مسئولیت حاکمیت در قبال حفظ جان، مال و عرض شهروندان معرفی شده است: «حفظ جان، مال و عرض شهروندان از وظایف اولیه حاکمیت و متقابلاً از حقوق عمومی آنان در مقابل تعدی و تجاوز متجاوزان و متخلفان است» (محقق داماد، ۱۳۹۹، ۲۱).

در تفسیر لفظ «دم» آمده است: «گستره قاعده بسیار وسیع است و ناظر به التزام و تکلیف دولت در حمایت از حق حیات با اعمال ضمانت اجراهای مربوطه در خصوص متجاوزان به حقوق انسانی فرد است» (محقق داماد، ۱۳۹۹، ۳۷-۴۰). امروزه حریم خصوصی داده‌ها و آبروی دیجیتالی افراد، از مصادیق روشن «عرض» و «حقوق انسانی فرد» محسوب می‌شوند. اگر اطلاعات شخصی در یک بلاکچین عمومی باعث هتک حرمت، اخاذی، ضرر مالی یا روانی شدید شود، این مصداق «اهدار عرض» و «تضییع حق» شهروند است. بنابراین، بر اساس این قاعده، حاکمیت اسلامی موظف است؛ با ایجاد سازوکارهای قانونی و فنی[۲۱]، از هدر رفتن حق و آبروی شهروند جلوگیری کند. در نتیجه حق فراموشی در این موارد نه‌تنها جایز، بلکه لازم الاجرا است.

نظر فقهی دیگر جواز یا حتی لزوم محدودسازی بر اساس قاعده «نفی سبیل» می‌باشد؛ مفاد کلی این قاعده عدم سلطه کافران بر مومنان است (محقق داماد، ۱۳۹۹، ۱۰-۱۲). ذخیره‌سازی داده‌های حساس و غیرقابل حذف شهروندان یک کشور اسلامی در بلاکچین‌های عمومی و بین‌المللی که کنترل آن در دست قدرت‌های غیرمسلمان یا رقبای سیاسی است، می‌تواند مصداق روشن «ایجاد سلطه» و «سبیل» باشد. این داده‌ها می‌تواند برای جاسوسی، فشار اقتصادی، تخریب شخصیت‌ها و ایجاد بحران اجتماعی مورد سوءاستفاده قرار گیرد. بنابراین، قاعده نفی سبیل، حاکمیت را موظف می‌کند تا از چنین سلطه‌ای جلوگیری کند. این می‌تواند به معنای ممنوعیت استفاده از چنین پلتفرم‌هایی برای داده‌های حساس یا توسعه بلاکچین‌های مستقل و داخلی باشد که در آن حق فراموشی قابل اجرا است. نتیجه در این چهارچوب، حق فراموشی یک ابزار برای نفی سبیل است (محقق داماد، ۱۳۹۹، ۱۵).

سومین نظر فقهی؛ منع حق فراموشی بر اساس قاعده لزوم وفای به عهود است. قبل از هر چیز باید توجه داشت که اصل یا قاعده لزوم وفای به عهد، امری کاملاً جدا از اصل یا قاعده لزوم عقد است (محقق داماد، ۱۳۹۹، ۴۷). اصل وفای به عهد، امری اعم از آن و گستره آن حقوق عمومی را نیز فرا می‌گیرد. ذات

۲۱- حتی اگر مستلزم طراحی بلاکچین‌های خاص باشد

و فلسفه فناوری بلاکچین، بر «تغییرناپذیری» و «وفاداری به تاریخچه تراکنش ها» استوار است. وقتی کاربری داوطلبانه در یک شبکه عمومی[۲۲] اقدام به ثبت داده می‌کند، این عمل می‌تواند نوعی عهد و پیمان ضمنی با کل شبکه برای «تغییرناپذیر ماندن آن داده» تلقی شود. در این صورت، می‌توان استدلال کرد که حق فراموشی و حذف داده، نقض این عهد و پیمان شبکه است. قاعده وفای به عهود، وفا به این تعهد ذاتی را واجب می‌شمارد. در نتیجه در این نگاه، حق فراموشی در بلاکچین‌های عمومی غیرمجاز است.

در خصوص تقدم قاعده «لا ضرر» و حل تعارض آن؛ بین نظر موافق[۲۳] و نظر مخالف[۲۴] تعارض پیش می‌آید. قاعده «لا ضرر» که از قواعد مسلم و اولیه فقه است، می‌گوید: «لَا ضَرَرَ وَلَا ضِرَارَ فِی الْإِسْلَام». هرگاه اجرای یک حکم[۲۵] منجر به ضرر واضح و غیرقابل تحملی برای فرد یا جامعه شود، این قاعده برای دفع آن ضرر وارد عمل می‌شود. بنابراین، اگر حفظ داده در بلاکچین برای فرد ضرر قابل توجه[۲۶] داشته باشد، قاعده لا ضرر بر قاعده وفای به عهود تقدم می‌یابد. در این حالت، حذف داده یا ایجاد مکانیزم برای آن، نه‌تنها جایز، بلکه واجب می‌شود. در نتیجه در موارد وجود ضرر، حق فراموشی مشروعیت می‌یابد.

با تلفیق این قواعد و با در نظر گرفتن ملاکات و اهداف شریعت در حفظ مصالح مردم، می‌توان گفت؛ حق فراموشی در بلاکچین، در مواردی که بقای داده‌ها منجر به ضرر واضح یا هتک عرض شود، بر اساس قواعد لایبطل و لا ضرر مشروع و لازم الرعایه است. البته تحقق این حق نیازمند تمهیدات فنی و حکومتی مانند توسعه بلاکچین‌ها یا استفاده از روش‌های رمزنگاری پیشرفته است تا هم حق افراد رعایت شود و هم اعتماد به سیستم خدشه دار نگردد. این تحلیل نشان می‌دهد که فقه پویای امامیه با ابزار قواعد فقه عمومی، توانایی استنباط احکام مسائل نوپدید را دارد.

۲۲- مثل بیت‌کوین یا اتریوم

۲۳- بر اساس لایبطل و نفی سبیل

۲۴- بر اساس وفای به عهود

۲۵- مانند وفای به عهد تغییرناپذیری

۲۶- مالی، جانی و آبرویی

۳- آثار حق فراموش شدن بر روابط قراردادی در بلاکچین‌های عمومی

۳-۱- ماهیت روابط قراردادی در بلاکچین

قراردادهای هوشمند به‌عنوان خوداجراگر[۲۷] در محیط غیرمتمرکز بلاکچین عمل می‌کنند و امکان اجرای خودکار شرایط توافق شده بین طرفین را بدون نیاز به واسطه فراهم می‌کنند. این ویژگی، قراردادهای هوشمند را از عقود سنتی متمایز می‌سازد، چرا که در قراردادهای سنتی اجرای تعهدات معمولاً نیازمند دخالت نهادهای مرکزی یا قانونی است، درحالی‌که در قراردادهای هوشمند، کد به‌صورت خودکار و بر اساس شرایط از پیش تعریف شده اجرا می‌شود. بااین‌حال، عبارت قرارداد هوشمند ممکن است گمراه‌کننده باشد، چرا که در واقع این قراردادها صرفاً کدهای کامپیوتری هستند که منطق از پیش تعریف شده را اجرا می‌کنند و لزوماً نمایانگر یک قرارداد قانونی نیستند. این مسئله نشان می‌دهد که ماهیت حقوقی قراردادهای هوشمند هنوز به‌طور کامل با چهارچوب‌های قراردادی سنتی تطبیق نیافته است (Taherdoost,2023,7).

در مورد داده‌های شخصی در قراردادهای هوشمند، باید توجه داشت که اگرچه بلاکچین به‌طور ذاتی از شفافیت و تغییرناپذیری برخوردار است، اما این ویژگی‌ها می‌تواند با مقررات حفاظت از داده‌ها مانند حق فراموش شدن در تضاد باشد. به‌عنوان مثال، آدرس کیف پول اگرچه به‌طور مستقیم هویت فرد را آشکار نمی‌کند، اما می‌تواند به‌عنوان یک‌شناسه[۲۸] در نظر گرفته شود که در صورت تحلیل رفتاری تراکنش‌ها، امکان‌شناسایی فرد وجود دارد. همچنین، شرایط قرارداد و تاریخچه تراکنش‌ها که در بلاکچین ثبت می‌شوند، ممکن است حاوی اطلاعاتی باشند که به‌طور غیرمستقیم به هویت افراد مرتبط شوند. ذخیره‌سازی تمام داده‌ها توسط تمامی اعضای شبکه، چالش‌های امنیت داده و حریم خصوصی را به همراه دارد، زیرا داده‌های ذخیره شده در بلاکچین را نمی‌توان به سادگی حذف کرد. این امر به‌ویژه در مواردی که داده‌ها دارای ماهیت شخصی هستند، می‌تواند با قوانینی مانند مقررات عمومی حفاظت از داده‌های اتحادیه اروپا در تعارض باشد. بنابراین، اگرچه قراردادهای هوشمند مزایای زیادی از جمله شفافیت و کاهش هزینه‌ها ارائه می‌دهند، اما مدیریت داده‌های شخصی در آن‌ها نیازمند راهکارهای فنی و حقوقی دقیق‌تری است تا بین حریم خصوصی افراد و یکپارچگی داده‌ها تعادل برقرار شود (Taherdoost,2023,7).

27- self-executing

۲۸- نیمه ناشناس

در سیستم‌های مبتنی‌بر فناوری‌های مدرن مانند دفاتر کل توزیع‌شده یا پایگاه‌های داده امن، داده‌ها اغلب به گونه‌ای طراحی شده‌اند که تغییرناپذیر باشند تا از دستکاری غیرمجاز جلوگیری شود. این ویژگی با هدف حفظ یکپارچگی و اصالت داده‌ها ایجاد شده است، اما اجرای حق فراموش شدن را با مشکل مواجه می‌کند. به‌عنوان مثال، در محیط‌های پژوهشی که از چهارچوب‌های برنامه نویسی توزیع‌شده استفاده می‌شود، حذف یا اصلاح داده‌ها بدون تأثیر بر سایر بخش‌های سیستم دشوار است. اجرای حق فراموش شدن در محیط‌های پژوهشی و فناورانه با چالش‌های فنی[۲۹]، اخلاقی[۳۰] و حاکمیتی[۳۱] روبرو است (Bala,2022,3).

به‌طورکلی، در واقع قراردادهای هوشمند با ایجاد تحولی اساسی در ماهیت اجرای تعهدات، رابطه قراردادی را از حالت سنتی خود خارج کرده‌اند. در قراردادهای سنتی، اجرای تعهدات همواره مبتنی‌بر اعتماد به نهادهای مرکزی مانند دادگاه‌ها، بانک‌ها یا دفاتر اسناد رسمی بود که نقش ضمانت اجرا و تفسیر قرارداد را ایفاء می‌کردند. اما در محیط غیرمتمرکز بلاکچین، قراردادهای هوشمند با حذف این واسطه‌ها، منطق قرارداد را در قالب کدهای خود اجرا پیاده‌سازی می‌کنند. این تحول اساسی، ماهیت رابطه قراردادی را به کلی دگرگون کرده و آن را از اعتماد به افراد و نهادها به سمت اعتماد به کد و ریاضیات سوق می‌دهد. نتیجه این تغییر، افزایش چشمگیر سرعت، کاهش هزینه‌های تراکنش و حذف خطر تقلب از سوی واسطه‌ها است.

بااین‌حال، این تحول اساسی با چالش‌های عمیقی همراه است که اصلی‌ترین آن مربوط به تعریف حقوقی قراردادهای هوشمند می‌باشد. در حقیقت این پرسش اساسی مطرح است که آیا کد کامپیوتری می‌تواند به‌عنوان یک قرارداد حقوقی شناخته شود؟ در حقوق قراردادهای سنتی، قصد و نیت طرفین برای تشکیل قرارداد امری ضروری محسوب می‌شود، درحالی‌که قرارداد هوشمند صرفاً بر اساس منطق از پیش تعریف شده و بدون توجه به قصد طرفین عمل می‌کند. علاوه بر این، دادگاه‌ها در سیستم سنتی در مواقع بروز اختلاف، امکان تفسیر قرارداد و در نظر گرفتن شرایط قهری را دارند، اما قرارداد هوشمند به‌صورت جبری و بدون امکان تعدیل اجرا می‌شود. همین امر موجب شده که این قراردادها لزوماً در چهارچوب

۲۹- مانند تغییرناپذیری

۳۰- تضاد با شفافیت

۳۱- عدم وضوح مسئولیت

حقوقی تعریف‌شده فعلی جای نگیرند و این ابهام می‌تواند در صورت بروز اختلافات پیچیده مانند وجود باگ در کد، به چالش‌های حقوقی جدی منجر شود.

یکی دیگر از چالش‌های بنیادین، تضاد ذاتی این فناوری با حریم خصوصی و قوانین مدرن حفاظت از داده است. شفافیت و تغییرناپذیری ذاتی بلاکچین که برای تضمین سلامت قرارداد ضروری به نظر می‌رسد، در تعارض مستقیم با قوانینی مانند حق فراموش شدن در مقررات عمومی حفاظت از داده‌های اتحادیه اروپا قرار می‌گیرد. ذخیره شدن دائمی تاریخچه تراکنش‌ها و شرایط قرارداد در بلاکچین، امکان اجرای حق حذف داده را به‌طور کامل سلب می‌کند. از سوی دیگر، اگرچه آدرس‌های کیف پول به‌صورت مستقیم هویت واقعی کاربران را فاش نمی‌کنند، اما این سیستم در حالت شبه ناشناس عمل می‌کند و با تحلیل رفتاری تراکنش‌ها می‌توان به هویت افراد پی برد. این امر حریم خصوصی طرفین قرارداد را در معرض تهدید جدی قرار می‌دهد و با اصول حفاظت از داده در تضاد است.

در ادامه این چالش‌ها، مسئله ابهام در حاکمیت و مسئولیت نیز نیاز به توجه دارد. در یک رابطه قراردادی سنتی، مسئولیت‌ها و مرجع حل اختلاف به وضوح مشخص است. اما در محیط غیرمتمرکز بلاکچین، هنگامی که یک قرارداد هوشمند اجرا می‌شود، هیچ نهاد مرکزی وجود ندارد که در صورت بروز خطا مسئول جبران خسارت باشد. همچنین، در یک شبکه جهانی و غیرمتمرکز، این ابهام وجود دارد که در صورت بروز اختلاف، کدام قانون و صلاحیت قضایی باید حاکم باشد. این عدم شفافیت در حاکمیت، به‌ویژه در محیط‌های پژوهشی بین‌المللی که تحت قوانین مختلفی عمل می‌کنند، تشدید می‌شود.

در جمع‌بندی نهایی می‌توان گفت که روابط قراردادی در بلاچین نمایانگر یک پارادایم کاملاً جدید است که در آن اجرا بر تفسیر کد بر متن اولویت دارد. این مدل جدید، با وجود مزایای انقلابی خود در زمینه شفافیت و کارایی، هنوز نتوانسته است با چهارچوب‌های حقوقی موجود، هنجارهای اجتماعی در مورد حریم خصوصی و نیاز به انعطاف‌پذیری در تعاملات انسانی همسو شود. برای این که این روابط به بلوغ لازم برسند، نیاز به توسعه راهکارهای فنی–حقوقی ترکیبی احساس می‌شود. راهکارهایی مانند طراحی قراردادهای هوشمند خصوصی برای داده‌های حساس، به کارگیری الگوریتم‌های رمزنگاری پیشرفته مانند محاسبات امن چندطرفه و تدوین چهارچوب‌های قانونی جدید که هم خوداجرایی کد را به رسمیت بشناسند و هم مکانیزم‌هایی برای حمایت از مصرف‌کننده و حریم خصوصی در نظر بگیرند. در

نهایت، به نظر می‌رسد قراردادهای هوشمند نه به‌عنوان جایگزین کامل قراردادهای سنتی، بلکه به‌عنوان یک ابزار تکمیلی قدرتمند در حوزه‌های خاصی که شفافیت و خودکارسازی در اولویت هستند، نقش آفرینی خواهند کرد.

۳-۲- آثار بر مراحل مختلف رابطه قراردادی

پیش از تشکیل قرارداد: الزام به حذف داده‌های مذاکرات اولیه را می‌توان این طور تحلیل کرد. در این مرحله، طرفین ممکن است داده‌های شخصی زیادی را در طول مذاکرات اولیه مبادله کنند.[۳۲] طبق ماده ۱۷ مقررات عمومی حفاظت از داده‌ها افراد حق دارند درخواست حذف این داده‌ها را در مواردی مانند عدم ضرورت داده برای هدف اولیه، لغو رضایت، یا پردازش غیرقانونی داشته باشند. چالش این مسئله در بلاکچین این است که؛ اگر داده‌های مذاکرات در یک بلاکچین ذخیره شده باشند، به دلیل تغییرناپذیری ذات این فناوری، حذف یا تغییر داده‌های قبلی تقریباً غیرممکن است. این ویژگی با حق فراموش شدن در تضاد مستقیم قرار می‌گیرد (Celador Angón,2024,5).

در حین اجرای قرارداد، درخواست حذف داده‌های شخصی در قرارداد هوشمند در بلاکچین، شرایط قرارداد را به‌صورت کدهای خوداجرا ذخیره می‌کنند که ممکن است حاوی داده‌های شخصی باشند.[۳۳] اصول مقررات عمومی حفاظت از داده‌ها ممکن است با بلاکچین ناسازگار باشد؛ زیرا این فناوری با شفافیت و تغییرناپذیری مشخص می‌شود؛ حق فراموش شدن نمی‌تواند در مورد بلاکچین اعمال شود، زیرا تغییر زنجیره داده‌ها غیرممکن است (Celador Angón,2024,17).

پرسشی که مطرح می‌شود این است که؛ چگونه می‌توان حق فراموش شدن را با عدم امکان تغییر زنجیره داده‌های بلاکچین هماهنگ کرد؟ راه‌حل‌های فنی مانند رمزگشایی کلیدهای رمزنگاری یا ذخیره داده‌ها در پایگاه داده خارجی پیشنهاد شده‌اند. پرسش دیگر این است که آیا حذف داده‌ها قرارداد را باطل می‌کند؟ اگر داده‌های شخصی بخشی از شرایط اساسی قرارداد باشند[۳۴]، حذف آن ممکن است اجرای قرارداد را غیرممکن کرده و به ابطال قرارداد منجر شود. بااین‌حال، اگر داده‌ها صرفاً جنبه فرعی داشته

۳۲- مانند ایمیل‌ها، پیشنهادها، مدارک‌شناسایی، سوابق مالی و...

۳۳- مانند نام، آدرس و اطلاعات پرداخت

۳۴- مانند هویت طرفین

باشند، ممکن است قرارداد بتواند بدون آن داده‌ها به اجرای خود ادامه دهد. همچنین، راه‌حل‌هایی مانند ذخیره‌سازی خارج از زنجیره را پیشنهاد شده؛ داده‌های حساس در پایگاه‌های داده متمرکز ذخیره شود و فقط یک هش از آن در بلاکچین ثبت شود (Celador Angón,2024,18).

در نهایت چگونه می‌توان اثبات کرد قراردادی منقضی شده درحالی‌که تمام آثار آن حذف شده است؟ اگر تاریخچه قرارداد به‌طور کامل حذف شود، اثبات انحلال قرارداد با مشکل مواجه خواهد شد. در این حالت، می‌توان از راهکارهای زیر استفاده کرد: ذخیره‌سازی اسناد خارج از زنجیره: نگهداری اسناد انحلال قرارداد در یک پایگاه داده متمرکز خارج از بلاکچین. استفاده از هش: ثبت هش اسناد انحلال در بلاکچین بدون افشای محتوای اصلی. این هش می‌تواند به‌عنوان مدرک غیرقابل انکار برای اثبات انحلال قرارداد استفاده شود. قراردادهای هوشمند با قابلیت انحلال: طراحی قراردادهای هوشمندی که به‌طور خودکار پس از انحلال، وضعیت منقضی شده را در بلاکچین ثبت می‌کنند (Goossens,2021,6).

این موارد نشان می‌دهند که استفاده از بلاک چین در قراردادهای هوشمند، اگرچه مزایای زیادی دارد، اما با چالش‌های جدی در زمینه حریم خصوصی و حفاظت از داده‌ها روبرو است و نیازمند طراحی دقیق و انطباق با قوانین موجود است.

۴- راهکارهای حقوقی و قراردادی

یکی از چالش‌های اصلی فناوری دفتر کل توزیع شده، عدم امکان تغییر یا حذف داده‌ها به دلیل ماهیت تغییرناپذیر آن است. این ویژگی با مقررات حفاظت از داده مانند مقررات عمومی حفاظت از داده‌های اتحادیه اروپا که حق حذف داده را به کاربران می‌دهد، در تعارض است. راهکار پیشنهادی، ذخیره داده‌های حساس در پایگاه‌های داده متمرکز خارج از زنجیره و تنها ثبت یک هش یاشناسه غیرقابل بازگشت در بلاکچین است. این روش علاوه بر حفظ یکپارچگی داده‌ها، امکان مدیریت داده‌های حساس را مطابق با قوانین حفاظت از داده فراهم می‌کند. در چهارچوب نظارتی، این رویکرد می‌تواند توسط سیستم‌های ممیزی مورد بررسی قرار گیرد تا اطمینان حاصل شود که داده‌های حساس به‌صورت ایمن و مطابق با استانداردهای تعیین شده مدیریت می‌شوند (Ellul et al.2020,10).

در صورت تعارض بین پیاده‌سازی فنی و توصیف متنی ارائه شده به کاربر، توصیف متنی مقدم خواهد بود. این اصل می‌تواند مبنایی برای گنجاندن شروط صریح در قراردادهای هوشمند یا قراردادهای الحاقی باشد که به کاربر حق درخواست حذف داده را می‌دهد و نحوه جبران خسارت ناشی از آن را مشخص می‌کند. در خصوص چالش‌های ناشی از عدم تمرکز و تغییرناپذیری و لزوم توسعه چهارچوب‌های حقوقی جدید برای مقابله با این چالش‌ها در مواردی که حریم خصوصی کاربران در تعارض با امنیت تراکنش‌ها یا مقررات ضدپولشویی قرار می‌گیرد، می‌توان از دکترین توازن مصالح استفاده کرد. این دکترین می‌تواند توسط مراجع قضایی یا نهادهای نظارتی برای تعیین حدود حقوق افراد و تکالیف ارائه دهندگان خدمات به کار رود. در گزارش اتحادیه اروپا نیز بر لزوم تعیین مسئولیت‌پذیری و ایجاد راهکارهای حقوقی برای مدیریت تعارض‌های ناشی از فناوری‌های غیرمتمرکز تأکید شده است (Ellul et al.2020,6).

با توجه به ماهیت غیرمتمرکز و تغییرناپذیر بلاکچین، ذخیره‌سازی تمام داده‌های حساس درون زنجیره می‌تواند به چالشی برای حریم خصوصی و انطباق با قوانین حفاظت از داده تبدیل شود. بلاکچین یک پایگاه داده توزیع شده است که در آن هر شرکت‌کننده حداقل بخشی از داده‌ها را نگهداری می‌کند. این ویژگی، حذف یا اصلاح داده‌ها را غیرممکن می‌سازد. ازاین‌رو، راهکار حقوقی پیشنهادی، تفکیک داده‌ها است، به این شکل که تنهاشناسه‌ها یا هش داده‌های حساس در بلاکچین ثبت شوند و خود داده‌ها در پایگاه‌های داده متمرکز و خارج از زنجیره ذخیره گردند. این روش نه‌تنها امکان مدیریت داده‌ها را فراهم می‌کند، بلکه با قوانینی مانند مقررات عمومی حفاظت از داده‌های اتحادیه اروپا نیز سازگارتر است (Deeva,2020,2).

قراردادهای هوشمند در حال حاضر در چهارچوب حقوق کلاسیک قراردادها قرار می‌گیرند، اما به دلیل خوداجرایی و برنامه‌ریزی شده بودن، ممکن است مفاهیم سنتی مانند «تعهد» و «عدم اجرا» به درستی بر آن‌ها منطبق نباشند. برای حل این مسئله، پیشنهاد می‌شود در قراردادهای هوشمند یا قراردادهای الحاقی مرتبط، شروط صریحی گنجانده شود که به کاربر حق درخواست حذف داده هایش را بدهد و همچنین نحوه جبران خسارت در صورت نقض حریم خصوصی یا عدم اجرای تعهدات به وضوح مشخص شود. این شروط می‌تواند شامل «شرایط فورس ماژور»، «تخلف از تعهدات جانبی» یا «حق فسخ قرارداد» باشد تا از انعطاف‌پذیری لازم در مواجهه با شرایط غیرمترقبه برخوردار شود (Deeva,2020,5).

در مورد تجربیات بین‌المللی در خصوه تنظیم‌گری بلاکچین برای مثال؛ تنظیم مقررات خاص[۳۵] یا الحاق مقررات به قوانین موجود.[۳۶] در روسیه نیز برنامه «اقتصاد دیجیتال» و طرح‌های قانونی مانند «دارایی‌های مالی دیجیتال» در دست تدوین است. بااین‌حال، برای حمایت از حریم خصوصی و حقوق کاربران، لازم است نهادهای تنظیم‌گر ویژه‌ای[۳۷] مقرراتی را برای پروژه‌های بلاکچینی تعیین کنند که شامل الزامات فنی[۳۸]، حقوقی[۳۹] و نظارتی باشد. این نهادها می‌توانند با همکاری مراجع استانداردسازی[۴۰] چهارچوب‌های امنیتی و حقوقی یکپارچه‌ای را ارائه دهند (Deeva,2020,5). راهکارهای پیشنهادی فوق به‌صورت یکپارچه و مکمل می‌توانند به ایجاد یک محیط حقوقی امن و قابل اعتماد برای توسعه فناوری بلاکچین و قراردادهای هوشمند کمک کنند. این راهکارها نه‌تنها به حفظ حریم خصوصی و حقوق کاربران می‌پردازند، بلکه با ایجاد وضوح حقوقی، بستر مناسبی برای توسعه اقتصادی و نوآوری در فضای دیجیتال فراهم می‌کنند.

نتیجه

تغییرناپذیری ذاتی و شفافیت بلاکچین‌های عمومی با ماهیت حق فراموش شدن که در قوانینی همچون مقررات عمومی حفاظت از داده‌های اتحادیه اروپا و تا حدی در حقوق ایران[۴۱] پیش‌بینی شده است، در تعارض اساسی قرار دارد. این تناقض، به‌ویژه در حوزه روابط قراردادی مبتنی‌بر قراردادهای هوشمند، چالش‌های حقوقی، فنی و اخلاقی متعددی را ایجاد کرده است. مطالعه تطبیقی نشان می‌دهد که اگرچه چهارچوب حقوقی اروپا با تصریح حق فراموش شدن در ماده ۱۷ مقررات عمومی حفاظت از داده‌های اتحادیه اروپا، گامی رو به جلو برداشته و رویه‌های اجرایی و استثنائات آن روشن‌تر است، اما در حقوق

۳۵- مانند چین
۳۶- مانند ایالات متحده آمریکا
۳۷- مانند مراجع حفاظت از داده
۳۸- مانند رمزنگاری و تفکیک داده
۳۹- مانند مسئولیت ناشی از نقض داده
۴۰- مانند مؤسسه ملی استاندارد
۴۱- با تأکید بر حق حذف داده

ایران این حق به‌صورت پراکنده و عمدتاً در قالب «حق حذف» در «لایحه حمایت از داده‌های شخصی» و با استناد به قواعد فقهی مانند «لاضرر»، «لایبطل» و «نفی سبیل» قابل استنباط است. بااین‌حال، هر دو نظام حقوقی با چالش مشترک اجرای این حق در محیط غیرمتمرکز و تغییرناپذیر بلاکچین مواجه هستند. هیچ‌یک از راهکارهای موجود اعم از فنی، حقوقی یا قراردادی به‌تنهایی قادر به حل کامل این تعارض نیست. بنابراین، راهبرد اصلی باید مبتنی‌بر کاهش تعارض و ایجاد توازن بین حریم خصوصی افراد و یکپارچگی داده‌ها باشد.

تعارض بین حق فراموش شدن و تغییرناپذیری بلاکچین‌های عمومی، پدیده‌ای پیچیده و چندبعدی است که تنها از طریق همکاری نهادهای قانونگذاری، توسعه دهندگان فناوری و جامعه علمی قابل مدیریت است. راه‌حل نهایی، نه حذف کامل یکی از این دو ارزش، بلکه ایجاد سازوکارهای هوشمندانه برای همزیستی آن‌ها در چهارچوبی متعادل و انعطاف پذیر است. در این مسیر، نظام حقوقی ایران می‌تواند با بهره‌گیری از ظرفیت‌های فقهی و هم افزایی با دستاوردهای جهانی، به الگویی اثرگذار در حوزه حکمرانی فناوری‌های غیرمتمرکز تبدیل شود.

پیشنهاد

پیشنهادات یکپارچه و عملی اول- به قانونگذاران و نهادهای تنظیم‌گر ایران: تدوین چهارچوب حقوقی خاص: الحاق ماده یا آیین نامه‌ای ویژه فناوری‌های دفترکل توزیع شده و قراردادهای هوشمند به قانون حمایت از داده‌ها، با در نظرگیری مفاهیمی چون «ذخیره‌سازی خارج از زنجیره» و «مسئولیت کنترل‌کنندگان داده». تعیین نهاد ناظر تخصصی: ایجاد یک مرجع تنظیمگر مستقل برای نظارت بر پروژه‌های بلاکچینی، تدوین استانداردهای فنی-حقوقی و انجام حسابرسی دوره ای. توسعه دکترین‌های حقوقی: ترویج استفاده از دکترین «توازن مصالح» در رویه قضایی برای ایجاد تعادل بین حریم خصوصی، شفافیت و امنیت.

دوم- به توسعه دهندگان، کسب و کارها و ارائه دهندگان خدمات بلاکچینی: رعایت اصل «حریم خصوصی از طریق طراحی». به‌کارگیری راهکارهای فنی مانند ذخیره‌سازی داده‌های حساس خارج از

زنجیره و ثبت تنها «هش» یاشناسه غیرقابل بازگشت در بلاکچین. استفاده از رمزنگاری پیشرفته[۴۲] و قراردادهای هوشمند خودتخریب‌گر برای داده‌های موقت. شروط قراردادی شفاف: گنجاندن بندهای صریح در قراردادهای هوشمند یا قراردادهای الحاقی مبنی بر حق درخواست حذف داده، شرایط فورس ماژور و شیوه‌های جبران خسارت.

ملاحظات اخلاقی: موارد مربوط به اخلاق در پژوهش و نیز امانتداری در استناد به متون و ارجاعات مقاله تماماً رعایت گردیده است.

تعارض منافع: تعارض منافع در این مقاله وجود ندارد.

تأمین اعتبار پژوهش: این پژوهش بدون تأمین اعتبار مالی نگارش یافته است.

منابع

فارسی

ـ خوبیاری، حامد، ۱۴۰۳، مطالعه تطبیقی و انتقادی حق بر فراموش شدن در پرتو اسناد بین‌المللی و حقوق ایران، **فصلنامه تحقیق و توسعه در حقوق تطبیقی**، شماره ۲۳.

ـ محقق داماد، سیدمصطفی، ۱۳۹۹، **قواعد فقه بخش عمومی**، چاپ اول، تهران، انتشارات مرکز نشر علوم اسلامی.

لاتین

- Ausloos, J., 2012, The ‘Right to be Forgotten’-Worth remembering? Computer Law & Security Review, 28 (2).
- Bala, R., 2022, Challenges and Ethical Issues in Data Privacy: Academic Perspective. International Journal of Information Retrieval Research, 12 (2).
- Benhamouda, F., Gentry, C., Gorbunov, S., Halevi, S., Krawczyk, H., Lin, C., Rabin, T., & Reyzin, L., 2020, Can a Public Blockchain Keep a Secret? In R. Pass & K. Pietrzak (Eds.) , Theory of Cryptography, Vol. 12550.
- Celador Angón, O., 2024, General Data Protection Regulation, Right to Be Forgotten, Blockchain Technology and Human Rights. The Age of Human Rights Journal, 23, e8702.
- Čtvrtník, M., 2023, Archives and Records: Privacy, Personality Rights, and Access. Springer International Publishing.
- Deeva, T. V., 2020, Blockchain Technologies and Smart Contracts: New Technological

۴۲- مانند محاسبات امن چندطرفه

Methods to Regulate Transactions and Trade Operations. International Journal of Emerging Trends in Engineering Research, 8 (7).
- Ellul, J., Galea, J., Ganado, M., Mccarthy, S., & Pace, G. J., 2020, Regulating Blockchain, DLT and Smart Contracts: A technology regulator's perspective. ERA Forum, 21 (2).
- Ferdous, M. S., Chowdhury, M. J. M., & Hoque, M. A., 2021, A survey of consensus algorithms in public blockchain systems for crypto-currencies. Journal of Network and Computer Applications.
- Goossens, J., 2021, Blockchain and democracy: Challenges and opportunities of blockchain and smart contracts for democracy in the distributed, algorithmic state. In O. Pollicino & G. De Gregorio (Eds.) , Blockchain and Public Law. Edward Elgar Publishing.
- Jain, P., Gyanchandani, M., & Khare, N., 2016, Big data privacy: A technological perspective and review. Journal of Big Data, 3 (1).
- Juliussen, B. A., Rui, J. P., & Johansen, D., 2023, Algorithms that forget: Machine unlearning and the right to erasure. Computer Law & Security Review, 51.
- Stainforth, E., 2022, Collective memory or the right to be forgotten? Cultures of digital memory and forgetting in the European Union. Memory Studies, 15 (2).
- Taherdoost, H., 2023, Smart Contracts in Blockchain Technology: A Critical Review. Information, 14 (2).
- Zheng, Z., Xie, S., Dai, H.-N., Chen, W., Chen, X., Weng, J., & Imran, M., 2020, An Overview on Smart Contracts: Challenges, Advances and Platforms. Future Generation Computer Systems.

Legal Civilization

ISSN: 2821-1022
ISSN: 2821-1081

No.25- Autumn 2025