

Digital Proceedings and Cybersecurity in the FIFA Football Tribunal

Saeed Mohammadpour navidan¹, Ali Hajipour Kondroud^{2*}, Yousef Molaei³, Adel Abbasi³

1- PhD Student, Department of civil Law, Ur.C. Branch, Islamic Azad University, Urmia, Iran

2*- Assistant Professor, Department of public Law, Ur.C. Branch, Islamic Azad University, Urmia, Iran

3 - Assistant Professor, Department of civil Law, Ur.C. Branch, Islamic Azad University, Urmia, Iran

ABSTRACT

Digitalisation has transformed football dispute resolution from paper correspondence and in-person communication into electronic filing, online exchange of pleadings, platform-based notification, and digital case management. In this environment, an electronic system is not merely a channel for transmitting information. It determines when an act is recorded, which document formats are acceptable, how a user is identified, who may access or modify case information, and whether the procedural history can later be reconstructed. The issue is particularly significant for the FIFA Football Tribunal because the parties to football disputes are frequently located in different countries and because the credibility of the Tribunal's decisions depends not only on substantive and procedural rules but also on the integrity of the communication infrastructure and the reliability of recorded data. The main research question is: How do electronic systems and cybersecurity requirements in the proceedings of the FIFA Football Tribunal affect the guarantee of fair proceedings and the validity of the Tribunal's decisions? The hypothesis is that electronic systems strengthen the legitimacy of proceedings and decisions only when they operate together with safeguards for data integrity, confidentiality, authentication, availability, technical logging, and effective remedies. Without these safeguards, the same technology may weaken the right to be heard and the reliability of procedural acts. This article uses a descriptive-analytical and comparative method. To answer the research question, it examines the procedural rules of the Football Tribunal, the regulations governing the status and transfer of players, official reports, relevant Court of Arbitration for Sport jurisprudence, legislation concerning electronic evidence, cybersecurity standards, and Persian and non-Persian academic literature. The findings demonstrate that filing a claim, submitting pleadings, uploading evidence, serving notifications, calculating time limits, and monitoring a case do not remain merely technical operations when the proceedings depend on a digital platform. Each operation may affect access to justice, the reasonable opportunity to present a case, and the ability to challenge an adverse procedural consequence. Electronic data also possesses adequate evidentiary value only when its source, creator, time of creation, alteration history, chain of custody, and independent verifiability can be established. System outages, compromised accounts, data alteration or deletion, unauthorised disclosure, and unreliable audit records may affect procedural deadlines, attribution of conduct, the opportunity to respond to the opposing party's evidence, and the validity of the final decision. The analysis of Court of Arbitration for Sport jurisprudence further indicates that the mere presence of information in a platform cannot replace proof of the legal elements of a claim or the parties' effective participation in the proceedings. The article concludes that cybersecurity should be recognised in FIFA procedural rules as a component of the guarantees of fair proceedings. The proposed framework therefore requires a defined notion of a security incident, prompt incident reporting, preservation of technical records, suspension or extension of time limits, an alternative communication channel, risk-based authentication, differentiated access controls, contractor auditing, and clear rules on responsibility and remediation. The framework connects digital efficiency with legal oversight and practical protection of the parties.

Keywords:

football dispute resolution; electronic systems; cybersecurity; digital evidence; fair proceedings

Article Type: Research Article

How to Cite: Mohammadpour navidan, S., Hajipour Kondroud, A., Molaei, Y., & Abbasi, A. (2026). Digital Proceedings and Cybersecurity in the FIFA Football Tribunal. *Journal of Cyber Law (JOCL)*, 3(1), 177-197. doi: 10.22054/jocl.2025.8563.9782

Journal of Cyber Law in Development and Evolution is licensed under a Creative Commons Attribution-Non Commercial 4.0 International License.

© Authors



Corresponding Author: Hajipour62@iau.ac.ir

دادرسی دیجیتال و امنیت سایبری در مرجع حل اختلافات فیفا

سعید محمدپور نویدان^۱، علی حاجی پور کندرود^{۲*}، یوسف مولایی^۳، عادل عباسی^۳

۱- دانشجوی دکتری، گروه حقوق خصوصی، واحد ارومیه، دانشگاه آزاد اسلامی، ارومیه، ایران

۲- استادیار گروه حقوق عمومی، واحد ارومیه، دانشگاه آزاد اسلامی، ارومیه، ایران

۳- استادیار گروه حقوق خصوصی، واحد ارومیه، دانشگاه آزاد اسلامی، ارومیه، ایران

چکیده

دیجیتالی شدن فرایندهای حل اختلاف در ورزش حرفه‌ای، ساختار رسیدگی به دعاوی فوتبالی را از مکاتبات کاغذی و ارتباطات حضوری به ثبت الکترونیکی دعوا، تبادل برخط اسناد، ابلاغ سامانه‌ای و مدیریت دیجیتال پرونده منتقل نموده است. در این محیط، سامانه فقط و سیله انتقال اطلاعات نیست؛ بلکه زمان ثبت اقدام، قالب قابل پذیرش سند، هویت کاربر، حدود دسترسی، وضعیت پرونده و امکان بازسازی سوابق را نیز تعیین می‌نماید. اهمیت موضوع در مورد مرجع حل اختلافات فدراسیون بین المللی فوتبال (فیفا) از آن جهت افزایش می‌یابد که طرفین اختلاف غالباً در کشورهای مختلف حضور دارند و اعتبار تصمیمات این نهاد، افزون بر رعایت قواعد ماهوی و آیینی، به سلامت زیر ساخت‌های ارتباطی و اعتمادپذیری داده‌های ثبت شده وابسته است. پرسش اصلی پژوهش آن است که سامانه‌های الکترونیکی و الزامات امنیت سایبری در فرایندهای مرجع حل اختلافات فیفا چگونه بر تضمین دادرسی منصفانه و اعتبار تصمیمات این نهاد اثر می‌گذارند؟ فرضیه پژوهش آن است که به کارگیری سامانه‌های الکترونیکی، هنگامی اعتبار دادرسی و تصمیمات مرجع را تقویت می‌نماید که با حفاظت هم‌زمان از تمامیت داده، محرمانگی، احراز هویت، قابلیت دسترسی، ثبت سوابق فنی و سازوکارهای اجرایی همراه گردد؛ در غیر این صورت، همان فناوری می‌تواند موجب تضعیف حق دفاع و قابلیت استناد اقدامات آیینی گردد. پژوهش حاضر با روش توصیفی-تحلیلی و رویکرد تطبیقی انجام پذیرفته است. برای پاسخ به پرسش پژوهش، قواعد آیینی مرجع حل اختلافات فوتبال، مقررات وضعیت و انتقال بازیکنان، گزارش‌های رسمی، آرای دیوان داور ورزش، قوانین مرتبط با ادله الکترونیکی، استانداردهای امنیت سایبری و منابع دانشگاهی فارسی و غیرفارسی بررسی گردیده است. یافته‌ها نشان می‌دهند که ثبت دعوا، ارسال لایحه، بارگذاری دلیل، ابلاغ، محاسبه مهلت و پیگیری پرونده، در صورت اتکای بیش از حد به عملکرد سامانه، ماهیتی صرفاً فنی ندارند و مستقیماً با حق دسترسی به رسیدگی و فرصت معقول دفاع ارتباط پیدا می‌نمایند. همچنین، داده‌های سامانه‌ای زمانی ارزش اثباتی کافی دارند که منشأ تولید، هویت ایجادکننده، زمان ثبت، سابقه تغییر، زنجیره نگهداری و امکان ارزیابی مستقل آن‌ها قابل احراز باشد. اختلال سامانه، سرقت حساب کاربری، تغییر یا حذف داده، افشای اطلاعات محرمانه و فقدان ثبت وقایع قابل اعتماد، ممکن است مهلت‌های آیینی، انتساب اقدام، امکان پاسخ به ادله طرف مقابل و اعتبار تصمیم نهایی را متأثر نماید. تحلیل آرای دیوان داور ورزش نیز نشان می‌دهد که درج اطلاعات در سامانه، به تنهایی جایگزین اثبات عناصر حقوقی دعوا و رعایت حق مشارکت طرفین نمی‌گردد. نتیجه پژوهش آن است که امنیت سایبری باید در قواعد آیینی فیفا به عنوان یکی از تضمین‌های دادرسی منصفانه شناسایی گردد. بر این اساس، تعریف رخداد امنیتی، اعلام فوری حادثه، حفظ سوابق فنی، تعلیق یا تمدید مهلت، تعیین مسیر ارتباطی جایگزین، احراز هویت متناسب با خطر، تفکیک سطوح دسترسی، ممیزی پیمانکاران و پیش‌بینی مسئولیت و جبران زیان، عناصر ضروری الگوی پیشنهادی پژوهش را تشکیل می‌دهند. این الگو، کارآمدی دیجیتال را با کنترل حقوقی و حمایت عملی از طرفین پیوند می‌دهد.

کلیدواژه‌ها:

حل اختلافات ورزشی؛ سامانه‌های الکترونیکی؛ امنیت سایبری؛ ادله دیجیتال؛ دادرسی منصفانه

نوع مقاله: پژوهشی

نحوه استناد:

محمدپور نویدان، سعید و حاجی پور کندرود، علی و مولایی، یوسف و عباسی، عادل. (۱۴۰۵). دادرسی دیجیتال و امنیت سایبری در مرجع حل اختلافات فیفا. حقوق سایبری، ۳(۱)، ۱۷۷-۱۹۷.

نشریه حقوق سایبری در توسعه و تکامل تحت مجوز کرییتیو کامنز انتساب - غیرتجاری ۴.۰ بین‌المللی منتشر شده است.

©نویسنده گان

ایمیل نویسنده مسئول: Hajipour62@iau.ac.ir



مقدمه

تحول دیجیتال، شیوه اداره و حل و فصل اختلافات ورزشی را دگرگون نموده است. در فوتبال حرفه‌ای، ثبت دعوا، تبادل لوایح، بارگذاری اسناد، دریافت ابلاغ و پیگیری وضعیت پرونده، بیش از گذشته از طریق سامانه‌های الکترونیکی انجام می‌پذیرد. این تحول در «مرجع حل اختلافات فدراسیون بین المللی فوتبال» (فیفا)^۱، جایگاه ویژه‌ای پیدا نموده است؛ زیرا این نهاد با اختلافاتی مواجه است که غالباً میان بازیکنان، باشگاه‌ها، مربیان، فدراسیون‌ها و کارگزاران مستقر در کشورهای مختلف شکل می‌گیرند.

بر اساس ساختار رسمی فیفا، مرجع حل اختلافات فیفا به موجب اساسنامه فیفا صلاحیت رسیدگی به اختلافات مرتبط با فوتبال و برخی درخواست‌های مقرراتی را دارد و از سه شعبه اصلی تشکیل می‌گردد. در قواعد آیینی این نهاد، برای ثبت دعوا، تبادل مکاتبات رسمی، ارائه ادله، محاسبه مهلت‌ها و ابلاغ تصمیمات، نقش مشخصی برای سامانه‌های الکترونیکی پیش‌بینی گردیده است (FIFA, 2026). بنابراین، سامانه‌های مذکور صرفاً ابزار اداری محسوب نمی‌گردند؛ بلکه در شکل‌گیری آثار حقوقی اقدامات طرفین مشارکت می‌نمایند.

اهمیت موضوع از آن جهت افزایش می‌یابد که هرگونه اختلال یا نقض امنیتی می‌تواند فراتر از افشای اطلاعات، حق دفاع و قابلیت اعتماد رسیدگی را متأثر نماید. برای نمونه، سرقت حساب کاربری ممکن است به ثبت لایحه‌ای بدون اراده واقعی طرف منجر گردد؛ از کارافتادن سامانه ممکن است رعایت مهلت را ناممکن سازد؛ و تغییر سابقه یک سند می‌تواند ارزیابی دلیل را با تردید مواجه نماید.

در گزارش رسمی سالانه فیفا و «دیوان داوری ورزش»^۲ حجم قابل توجهی از تصمیمات مرجع حل اختلافات فیفا و اعتراضات مربوط به آن گزارش گردیده است. این گزارش بر استمرار توسعه سازوکارهای حل اختلاف و ضرورت ثبت منظم عملکرد نهادهای فوتبالی تأکید می‌نماید (FIFA, 2025). گزارش مشترک سالانه نیز ضرورت توجه به کیفیت، قابلیت اعتماد و امنیت زیرساخت‌های دیجیتال را برجسته می‌سازد (FIFA & CAS, 2026).

اهمیت این پژوهش در پنج محور قابل بیان است: بین المللی بودن روابط فوتبالی، ارزش اقتصادی قراردادهای حساسیت داده‌های پرونده، آثار مستقیم ابلاغ سامانه‌ای بر مهلت‌ها و امکان اثرگذاری رخداد سایبری بر اعتبار تصمیم. در روابط فوتبالی، دیجیتالی شدن تنها به انتقال اسناد از کاغذ به فایل محدود نمی‌گردد. سامانه، ترتیب ورود اطلاعات، قالب قابل قبول سند، زمان ثبت اقدام و اشخاص مجاز برای مشاهده یا اصلاح داده را نیز تعیین می‌نماید. به همین دلیل، فناوری در این حوزه بخشی از معماری نهادی حل اختلاف به شمار می‌آید. تحلیل سامانه بدون توجه به صلاحیت، حق دفاع و حدود اختیار مرجع رسیدگی، تصویر ناقصی از آثار حقوقی دیجیتالی شدن ارائه می‌نماید. ادبیات عدالت دیجیتال نشان می‌دهد که فناوری می‌تواند مرزهای فیزیکی و حرفه‌ای دسترسی به عدالت را کاهش دهد (Katsh et al, 2017). در عین حال، محیط دیجیتال قواعد جدیدی برای شفافیت، مشارکت و کنترل تصمیمات سامانه‌ای لازم می‌سازد (Rabinovich et al, 2014).

ویژگی فرامرزی اختلافات فوتبال، این ضرورت را تشدید می‌نماید. طرفین ممکن است در کشورهای گوناگون اقامت داشته باشند، نمایندگان آنان در حوزه‌های قضایی متفاوت فعالیت نمایند و اسناد در چند سامانه یا نزد چند نهاد تولید

^۱ FIFA Football Tribunal

^۲ International Federation of Association Football (FIFA)

^۳ Court of Arbitration for Sport (CAS)

گردند. در چنین وضعیتی، اعتبار یک اقدام آیینی به سه عامل وابسته می‌گردد: نخست، قواعد روشن درباره زمان و شیوه ارتباط؛ دوم، سازوکار قابل اعتماد برای انتساب اقدام به شخص؛ و سوم، امکان دسترسی برابر به اطلاعات و ابزارهای دفاع. هرگاه یکی از این عوامل در اثر نقص فنی یا رخداد امنیتی مختل گردد، ارزیابی موضوع باید از سطح کارآمدی فناوری فراتر رود و با معیارهای دادرسی منصفانه انجام پذیرد.

بررسی پیشینه نشان می‌دهد که مطالعات فارسی و غیرفارسی موجود، هر کدام بخشی از موضوع حاضر را بررسی نموده‌اند. در پژوهش‌های فارسی، شعاعی و اعراب شیبانی (۱۴۰۱) ساختار حل و فصل اختلافات فوتبال در نظام ایران و عرصه بین المللی را تحلیل نموده‌اند، اما نقش سامانه‌های الکترونیکی در رسیدگی‌های فیفا را به صورت مستقل بررسی ننموده‌اند. صادقی‌نشاط (۱۳۹۳) اعتبارسنجی اسناد الکترونیکی و معیارهای اصالت و تمامیت آن‌ها را مورد مطالعه قرار داده است. قرایی و همکاران (۱۴۰۰) نیز امکان استنادپذیری ادله الکترونیکی را از منظر فقه و قانون تجارت الکترونیکی ایران بررسی نموده‌اند. همچنین، شریف‌زاده خرم (۱۴۰۴) اعتبار ادله الکترونیکی تولیدشده توسط الگوریتم‌ها را از منظر حقوق سایبری و دادرسی تحلیل نموده است. در ادبیات غیرفارسی، پذیرش ادله دیجیتال و معیارهای اصالت و قابلیت ارزیابی آن بررسی گردیده است (Ferreira et al, 2024). آثار فناوری‌های نوین بر ساختار داوری بین المللی نیز بررسی گردیده‌اند (Łągiewska, 2024). محرمانگی و حریم خصوصی در رسیدگی‌های دیجیتال نیز موضوع مطالعه مستقلی قرار گرفته است (Teramura & Trakman, 2024). با وجود ارزش علمی این مطالعات، بررسی هم‌زمان جایگاه سامانه‌های الکترونیکی، امنیت سایبری، اعتبار داده‌های سامانه‌ای و آثار نقض امنیت بر حق دفاع و اعتبار تصمیمات مرجع حل اختلافات فیفا همچنان با خلأ پژوهشی مواجه است.

پرسش اصلی پژوهش چنین مطرح می‌گردد: سامانه‌های الکترونیکی و الزامات امنیت سایبری در فرایندهای مرجع حل اختلافات فیفا چگونه بر تضمین دادرسی منصفانه و اعتبار تصمیمات این نهاد اثر می‌گذارند؟

فرضیه پژوهش آن است که به کارگیری سامانه‌های الکترونیکی، چنانچه با احراز هویت مطمئن، حفاظت از تمامیت داده‌ها، محرمانگی، ثبت قابل اعتماد وقایع، دسترسی برابر طرفین و سازوکار پاسخ‌گویی به رخدادهای سایبری همراه گردد، موجب افزایش سرعت، شفافیت و قابلیت اعتماد رسیدگی خواهد گردید؛ باین حال، ابهام در آثار حقوقی اختلال سامانه، نقض امنیت، تغییر یا از بین رفتن ادله دیجیتال و مسئولیت ناشی از این رخدادها می‌تواند دادرسی منصفانه و اعتبار تصمیمات را با چالش مواجه نماید.

پژوهش حاضر با روش توصیفی - تحلیلی و رویکرد تطبیقی انجام می‌پذیرد. منابع مورد استفاده شامل مقررات آیینی فیفا، مقررات وضعیت و انتقال بازیکنان، گزارش‌های رسمی، آرای دیوان داوری ورزش، قوانین مرتبط با داده‌های الکترونیکی، استانداردهای امنیت سایبری و مقالات دانشگاهی فارسی و غیرفارسی است. نوآوری پژوهش در آن قرار دارد که امنیت سایبری را نه صرفاً موضوعی فنی، بلکه به عنوان تضمین آیینی و شرط قابلیت اعتماد رسیدگی دیجیتال تحلیل می‌نماید.

در این پژوهش، سامانه به عنوان یک نهاد فنی بی طرف فرض نمی‌گردد؛ زیرا هر سامانه بر اساس انتخاب‌های طراحی، قواعد دسترسی و سیاست‌های نگهداری داده عمل می‌نماید. بنابراین، روش تحلیل علاوه بر مطالعه متن مقررات، به کارکرد حقوقی هر مرحله از گردش پرونده توجه می‌نماید: ایجاد حساب، شناسایی کاربر، ثبت اقدام، اطلاع‌رسانی، ذخیره دلیل، ارزیابی داده و امکان اعتراض. این رویکرد اجازه می‌دهد آثار امنیتی با نتیجه آیینی آن‌ها پیوند داده گردد و از ارائه فهرست

صرفی از تهدیدهای فنی جلوگیری گردد. در تحلیل تطبیقی نیز تجربه دادگاه‌های برخط و داوری بین‌المللی فقط به عنوان معیار راهنما به کار می‌رود و جایگزین قواعد خاص فوتبال نمی‌گردد.

۱. مبانی مفهومی و حقوقی حل و فصل اختلافات فوتبال در عصر دیجیتال

در این قسمت، مفاهیم و مبانی حقوقی لازم برای تحلیل سامانه‌های الکترونیکی در نظام حل اختلافات فوتبال بررسی می‌گردد. تمرکز این قسمت بر تعریف جایگاه مرجع حل اختلافات فیفا، مفهوم حل اختلاف الکترونیکی و رابطه امنیت سایبری با دادرسی منصفانه قرار دارد. جزئیات عملی سامانه‌ها و تهدیدهای امنیتی در بند دو و راهکارهای حقوقی در بند سه بررسی خواهند گردید.

۱-۱. ماهیت و جایگاه مرجع حل اختلاف فیفا در نظام حل اختلاف فوتبال

مرجع حل اختلافات فیفا در ساختار حقوقی فیفا قرار دارد و صلاحیت آن از اساسنامه، مقررات ماهوی فوتبال و قواعد آیینی فیفا ناشی می‌گردد. این نهاد از نظر سازمانی دادگاه دولتی محسوب نمی‌گردد، اما از نظر کارکردی وظایفی مشابه نهادهای شبه قضایی انجام می‌دهد؛ زیرا به اختلافات مشخص رسیدگی می‌نماید، به طرفین فرصت طرح ادعا و دفاع می‌دهد، ادله را ارزیابی می‌نماید و تصمیم الزام‌آور صادر می‌نماید.

سه شعبه اصلی این نهاد، حوزه‌های متفاوتی از اختلافات فوتبال را پوشش می‌دهند. «اتاق حل اختلاف» عمدتاً به اختلافات قراردادی و استخدامی میان بازیکنان و باشگاه‌ها، ثبات قراردادی و برخی دعاوی مربوط به آموزش بازیکنان رسیدگی می‌نماید. «اتاق وضعیت بازیکنان»^۱ در موضوعاتی مانند وضعیت بین‌المللی بازیکنان، انتقالات و برخی درخواست‌های مقرراتی صلاحیت دارد. «اتاق کارگزاران فوتبال»^۲ نیز در حدود مقررات فعالیت کارگزاران، اختلافات مربوط به این حرفه را بررسی می‌نماید.

مبنای صلاحیت هر شعبه، صرفاً توافق خصوصی طرفین نیست؛ بلکه مقررات فیفا در بسیاری از موارد صلاحیت نهادی را از پیش تعیین نموده‌اند. این ویژگی، مرجع حل اختلافات فیفا را از داوری خصوصی معمولی متمایز می‌سازد. در داوری خصوصی، صلاحیت داور غالباً بر رضایت طرفین مبتنی است؛ اما در نظام فیفا، عضویت در ساختار فوتبال سازمان‌یافته و پذیرش مقررات فیفا می‌تواند مبنای صلاحیت این نهاد قرار گیرد. اگرچه عضویت در ساختار فیفا به طور غیر مستقیم اعلام رضایت در شیوه داوری می‌باشد.

تصمیمات مرجع حل اختلافات فیفا در موارد مقرر نزد دیوان داوری ورزش قابل اعتراض است. امکان تجدید نظر، اهمیت اعتبار صورت جلسه‌ها، ابلاغ‌ها، اسناد و سوابق سامانه‌ای را افزایش می‌دهد؛ زیرا نقص در مرحله نخست ممکن است در مرحله اعتراض نیز بر ارزیابی صلاحیت یا رعایت حق دفاع اثر بگذارد. در چارچوب قواعد دیوان داوری ورزش، اعتراض به تصمیم‌های نهادهای ورزشی مستلزم رعایت شرایط شکلی و حفظ سابقه قابل‌بازبینی رسیدگی است (Court of Arbitration for Sport, 2025).

ماهیت تخصصی مرجع، ضرورت توازن میان سرعت و تضمین‌های آیینی را برجسته می‌نماید. اختلافات فوتبال غالباً با مهلت‌های نقل و انتقال، ثبت بازیکن، پرداخت‌های قراردادی و استمرار فعالیت حرفه‌ای پیوند دارد؛ بنابراین تأخیر در

¹ Dispute Resolution Chamber

² Players' Status Chamber

³ Football Agents Chamber

رسیدگی می‌تواند زیان اقتصادی یا ورزشی مستقلى ایجاد نماید. با وجود این، تخصص و سرعت نباید موجب کاهش سطح اطلاع‌رسانی، فرصت پاسخ یا امکان دسترسی به مدارک گردد. اعتبار تصمیم زمانی پایدار می‌ماند که طرفین بتوانند مسیر شکل‌گیری آن را بازسازی نمایند و بدانند کدام ادعا، سند و داده در نتیجه نهایی اثر گذاشته است. این برداشت با تحلیل‌های جدید از داوری بین‌المللی نیز هماهنگ است؛ زیرا نظم آیینی، استقلال مرجع و امکان کنترل تصمیم از عناصر مکمل مشروعیت نهادهای حل اختلاف محسوب می‌گردند (Born, 2021).

ارتباط مرجع با دیوان داوری ورزش، یک زنجیره چندمرحله‌ای از تصمیم‌گیری ایجاد می‌نماید. در مرحله نخست، داده‌های ثبت‌شده در سامانه برای تعیین تاریخ اقدام، هویت طرف، وضعیت پرونده و مدارک مبنا قرار می‌گیرند. در مرحله اعتراض، همان داده‌ها می‌توانند برای بررسی رعایت حق دفاع، حدود صلاحیت و منطق تصمیم مورد استفاده قرار گیرند. از این رو، نگهداری سوابق فنی و دسترسی کنترل‌شده به آن‌ها صرفاً وظیفه فناوری اطلاعات نیست؛ بلکه بخشی از وظیفه نهادی برای حفظ قابلیت بازبینی تصمیم به شمار می‌آید. قواعد عمومی داوری نیز بر ضرورت ثبت منظم اقدامات، حفظ پرونده و امکان بررسی فرایند تأکید دارند (Blackaby et al., 2022).

مشروعیت نهادی مرجع از ترکیب سه عنصر به دست می‌آید: مبنای صلاحیت، سلامت فرایند و قابلیت اجرای تصمیم. سامانه الکترونیکی بر هر سه عنصر اثر می‌گذارد. اگر ثبت درخواست در سامانه مبنای شروع رسیدگی باشد، نقص در ثبت می‌تواند بر صلاحیت زمانی اثر بگذارد؛ اگر تبادل اسناد از طریق درگاه انجام پذیرد، امنیت آن با سلامت فرایند پیوند می‌خورد؛ و اگر تصمیم برای اجرا به سابقه دیجیتال متکی باشد، قابلیت اعتماد داده بر اجرای آن اثر می‌گذارد. از این رو، اصلاح سامانه نباید به واحد فنی واگذار گردد، بلکه باید با مشارکت دبیرخانه حقوقی، اعضای مرجع و نمایندگان کاربران انجام پذیرد. این مشارکت، امکان شناسایی آثار پنهان طراحی بر حقوق طرفین را افزایش می‌دهد و با دیدگاه نهاد گرایانه درباره عدالت دیجیتال سازگارتر است.

۱-۲. مفهوم حل اختلاف الکترونیکی و مبانی حقوقی آن

حل اختلاف الکترونیکی به استفاده سازمان‌یافته از فناوری‌های دیجیتال برای ثبت، مدیریت، ارتباط، ارائه ادله و حل و فصل اختلافات گفته می‌گردد. این مفهوم با برگزاری صرف جلسه از طریق ارتباط تصویری تفاوت دارد. در الگوی کامل، فناوری در تمام چرخه پرونده، از ایجاد حساب کاربری و ثبت دعوا تا تبادل لوایح، اطلاع‌رسانی درباره مهلت‌ها و دریافت تصمیم حضور می‌یابد.

در چارچوب سازمان همکاری و توسعه اقتصادی، «حل اختلاف برخط» فرایندی است که در آن فناوری و داده‌های دیجیتال برای تسهیل حل اختلاف مورد استفاده قرار می‌گیرند. این چارچوب بر حکمرانی، ابزارهای سیاستی و ملاحظات اخلاقی و حفاظتی تأکید می‌نماید (OECD, 2024). بنابراین، کیفیت سامانه تنها با سرعت یا کاهش هزینه سنجیده نمی‌گردد؛ بلکه اعتماد، حفاظت از داده، شفافیت و دسترسی مؤثر نیز اهمیت دارد.

«اصل برابری کارکردی»^۱ در حقوق تجارت الکترونیکی اقتضا می‌نماید که سند یا اقدام الکترونیکی صرفاً به دلیل غیر کاغذی بودن از آثار حقوقی محروم نگردد؛ مشروط بر آنکه کارکردهای لازم مانند قابلیت دسترسی، تمامیت، انتساب و قابلیت بازتولید را تأمین نماید. در نتیجه، ثبت الکترونیکی دعوا یا ارسال دیجیتال لایحه، زمانی اعتبار حقوقی پیدا می‌نماید که سامانه بتواند نشان دهد چه شخصی، در چه زمانی و با چه سطحی از احراز هویت، اقدام موردنظر را انجام داده است. در فرایندهای مرجع حل اختلافات فیفا، دیجیتالی شدن با خود کارشدن تصمیم‌گیری یکی نیست. تصمیم‌نهایی توسط مقام یا مرجع صالح انسانی اتخاذ می‌گردد و سامانه نقش زیرساختی و ارتباطی ایفا می‌نماید. این تمایز اهمیت دارد؛ زیرا استفاده از فناوری، مسئولیت حقوقی نهاد رسیدگی را از بین نمی‌برد، بلکه تکلیف آن را برای تضمین قابلیت اعتماد و دسترس‌پذیری افزایش می‌دهد.

درک درست از حل اختلاف الکترونیکی، به تفکیک سه سطح نیاز دارد: سطح ارتباطی، سطح مدیریتی و سطح تصمیم‌گیری. در سطح ارتباطی، پیام و سند به شکل دیجیتال مبادله می‌گردد. در سطح مدیریتی، مدیریت زمان‌بندی و مهلت‌های پرونده، وضعیت، دسترسی و گردش پرونده را سازمان‌دهی می‌نماید. در سطح تصمیم‌گیری، داده‌های گردآوری شده ممکن است بر تشخیص واقعیت و ارزیابی دلیل اثر بگذارد. هرچه رسیدگی از سطح نخست به سطوح دوم و سوم نزدیک‌تر گردد، ضرورت نظارت انسانی، امکان توضیح‌خواهی و کنترل خطا نیز افزایش می‌یابد. از این منظر، سامانه مطلوب سامانه‌ای نیست که فقط سریع باشد؛ بلکه باید قابل فهم، قابل بازبینی و قابل اصلاح نیز باشد. نظریه دادگاه‌های برخط بر همین نکته تأکید می‌نماید که دسترسی به عدالت با انتقال فرایند به اینترنت پایان نمی‌پذیرد و طراحی خدمت، زبان ارتباط و امکان پشتیبانی نیز جزء دسترسی واقعی محسوب می‌گردد (Susskind, 2019).

مبنای حقوقی پذیرش ارتباطات الکترونیکی، در عین حمایت از بی‌طرفی فناوری، به معنای بی‌نیازی از قواعد شکلی نیست. باید معلوم باشد ارسال‌کننده چه کسی است، پیام به کدام پرونده تعلق دارد، نسخه‌نهایی کدام است و آیا مخاطب فرصت متعارف برای پاسخ داشته است. این پرسش‌ها در اختلافات فوتبالی اهمیت بیشتری پیدا می‌نمایند؛ زیرا نماینده حقوقی ممکن است تغییر کند، چند کاربر از یک حساب سازمانی استفاده نمایند و اسناد به زبان‌ها و قالب‌های متفاوت بارگذاری گردند. راه‌حل آن است که هر حساب به نماینده مشخص متصل گردد، تغییر نماینده در پرونده ثبت گردد، نسخه‌نهایی با تأیید روشن از نسخه پیش‌نویس جدا گردد و در صورت تردید، مرجع رسیدگی از کاربر توضیح تکمیلی مطالبه نماید. بدین ترتیب، اصل برابری کارکردی با حق دفاع همراه می‌گردد.

۱-۳. امنیت سایبری، محرمانگی و دادرسی منصفانه

امنیت سایبری در رسیدگی‌های دیجیتال بر چهار ارزش اصلی استوار می‌گردد: محرمانگی، تمامیت، دسترس‌پذیری و قابلیت انتساب. محرمانگی از دسترسی اشخاص غیرمجاز جلوگیری می‌نماید؛ تمامیت تغییرناپذیری داده را تضمین می‌نماید؛ دسترس‌پذیری امکان استفاده به‌موقع از سامانه را فراهم می‌نماید و قابلیت انتساب مشخص می‌سازد که اقدام الکترونیکی به کدام کاربر یا مقام قابل نسبت دادن است.

^۱ اصل برابری کارکردی در حقوق تجارت الکترونیکی به این معناست که سند یا اقدام الکترونیکی صرفاً به دلیل فقدان شکل کاغذی، از اعتبار و آثار حقوقی محروم نشود؛ مشروط بر آنکه بتواند کارکردهای حقوقی مورد انتظار از شکل سنتی، از جمله قابلیت دسترسی، شناسایی صادرکننده، اعلام قصد، حفظ تمامیت و امکان بازتولید، را تأمین کند. این اصل به معنای یکسانی فنی یا ماهوی سند الکترونیکی و سند کاغذی نیست، بلکه برابری آثار حقوقی آن‌ها در صورت تحقق شرایط لازم دلالت دارد. این اصل در قانون نمونه تجارت الکترونیکی آنتیترال، به‌ویژه در ارتباط با الزامات نوشتار، امضا و اصل بودن سند، مورد شناسایی قرار گرفته است.

این ارزش‌ها مستقیماً با دادرسی منصفانه ارتباط دارند. اگر شخصی به دلیل اختلال سامانه نتواند در مهلت مقرر لایحه خود را ثبت نماید، مسئله صرفاً فنی محسوب نمی‌گردد؛ بلکه حق دفاع او محدود می‌گردد. اگر حساب کاربری نماینده به سرعت رود، اعتبار اسناد ثبت‌شده و قابلیت انتساب آن‌ها محل تردید قرار می‌گیرد. اگر محتوای پرونده تغییر یابد، اصل برابری طرفین و امکان ارزیابی منصفانه ادله آسیب می‌بیند.

قواعد آیینی مرجع حل اختلافات فیفا، محرمانگی رسیدگی، ارائه اسناد و دسترسی طرفین به پرونده را مورد توجه قرار داده‌اند. از این‌رو، امنیت سامانه پیش‌شرط اجرای بسیاری از قواعد آیینی محسوب می‌گردد. چارچوب امنیت سایبری مؤسسه ملی استاندارد و فناوری ایالات متحده نیز امنیت را در قالب حکمرانی، شناسایی، حفاظت، کشف، پاسخ و بازیابی سازمان‌دهی نموده است (NIST, 2024).

در نهایت، امنیت سایبری در نظام حل اختلاف فوتبال سه کارکرد دارد: کارکرد حفاظتی برای جلوگیری از نفوذ و افشای اطلاعات؛ کارکرد اثباتی برای حفظ تمامیت و قابلیت اعتماد ادله؛ و کارکرد آیینی برای تضمین ابلاغ، مهلت، دسترسی و حق دفاع. همین پیوند سه‌گانه، مبنای تحلیل بخش‌های بعدی را تشکیل می‌دهد.

محرمانگی در این زمینه با پنهان کردن مطلق اطلاعات یکسان نیست. مرجع رسیدگی باید میان حفاظت از داده و حق دسترسی طرفین به پرونده توازن ایجاد نماید. طرفین برای پاسخ‌گویی مؤثر باید بدانند چه ادعایی علیه آنان مطرح گردیده و کدام دلیل مورد استناد قرار گرفته است؛ اما اشخاص ثالث، کارکنان غیرمرتبط و حتی طرف مقابل نباید بیش از اندازه لازم به اطلاعات شخصی یا تجاری دسترسی پیدا نمایند. از این‌رو، تفکیک سطح دسترسی، حذف داده‌های غیرضروری و ناشناس‌سازی بخش‌هایی از پرونده، ابزارهای حقوقی مهمی برای هم‌زمانی محرمانگی و برابری طرفین محسوب می‌گردند. در ادبیات حریم خصوصی نیز تأکید گردیده است که امنیت و حفاظت از داده دو حوزه جدا از هم نیستند و اقداماتی مانند رمزگذاری، کمینه‌سازی داده و محدودکردن نگهداری، می‌تواند هر دو هدف را تقویت نماید (Teramura & Trakman).

اصل برابری دسترسی در محیط دیجیتال، دسترسی صوری به حساب کاربری را کافی نمی‌داند. طرف باید از ابزار، زمان و اطلاعاتی برخوردار باشد که برای پاسخ‌گویی عملی لازم است. تفاوت در کیفیت اتصال، دسترسی به ترجمه، توانایی بارگذاری فایل‌های بزرگ، امکان مشاهده فرمت‌های خاص یا مهارت استفاده از سامانه، ممکن است به نابرابری واقعی منجر گردد. بنابراین، طراحی درگاه باید با راهنمای روشن، امکان دریافت رسید، مهلت معقول، پشتیبانی فنی و مسیر جایگزین همراه باشد. پژوهش‌های مربوط به عدالت دیجیتال نیز هشدار می‌دهند که فناوری در کنار کاهش موانع جغرافیایی، می‌تواند موانع تازه‌ای در زمینه مهارت، زبان و دسترسی ایجاد نماید (Latifah et al., 2019).

در پرونده‌های دارای طرف کم‌توان، بازیکن کم‌سن یا شخصی که بدون وکیل حرفه‌ای اقدام می‌نماید، رعایت برابری دیجیتال اهمیت مضاعف پیدا می‌نماید. مرجع رسیدگی باید اطلاعات ضروری درباره مراحل سامانه، مهلت‌ها و آثار ثبت را با زبان روشن ارائه نماید و در موارد قابل توجه، امکان اصلاح خطاهای غیرماهوی را فراهم سازد. این حمایت نباید به ترجیح یکی از طرفین یا دخالت در استدلال حقوقی آنان منجر گردد؛ بلکه هدف آن، فراهم کردن امکان استفاده واقعی از مسیر یکسان است. درک این نکته برای مرجع اهمیت دارد، زیرا سرعت و استانداردسازی سامانه ممکن است در ظاهر رفتار برابر ایجاد نماید، اما نتیجه عملی برای کاربران متفاوت باشد.

۲. کارکرد سامانه‌های الکترونیکی و چالش‌های امنیتی

در این قسمت، عملکرد سامانه‌های الکترونیکی را در جریان واقعی رسیدگی بررسی می‌نماییم. تمرکز بخش حاضر بر ثبت دعوا، ارتباطات آیینی، مدیریت پرونده، ادله دیجیتال و تهدیدهایی قرار دارد که می‌توانند نتیجه یا اعتبار رسیدگی را متأثر نمایند.

۲-۱. نقش سامانه‌ها در ثبت دعوا، ارتباطات و مدیریت پرونده

سامانه‌های الکترونیکی در فرایندهای مرجع حل اختلافات فیفا، صرفاً ابزار ارسال اسناد محسوب نمی‌گردند؛ بلکه بخش مهمی از ساختار آیینی رسیدگی را تشکیل می‌دهند. ثبت دعوا، معرفی نماینده، ارسال لوایح، بارگذاری مدارک، دریافت پیام‌های رسمی، اطلاع از مهلت‌ها و پیگیری وضعیت پرونده از طریق بسترهای تعیین شده انجام می‌پذیرد.

مطابق قواعد آیینی فیفا، ارتباطات مربوط به پرونده‌ها از طریق «درگاه حقوقی فیفا»^۱ یا «سامانه مدیریت نقل و انتقالات»^۲ انجام می‌پذیرد. انتخاب سامانه به ماهیت موضوع بستگی دارد. دعاوی قراردادی و استخدامی عمدتاً از طریق درگاه حقوقی و درخواست‌های مقرراتی مرتبط با نقل و انتقال یا حق آموزشی از طریق سامانه مدیریت نقل و انتقالات پیگیری می‌گردند (FIFA, 2026, arts).

این تفکیک موجب تخصصی‌شدن مدیریت پرونده و کاهش مکاتبات پراکنده می‌گردد، اما احتمال خطا در تشخیص مسیر صحیح ثبت درخواست را نیز افزایش می‌دهد. چنانچه طرف دعوا پرونده را در بستر نامناسب ثبت نماید، درخواست ممکن است ناقص تلقی گردد یا رسیدگی به آن با تأخیر مواجه گردد. از این رو، راهنمایی روشن و دسترسی برابر، بخشی از الزامات عدالت ورزشی محسوب می‌گردد.

تمرکز سوابق در یک پرونده دیجیتال، امکان جست‌وجو، طبقه‌بندی، شماره‌گذاری و ارزیابی منظم اسناد را افزایش می‌دهد. در مقابل، سامانه می‌تواند به نقطه شکست واحد تبدیل گردد؛ زیرا اختلال آن به صورت هم‌زمان بر ثبت دعوا، ارائه دفاع، مشاهده پرونده و رعایت مهلت اثر می‌گذارد.

از نظر حقوقی باید میان ابلاغ فنی و اطلاع واقعی تفکیک ایجاد گردد. ابلاغ فنی زمانی رخ می‌دهد که پیام در حساب کاربری یا نشانی ثبت‌شده قرار گیرد، اما اطلاع واقعی به آگاهی عملی شخص از محتوای پیام مربوط است. در صورت سرقت حساب، اختلال گسترده یا عدم دسترسی واقعی، صرف قرار گرفتن پیام در سامانه نباید بدون بررسی اوضاع پرونده، تعیین‌کننده اعتبار ابلاغ قرار گیرد. در تحلیل جلسات برخط نیز امکان فنی حضور، به‌تنهایی معادل مشارکت مؤثر و رعایت حق دفاع محسوب نمی‌گردد (Chen, 2024).

برای جلوگیری از اختلاف درباره زمان اقدام، سامانه باید پس از هر ثبت، رسیدی قابل نگهداری در اختیار کاربر قرار دهد. این رسید باید دست‌کم شناسه پرونده، زمان ثبت بر مبنای منطقه زمانی اعلام‌شده، نام فایل، حجم فایل، وضعیت موفق یا ناموفق بارگذاری و شماره یکتای تراکنش را مشخص نماید. نمایش یک پیام ساده مبنی بر ارسال فایل، در پرونده‌های حساس برای اثبات کامل کافی نیست؛ زیرا کاربر باید بتواند در آینده رابطه میان فایل و اقدام ثبت‌شده را نشان دهد. همچنین سامانه باید میان پیش‌نویس، ثبت نهایی و ارسال موفق تفاوت آشکار ایجاد نماید تا کاربر تصور ننماید ذخیره موقت، اقدام آیینی نهایی محسوب می‌گردد. این الزامات، خطای انسانی را کاهش می‌دهد و در صورت اختلاف درباره

^۱ FIFA Legal Portal

^۲ Transfer Matching System (TMS)

رعایت مهلت، مبنای ارزیابی فنی و حقوقی فراهم می‌نماید. پژوهش‌های مربوط به جهان دیجیتال داوری نیز ثبت مسیر اقدام و امکان بازسازی فرایند را برای اعتمادپذیری ارتباطات ضروری می‌دانند (Łagiewska et al). دسترسی برابر، مستلزم آن است که اطلاعات پرونده در قالبی قابل استفاده و در زمان مناسب در اختیار طرفین قرار گیرد. محدودیت حجم فایل، ناسازگاری قالب، قطع ارتباط هنگام بارگذاری یا نبود امکان مشاهده سوابق قبلی، نباید بدون بررسی اثر واقعی آن بر دفاع، به زیان کاربر تفسیر گردد. در رسیدگی‌های فرامرزی، اختلاف منطقه زمانی و تعطیلات کشورهای مختلف نیز باید با اعلام روشن و یکنواخت مدیریت گردد. مرجع رسیدگی می‌تواند برای این منظور، زمان مرجع سامانه را در قواعد اعلام نماید و در صورت بروز خطای سامانه، گزارش عمومی وضعیت و دستورالعمل مسیر جایگزین منتشر کند. چنین تدبیری، هم پیش‌بینی‌پذیری را افزایش می‌دهد و هم از طرح اختلافات تکراری درباره دریافت یا عدم دریافت پیام جلوگیری می‌نماید.

مدیریت پرونده در سامانه باید به نحوی طراحی گردد که مرز میان داده اداری و داده مؤثر بر تصمیم روشن باشد. اطلاعات تماس، وضعیت نمایندگی و تاریخ دریافت، در ظاهر داده‌های اجرایی‌اند؛ اما همین داده‌ها می‌توانند تعیین نمایند که کدام شخص مخاطب ابلاغ قرار گیرد یا کدام دفاع در مهلت مقرر ارائه گردد. از این‌رو، تغییر هر یک از این داده‌ها باید با ثبت علت، هویت تغییردهنده و زمان اصلاح همراه باشد. دسترسی طرفین به تاریخچه اقدامات نیز باید به اندازه‌ای باشد که امکان کنترل فرایند را فراهم نماید، بدون آنکه اسرار تجاری یا داده‌های شخصی غیرمرتبط افشا گردد. ایجاد دفتر ثبت تغییرات و تفکیک نقش میان ثبت‌کننده، ناظر و تصمیم‌گیرنده، اعتماد به مدیریت پرونده را افزایش می‌دهد و مانع آن می‌گردد که اصلاح اداری بدون ردپای قابل بررسی در پرونده باقی بماند.

پشتیبانی کاربر بخشی از تضمین دسترسی مؤثر به سامانه است. در دعاوی بین‌المللی، همه کاربران از سطح یکسانی از دانش فنی یا آشنایی با زبان مقررات برخوردار نیستند. در گاه باید خطاهای بارگذاری را به‌صورت قابل فهم توضیح دهد، امکان اصلاح پیش از ثبت نهایی را فراهم نماید و در صورت از دست رفتن ارتباط، وضعیت اقدام را روشن سازد. همچنین، وجود نشانی ارتباط اضطراری برای ثبت گزارش اختلال یا درخواست راهنمایی اهمیت دارد. این پشتیبانی نباید به مشاوره ماهوی درباره دعوا تبدیل گردد؛ اما باید مانع آن گردد که خطای قابل پیشگیری در کار با سامانه به از دست رفتن حق دفاع بینجامد. معیار سنجش، آن است که کاربر متعارف بتواند با تلاش معقول اقدام لازم را انجام دهد و در صورت بروز خطا، مسیر اصلاح برای او قابل شناسایی باشد. در این میان، شکل ارائه استدلال و ارتباط حقوقی نیز بر فهم و ارزیابی مشارکت طرفین اثر می‌گذارد (Gómez-Moreno, 2024).

۲-۲. ادله دیجیتال و حکمرانی داده‌های پرونده

در پرونده‌های فوتبال، ادله دیجیتال از منابع گوناگون به دست می‌آید. قراردادهای الکترونیکی، پیام‌های رسمی، رایانامه‌ها، رسیدهای بانکی، سوابق ثبت انتقال، گزارش‌های ورود کاربران، داده‌های زمانی، نسخه‌های مختلف یک سند و مکاتبات نمایندگان، از جمله ادله قابل استفاده محسوب می‌گردند.

قواعد آیینی مرجع حل اختلافات فیفا، نوع خاصی از دلیل را به‌صورت انحصاری مقرر ننموده و اختیار ارزیابی ارزش اثباتی را به مرجع رسیدگی واگذار نموده‌اند. همچنین، مرجع می‌تواند به اطلاعاتی توجه نماید که در سامانه‌های فیفا تولید یا نگهداری گردیده‌اند. این امر امکان استفاده از داده‌های فنی را فراهم می‌نماید، اما ضرورت شفافیت درباره منشأ و سابقه داده را نیز ایجاد می‌نماید.

هر داده دیجیتال برای برخورداری از ارزش اثباتی باید از چهار جهت بررسی گردد: انتساب به شخص یا سامانه، تمامیت محتوا، قابلیت بازسازی فرایند تولید و ارتباط با موضوع اختلاف. تصویر یک پیام یا نسخه چاپی یک صفحه، بدون اطلاعات مربوط به منشأ، زمان ایجاد، حساب کاربری و سابقه تغییر، ممکن است برای اثبات کامل ادعا کفایت ننماید (صادقی‌نشاط، ۱۳۹۳، ص. ۵۲).

یکی از مفاهیم اساسی در این زمینه، «زنجیره نگهداری دلیل» است. این مفهوم مجموعه اقداماتی را دربرمی‌گیرد که از زمان تولید یا دریافت دلیل تا زمان ارائه و ارزیابی آن، امکان نظارت بر جابه‌جایی، نگهداری، دسترسی و تغییرات احتمالی را فراهم می‌نماید.

«ثبت وقایع سامانه» نیز اهمیت ویژه‌ای دارد. این سوابق می‌تواند زمان ورود کاربر، بارگذاری سند، مشاهده پیام، تغییر اطلاعات تماس، حذف یا جایگزینی فایل و تلاش‌های ناموفق برای ورود را ثبت نماید. وجود این اطلاعات، اختلافات مربوط به ابلاغ، مهلت و انتساب اقدام را کاهش می‌دهد.

داده‌های سامانه‌ای نباید بدون امکان بررسی طرفین، ارزش قطعی و غیرقابل خدشه پیدا نمایند. اگر مرجع رسیدگی به داده‌ای استناد نماید که درون سامانه تولید گردیده، طرفین باید بتوانند در حدود محرمانگی پرونده، منشأ داده، مبنای تولید، زمان ثبت و سوابق تغییر آن را بررسی نمایند.

در حقوق ایران نیز اصل پذیرش داده‌های الکترونیکی مورد شناسایی قرار گرفته است. قانون تجارت الکترونیکی، داده‌پیام را در شرایط مقرر دارای ارزش اثباتی دانسته و ارزش آن را با میزان اطمینان به روش تولید، ذخیره، انتقال و حفاظت مرتبط نموده است (قانون تجارت الکترونیکی، ۱۳۸۲، مواد ۱۲ و ۱۳).

در ارزیابی ادله دیجیتال، میان قابلیت پذیرش و وزن اثباتی باید تفکیک صورت پذیرد. قابلیت پذیرش به این پرسش پاسخ می‌دهد که آیا دلیل اصولاً می‌تواند وارد فرایند رسیدگی گردد؛ وزن اثباتی به میزان اعتمادی مربوط است که مرجع رسیدگی پس از بررسی مجموعه اوضاع به آن اختصاص می‌دهد. یک رایانامه، تصویر صفحه یا سابقه سامانه‌ای ممکن است قابل بررسی باشد، اما ارزش آن به کیفیت انتساب، پیوستگی زمانی، امکان دسترسی به داده اصلی و نبود نشانه‌های دست‌کاری وابسته است. این تفکیک مانع از آن می‌گردد که داده‌ای صرفاً به دلیل تولیدشدن در محیط رسمی، دلیل قطعی تلقی گردد. در داوری بین‌المللی نیز توجه به اصالت، تمامیت و نحوه به‌دست‌آوردن داده، برای سنجش ارزش دلیل اهمیت دارد (Ferreira et al 2024).

در پرونده‌های مربوط به نقل و انتقال و حق آموزش، گذرنامه الکترونیکی بازیکن می‌تواند در تعیین زنجیره انتقال، تاریخ ثبت و ذی‌نفعان احتمالی نقش مهمی ایفا نماید. با وجود این، داده ثبت‌شده در چنین سامانه‌ای معمولاً نتیجه ورود اطلاعات توسط اشخاص یا نهادهای مختلف است و خطای اولیه، تأخیر در اصلاح یا تفاوت میان ثبت سامانه‌ای و واقعیت قراردادی را منتفی نمی‌سازد. مرجع رسیدگی باید مشخص نماید داده در چه مرحله‌ای تولید گردیده، چه کسی مسئول ورود آن بوده، آیا امکان اعتراض یا اصلاح وجود داشته و کدام اسناد مستقل آن را تأیید یا تضعیف می‌نمایند. این شیوه، هم از اتکای افراطی به داده سامانه‌ای جلوگیری می‌نماید و هم جایگاه فنی آن را در کشف واقعیت حفظ می‌نماید.

حکمرانی داده فقط به زمان رسیدگی محدود نمی‌گردد و دوره پس از صدور تصمیم را نیز دربرمی‌گیرد. باید معلوم باشد پرونده تا چه زمانی نگهداری می‌گردد، چه داده‌ای برای اعتراض یا اجرای تصمیم ضروری است، چه داده‌ای باید حذف یا ناشناس گردد و چه نهادی مجاز به نگهداری نسخه پشتیبان است. نگهداری بی‌ضابطه اطلاعات، خطر افشا و استفاده

ثانویه را افزایش می‌دهد؛ حذف شتاب‌زده نیز می‌تواند امکان اعتراض و بازبینی را از بین ببرد. راه‌حل، جدول نگهداری مبتنی بر نوع داده و مرحله پرونده است. داده‌های لازم برای اثبات ثبت و ابلاغ باید تا پایان دوره اعتراض و اجرای تصمیم حفظ گردد، اما اطلاعات غیرضروری پس از سپری‌شدن ضرورت حقوقی باید حذف یا ناشناس گردد. این رویکرد با الزامات محرمانگی داوری و اصول کمینه‌سازی داده سازگارتر است (Teramura et al, 2024).

کاربرد ابزارهای تحلیلی در دسته‌بندی یا جست‌وجوی پرونده نیز باید تحت کنترل حقوقی باقی بماند. اگر سامانه بر اساس کلید واژه، نوع اختلاف یا وضعیت قرارداد، اسناد را مرتب نماید، نتیجه این مرتب‌سازی نباید جایگزین ارزیابی انسانی دلیل گردد. داده ناقص یا برجسته‌گذاری نادرست می‌تواند سند مهمی را از دسترس دور سازد و بر برداشت اولیه تصمیم‌گیرنده اثر بگذارد. برای کاهش این خطر، معیارهای جست‌وجو و طبقه‌بندی باید قابل توضیح باشند، امکان جست‌وجوی دستی حفظ گردد و کاربر بتواند درباره حذف یا جای‌گذاری نادرست سند اعتراض نماید. هرچه نقش ابزارهای تحلیلی در گردش پرونده بیشتر گردد، ضرورت ثبت نسخه معیارها، زمان اجرای فرایند و شخص مسئول بازبینی نیز افزایش می‌یابد. منظور از شفافیت فرایندی، افشای کد یا اسرار فنی سامانه نیست؛ بلکه باید مشخص باشد سامانه بر اساس چه معیارهایی اسناد را جست‌وجو و طبقه‌بندی کرده و این فرایند چه اثری بر دسترسی و ارزیابی اسناد پرونده داشته است.

مطالعه تجربی درباره پرونده‌های داوری نیز نشان می‌دهد که پیام‌های متنی، رسیدهای پرداخت، تصاویر و داده‌های سامانه‌ای در عمل به‌طور منظم مورد استفاده قرار می‌گیرند و ارزیابی ارزش آن‌ها به معیارهای پذیرش، ارتباط و وزن اثباتی وابسته است (Ferreira et al, 2023).

در جلسات برخط، ارزیابی اعتبار اظهارات نیز با محدودیت‌های ادراکی و فنی مواجه می‌گردد؛ از این رو، کیفیت تصویر، امکان مشاهده واکنش‌ها و ثبت کامل جلسه باید در کنار سایر ادله سنجیده گردد (Moreira et al).

۳-۲. تهدیدهای امنیت سایبری و آثار آیینی آن‌ها

سامانه‌های حل اختلاف ورزشی، به دلیل ارزش اقتصادی پرونده‌ها و حساسیت اطلاعات، در معرض تهدیدهای گوناگون قرار دارند. سرقت نام کاربری و گذرواژه، فریب کاربران، بدافزار، اخاذی دیجیتال، حمله برای از کارانداختن سامانه، دسترسی غیرمجاز کارکنان، نشت اطلاعات از پیمانکاران و دست‌کاری داده‌ها از مهم‌ترین تهدیدهای این حوزه محسوب می‌گردند.

سرقت حساب کاربری از مهم‌ترین تهدیدهای آیینی است. اگر شخص ثالثی با استفاده از اطلاعات کاربر وارد سامانه گردد و لایحه‌ای ثبت نماید، باید مشخص گردد که اقدام انجام‌شده به چه شخصی قابل انتساب است. در این وضعیت، ثبت اقدام با نام کاربری به‌تنهایی برای اثبات اراده طرف کافی نخواهد بود؛ زیرا سطح احراز هویت، سوابق ورود، دستگاه مورد استفاده و الگوی معمول فعالیت باید بررسی گردد.

استفاده از «احراز هویت چندمرحله‌ای» می‌تواند احتمال سرقت حساب را کاهش دهد، اما این روش به‌تنهایی مشکل انتساب را حل نمی‌نماید. سامانه باید سوابق ورود، تغییر رمز، دستگاه مورد استفاده و زمان فعالیت را نیز ثبت نماید. در صورت مشاهده فعالیت غیرعادی، امکان توقف موقت حساب و اطلاع‌رسانی فوری باید وجود داشته باشد.

اختلال سامانه نیز آثار متفاوتی ایجاد می‌نماید. اختلال کوتاه و قابل پیش‌بینی الزاماً موجب بی‌اعتباری مهلت نخواهد گردید؛ اما قطعی گسترده، حمله هدفمند یا عدم امکان بارگذاری سند در پایان مهلت می‌تواند حق دفاع را متأثر نماید. معیار مناسب، میزان تأثیر اختلال بر فرصت واقعی دفاع و امکان استفاده از مسیر جایگزین است.

افشای اطلاعات نیز با اصل محرمانگی رسیدگی تعارض پیدا می‌نماید. پرونده‌های فوتبالی ممکن است شامل قرارداد، حساب بانکی، وضعیت پزشکی یا اطلاعات بازیکنان کم‌سن باشد. انتشار یا انتقال غیرمجاز چنین اطلاعاتی می‌تواند علاوه بر مسئولیت قراردادی و انتظامی، مسئولیت ناشی از نقض حریم خصوصی را نیز ایجاد نماید.

از بررسی قواعد موجود می‌توان نتیجه گرفت که فیفا به ارتباطات دیجیتال و محرمانگی توجه نموده است، اما درباره پیامدهای تفصیلی رخدادهای امنیتی، نظام جامعی ایجاد ننموده است. این خلأ باید از طریق تعریف رخداد، شیوه اعلام، حفظ سوابق فنی، تعلیق مهلت و مسیر ارتباطی جایگزین برطرف گردد.

تهدیدهای سایبری از نظر اثر حقوقی یکسان نیستند و باید بر مبنای نتیجه آن‌ها طبقه‌بندی گردند. نفوذی که فقط یک تلاش ناموفق برای ورود بوده است، با رخدادی که موجب تغییر لایحه، حذف سابقه یا افشای اطلاعات پزشکی گردیده، آثار یکسانی ندارد. معیار مناسب برای واکنش، ترکیبی از دامنه دسترسی، نوع داده، مدت اختلال، قابلیت تشخیص رخداد، تأثیر بر فرصت دفاع و امکان بازسازی وضعیت پیشین است. این طبقه‌بندی به مرجع رسیدگی کمک می‌نماید میان اقدام‌های پیشگیرانه و جبرانی تناسب برقرار سازد. برای مثال، در رخداد کم‌خطر می‌توان ثبت گزارش و تقویت نظارت را کافی دانست؛ اما در رخداد مؤثر بر مهلت یا اصالت دلیل، تمدید مهلت، بررسی فنی مستقل و اجازه ارائه توضیح تکمیلی ضرورت پیدا می‌نماید.

خطر از درون سازمان نیز نباید نادیده گرفته گردد. کارمند یا پیمانکار دارای دسترسی گسترده می‌تواند بدون حمله بیرونی، اطلاعات را مشاهده، کپی یا تغییر دهد. پاسخ حقوقی مناسب، بر اصل کمینه‌سازی دسترسی، تفکیک وظایف، ثبت فعالیت مدیران سامانه و بازبینی دوره‌ای مجوزها استوار می‌گردد. همچنین باید معلوم باشد گزارش فنی رخداد را چه شخصی تهیه می‌نماید، چه مدت نگهداری می‌گردد و آیا طرفین می‌توانند بخش مرتبط با حق دفاع خود را مطالبه نمایند. حفاظت از گزارش امنیتی نباید به پوششی برای پنهان کردن خطای مؤثر بر پرونده تبدیل گردد؛ در عین حال، افشای بی‌ضابطه جزئیات فنی نیز نباید آسیب‌پذیری سامانه را افزایش دهد. بنابراین، افشای مرحله‌ای و دسترسی محدود، راه‌حل متوازن‌تری ارائه می‌نماید.

پاسخ به رخداد باید از لحظه کشف آغاز گردد و به پایان حمله محدود نماند. در مرحله نخست، حساب یا داده در معرض خطر باید مهار گردد؛ در مرحله دوم، نسخه‌ای از سوابق فنی بدون تغییر حفظ گردد؛ در مرحله سوم، دامنه اثر بر پرونده‌های مشخص و فرصت دفاع ارزیابی گردد؛ و در مرحله چهارم، نتیجه و اقدام جبرانی به اشخاص ذی‌نفع اطلاع داده گردد. اگر رخداد بر چند پرونده اثر بگذارد، اعلام عمومی وضعیت سامانه می‌تواند از رفتار نابرابر و اطلاع‌رسانی پراکنده جلوگیری نماید. مرجع رسیدگی همچنین باید مشخص نماید چه شخصی اختیار اعلام توقف مهلت را دارد و این تصمیم چگونه به کاربران ابلاغ می‌گردد. در امنیت فرایند داوری، حفاظت از سامانه‌ها، حفظ حریم خصوصی و سرعت رسیدگی ممکن است گاهی با یکدیگر تعارض پیدا کنند. این تعارض را می‌توان با تعیین مراحل واکنش به رخداد، تقسیم وظایف میان اشخاص مسئول و تدوین دستورالعمل‌های روشن برای اطلاع‌رسانی و ادامه رسیدگی مدیریت نمود (Chatterjee et al, 2024).

۳. ارزیابی حقوقی و الگوی پیشنهادی

دو بخش پیشین، جایگاه مرجع حل اختلافات فیفا و کارکرد سامانه‌های الکترونیکی را بررسی نمودند. این قسمت، میزان سازگاری ساختار موجود با دادرسی منصفانه، تمامیت ادله، محرمانگی و پاسخ‌گویی سایبری را ارزیابی می‌نماید و سپس الگوی حقوقی - امنیتی پیشنهادی را ارائه می‌نماید.

۳-۱. ارزیابی مقررات، گزارش‌ها و آرای مرتبط

قواعد آیینی مرجع حل اختلافات فیفا، ارتباطات الکترونیکی را به‌عنوان مسیر اصلی انجام بسیاری از اقدامات آیینی پذیرفته‌اند. ثبت دعوا، تبادل لوایح، ارائه ادله و اطلاع‌رسانی درباره تصمیمات از طریق بسترهای رسمی فیفا انجام می‌پذیرد و مهلت‌ها نیز بر اساس دریافت پیام یا ابلاغ رسمی محاسبه می‌گردند (FIFA, 2026, arts).

از جمله نقاط قوت این قواعد آن است که مسیر ارتباطات رسمی را مشخص کرده، امکان ثبت زمان و سابقه اقدامات را فراهم نموده و تبادل اسناد را منظم کرده‌اند. با این حال، در خصوص رخدادهایی مانند ازکارافتادن سامانه در پایان مهلت، سرقت حساب کاربری، افشای پرونده، تغییر سند یا مسئولیت پیمانکار فنی، مقررات تفصیلی کافی به چشم نمی‌خورد.

در «پرونده باشگاه استاک تروا علیه باشگاه تورینو و فیفا»^۱، موضوع اصلی به حق دریافت «حق آموزش بازیکن»^۲ و اطلاعات درج‌شده در «گذرنامه الکترونیکی بازیکن»^۳ مربوط بود. دیوان داور و ورزش در رسیدگی به اعتراض و در مرحله تجدید نظر بیان نمود؛ باشگاه مدعی باید شرایط لازم برای دریافت پاداش را اثبات نماید و صرف درج یا عدم درج داده در سامانه، بدون اثبات عناصر حقوقی، نتیجه را تعیین نمی‌نماید (FIFA & CAS, 2026).

اهمیت این رأی در آن است که داده سامانه‌ای را از دلیل قطعی به دلیل قابل ارزیابی تبدیل می‌نماید. اطلاعات سامانه ارزش اثباتی دارد، اما باید با اسناد قراردادی، وضعیت ثبت بازیکن و اقدامات طرفین تطبیق داده گردد.

در «پرونده باشگاه رایت تو دریم علیه فدراسیون بین‌المللی فوتبال (فیفا)»^۴، اختلاف درباره صحت اطلاعات مندرج در گذرنامه الکترونیکی بازیکن و استحقاق دریافت حق آموزش مطرح شد. دیوان داور و ورزش اعلام کرد هرگاه اعتراض به اطلاعاتی مربوط باشد که توسط یک فدراسیون عضو در سامانه ثبت شده و نتیجه رسیدگی مستقیماً بر حقوق یا منافع مالی آن فدراسیون اثر بگذارد، آن نهاد باید امکان مشارکت مؤثر و دفاع از موضع خود را داشته باشد. این رویکرد با اصل حق استماع و ضرورت حضور خواننده ضروری ارتباط دارد.

در یکی از آرای «دادگاه عالی فدرال سوئیس»^۵ نیز بیان گردید که حق دفاع شامل فرصت اظهارنظر درباره واقعیات اساسی، ارائه استدلال حقوقی، تقدیم دلیل، شرکت در جلسه و دسترسی به پرونده است. اگر اختلال سامانه موجب گردد طرف نتواند به پرونده دسترسی یابد یا دلیل خود را ارائه نماید، مسئله از سطح نقص فنی فراتر می‌رود و به حق دفاع مربوط می‌گردد.

^۱ Espérance Sportive Troyes Aube Champagne (ESTAC) v. Torino Football Club S.P.A. & Fédération Internationale de Football Association (FIFA)

^۲ Training Compensation

^۳ Electronic Player Passport (EPP)

^۴ سند الکترونیکی ایجادشده در سامانه TMS است که سابقه ثبت بازیکن را در طول دوران فعالیت او، از سال تقویمی دوازده سالگی، شامل باشگاه‌های محل ثبت، وضعیت بازیکن، نوع ثبت و طبقه‌بندی آموزشی باشگاه‌ها، گردآوری و نمایش می‌دهد. این اطلاعات برای شناسایی باشگاه‌های مستحق دریافت حق آموزش و محاسبه مبالغ مربوط به آن آموزش مورد استفاده قرار می‌گیرد؛ با این حال، درج اطلاعات در گذرنامه به تنهایی حق قطعی ایجاد نمی‌کند و استحقاق نهایی باید بر اساس مقررات فیفا و ادله موجود در پرونده احراز شود.

^۵ Right to Dream FC v. Fédération Internationale de Football Association (FIFA), CAS ۲۰۲۴/A/۱۰۴۲۷, Arbitral Award, ۲۳ May ۲۰۲۵

^۶ Federal Supreme Court of Switzerland

از مجموع مقررات و آرا می‌توان سه اصل را استخراج نمود: قابلیت انتساب، تمامیت داده و قابلیت اعتراض. رعایت این اصول، شرط لازم برای پذیرش داده سامانه‌ای به عنوان دلیل قابل اعتماد محسوب می‌گردد.

مقایسه این وضعیت با اصول شناخته شده در داوری بین المللی نشان می‌دهد که دیجیتالی بودن رسیدگی، از ضرورت رعایت تشریفات اساسی نمی‌کاهد. اصل فرصت معقول برای ارائه دعوا و دفاع، بی طرفی مرجع، امکان پاسخ به ادله طرف مقابل و وجود سابقه‌ای قابل بازبینی، در محیط سامانه‌ای نیز باید حفظ گردد. پروتکل‌های امنیت سایبری داوری بین المللی بر این مبنا، مسئولیت مشترک طرفین و نهاد رسیدگی را در حفاظت از داده، تعیین سطح دسترسی، استفاده از ابزارهای امن و گزارش رخداد مورد توجه قرار داده‌اند (International Council for Commercial Arbitration et al., 2022). برای مرجع حل اختلافات فیفا، استفاده از این تجربه می‌تواند به تدوین ضوابطی متناسب با حجم بالای پرونده‌ها و وضعیت فرامرزی کاربران کمک نماید؛ مشروط بر آنکه این ضوابط به بیان روشن در قواعد آیینی یا دستورالعمل رسمی اعلام گردند.

ارزیابی حقوقی باید میان نقصی که فقط نظم اداری را مختل می‌نماید و نقصی که نتیجه رسیدگی یا فرصت دفاع را تغییر می‌دهد، تمایز قائل گردد. برای نمونه، تأخیر در نمایش یک اعلان عمومی با ناتوانی در مشاهده لایحه طرف مقابل یکسان نیست؛ همان گونه که تغییر قالب ظاهری سند با تغییر محتوای آن تفاوت دارد. این تمایز در مرحله اعتراض اهمیت دارد، زیرا هر نقص شکلی الزاماً موجب نقض تصمیم نمی‌گردد و هر نقص فنی نیز بی‌اثر تلقی نمی‌گردد. معیار پیشنهادی آن است که مرجع رسیدگی، اثر واقعی نقص، امکان جبران، رفتار متعارف کاربر و اهمیت داده مورد اختلاف را بررسی نماید. چنین رویکردی از یک سو از بی اعتبارسازی خود کار اقدامات دیجیتال جلوگیری می‌نماید و از سوی دیگر، اجازه نمی‌دهد تشریفات فنی، نقض مؤثر حق دفاع را پنهان سازد.

در این ارزیابی، اصل تفسیر مضیق استثنای آیینی نیز اهمیت دارد. اگر سامانه مسیر اصلی ثبت را تعیین نموده باشد، نمی‌توان هر خطای کاربر را بدون توجه به راهنمایی ارائه شده، موجب سقوط حق دانست. در مقابل، اگر کاربر از مسیر معتبر و مهلت روشن آگاه بوده و بدون عذر قابل قبول اقدام ننموده باشد، امنیت سامانه نباید وسیله تمدید نامحدود مهلت گردد. سنجش حسن نیت، امکان اصلاح و میزان زیان، به تصمیم گیرنده اجازه می‌دهد میان نظم رسیدگی و عدالت موردی توازن برقرار نماید.

۲-۳. خالهای حقوقی و مسئولیت ناشی از نقض امنیت

مهم ترین خلأ حقوقی در ساختار موجود، فقدان نظام جامع برخورد با رخدادهای سایبری در جریان رسیدگی است. قواعد آیینی، وظایف عمومی طرفین در بررسی سامانه و رعایت مهلت‌ها را بیان نموده‌اند، اما برای استفاده غیرمجاز از داده یا سامانه برای تهدید و مطالبه پول، سرقت حساب نماینده، حذف سند، تغییر داده یا افشای پرونده، سازوکار تفصیلی ارائه ننموده‌اند.

این خلأ در پنج حوزه مشاهده می‌گردد: تشخیص رخداد، اعلام رخداد، حفظ ادله فنی، آثار رخداد بر مهلت‌ها و جبران زیان. مسئولیت نیز ممکن است میان نهاد اداره کننده سامانه، پیمانکار فنی، فدراسیون، باشگاه، نماینده و کاربر توزیع گردد. نباید هر اختلالی به صورت خودکار به نهاد رسیدگی منتسب گردد و نمی‌توان همه پیامدهای امنیتی را نیز به بی احتیاطی کاربر نسبت داد. تعیین مسئولیت باید بر اساس قابلیت پیش‌بینی، سطح حفاظت متعارف، میزان رعایت دستورالعمل‌ها، امکان جلوگیری از زیان، سرعت اعلام حادثه و شدت تأثیر رخداد بر حق دفاع صورت پذیرد.

راهکارهای جبرانی می‌تواند شامل تمدید مهلت، پذیرش دلیل تکمیلی، تعلیق آثار تصمیم، حفظ گزارش فنی، دسترسی محدود به سوابق ورود، ناشناس‌سازی داده‌های افشا شده و بازگشایی استثنایی رسیدگی باشد. بازگشایی باید فقط هنگامی صورت پذیرد که نقض امنیت، مؤثر و قابل انتساب باشد و طرف متضرر در ایجاد آن نقش تعیین‌کننده نداشته باشد.

تعیین مسئولیت در رخداد سایبری، به رابطه قراردادی کاربران با فیفا محدود نمی‌گردد. در یک زنجیره فنی، ممکن است سامانه توسط پیمانکار بیرونی میزبانی گردد، خدمات ذخیره‌سازی در کشور دیگری ارائه گردد و حساب کاربری به نماینده یا کارمند باشگاه واگذار گردد. در چنین ساختاری، مسئولیت باید بر پایه نقش واقعی هر بازیگر در تولید خطر و توانایی او برای جلوگیری از زیان تحلیل گردد. نهاد اداره‌کننده باید استانداردهای حداقلی امنیت، آموزش کاربران، کنترل دسترسی و ثبت وقایع را فراهم نماید؛ کاربر باید از واگذاری رمز و استفاده ناامن جلوگیری کند؛ و پیمانکار باید تعهدات قراردادی خود درباره محرمانگی، پشتیبان‌گیری، اعلام رخداد و همکاری در بررسی را اجرا نماید. فقدان تعیین این نقش‌ها، رسیدگی به اعتراض‌های سایبری را طولانی و غیرقابل پیش‌بینی می‌نماید.

در کنار مسئولیت، مسئله جبران نیز باید بر پایه شدت و قابلیت انتساب رخداد تنظیم گردد. تمدید مهلت زمانی مناسب است که اختلال در فاصله دفاع یا ثبت اقدام رخ داده باشد؛ پذیرش سند تکمیلی زمانی ضرورت پیدا می‌نماید که حذف یا عدم دسترسی به فایل ناشی از حادثه اثبات گردد؛ و تجدید رسیدگی فقط در وضعیتی توجیه دارد که رخداد، بر بخش اساسی تصمیم اثر گذاشته باشد. جبران نباید به ابزار تأخیر بی‌پایان تبدیل گردد، اما بار اثبات فنی نیز نباید به‌طور کامل بر دوش طرفی قرار گیرد که به گزارش‌های سامانه دسترسی ندارد. ایجاد مسیر اعتراض کوتاه و تخصصی، همراه با حفظ محرمانگی و تعیین مهلت پاسخ، می‌تواند میان قطعیت تصمیم و اصلاح خطای مؤثر تعادل برقرار نماید.

۳-۳. الگوی پیشنهادی حقوقی - امنیتی

الگوی پیشنهادی بر پنج لایه استوار می‌گردد. لایه نخست، حکمرانی و طبقه‌بندی ریسک است. پرونده‌های عادی، مالی، مرتبط با بازیکنان کم‌سن و حاوی اطلاعات پزشکی نباید از سطح حفاظت یکسان برخوردار باشند. میزان رمزگذاری، محدودیت دسترسی، مدت نگهداری و نظارت فنی باید با حساسیت اطلاعات تناسب داشته باشد. لایه دوم، احراز هویت و کنترل دسترسی است. دسترسی کاربران باید بر اساس نقش آنان تنظیم گردد و بازیکن، باشگاه، فدراسیون، وکیل، کارمند اداری و عضو مرجع رسیدگی نباید دسترسی یکسان داشته باشند. احراز هویت چندمرحله‌ای، هشدار ورود از دستگاه ناشناس و ثبت تغییرات حساب کاربری باید الزامی گردد.

لایه سوم، به تضمین تمامیت و قابلیت اثبات داده‌ها مربوط می‌شود. هر سند باید دارای شناسه‌ای یکتا و تاریخ و ساعت دقیق ثبت، ارسال، دریافت یا تغییر در سامانه باشد و سابقه تمامی تغییرات آن نیز ثبت گردد. نسخه اولیه سند باید حفظ شود و هرگونه اصلاح، جایگزینی یا حذف با ذکر زمان و شخص انجام‌دهنده در پرونده ثبت گردد. همچنین، طرفین باید بتوانند گواهی الکترونیکی ثبت و سابقه گردش سند را از سامانه دریافت نمایند.

لایه چهارم، استمرار فعالیت و پاسخ به رخداد است. برای سامانه‌ها باید نسخه پشتیبان مستقل، مرکز جایگزین، روش ارتباط اضطراری و امکان ثبت موقت درخواست‌ها پیش‌بینی گردد. در صورت اختلال گسترده، مرجع رسیدگی باید وضعیت سامانه و مهلت‌های تحت تأثیر را به طرفین اطلاع دهد و در صورت لزوم مهلت‌ها را تمدید نماید.

لایه پنجم، تضمین‌های آیینی و نظارت مستقل است. طرف باید بتواند در صورت ادعای اختلال یا نقض امنیت، درخواست بررسی مستقل نماید. در صورت تردید جدی درباره اصل داده، بار اثبات نباید به صورت مطلق بر دوش کاربر قرار گیرد؛ به‌ویژه هنگامی که داده در اختیار انحصاری نهاد رسیدگی یا پیمانکار فنی قرار داشته باشد.

الگوی مطلوب باید میان سرعت رسیدگی، امنیت اطلاعات، حق دفاع و قطعیت تصمیم تعادل ایجاد نماید. سرعت بدون امنیت اعتماد ایجاد نمی‌نماید؛ امنیت بدون دسترسی حق دفاع را محدود می‌سازد؛ و قطعیت بدون امکان جبران ممکن است به تثبیت بی‌عدالتی منجر گردد.

برای سنجش اجرای این الگو، شاخص‌های حقوقی و فنی باید در کنار هم قرار گیرند. از شاخص‌های فنی می‌توان به درصد دسترسی‌های چندمرحله‌ای، زمان کشف و اعلام رخداد، میزان موفقیت بازیابی نسخه پشتیبان و درصد پرونده‌های دارای سابقه تغییر اشاره نمود. از شاخص‌های حقوقی نیز می‌توان تعداد درخواست‌های تمدید مهلت ناشی از اختلال، موارد پذیرش دلیل تکمیلی، زمان پاسخ‌گویی به اعتراض امنیتی و میزان دسترسی طرفین به گزارش مؤثر را سنجید. گزارش دوره‌ای این شاخص‌ها، بدون افشای جزئیات آسیب‌پذیر، امکان نظارت بر عملکرد سامانه را فراهم می‌نماید. افزون بر آن، ممیزی مستقل باید فقط به بررسی تجهیزات محدود نگردد؛ بلکه باید بررسی نماید که آیا رخدادها بر حق دفاع، برابری طرفین و قابلیت بازیابی تصمیم اثر گذاشته‌اند یا خیر. این پیوند میان ممیزی فنی و ارزیابی حقوقی، از تبدیل امنیت به تشریقاتی صوری جلوگیری می‌نماید.

این الگو باید با اصل تناسب اجرا گردد و برای همه پرونده‌ها بار فنی یکسان ایجاد ننماید. پرونده‌ای که فقط یک ارتباط اداری در آن مبادله می‌گردد، به سطح حفاظتی پرونده حاوی داده پزشکی یا اطلاعات بازیکن کم‌سن نیاز ندارد؛ اما هیچ پرونده‌ای نباید از حداقل‌های احراز هویت، ثبت زمان و پشتیبان‌گیری محروم بماند. سطح‌بندی ریسک باید بر اساس نوع داده، ارزش اقتصادی، شمار کاربران، آثار احتمالی افشا و حساسیت مهلت تعیین گردد و در طول عمر پرونده قابل بازیابی باشد. همچنین، مقررات باید روشن نمایند که رعایت الزامات امنیتی، مانع استفاده از دلیل یا طرح دعوا برای شخصی نمی‌گردد که به دلیل ناتوانی فنی یا وضعیت خاص، نیازمند کمک متعارف است. عدالت دیجیتال زمانی تحقق می‌یابد که امنیت، دسترسی و امکان اصلاح خطا در کنار یکدیگر طراحی گردند.

در سطح حکمرانی، گزارش امنیتی باید به زبان حقوقی قابل استفاده برای تصمیم‌گیرنده تبدیل گردد. گزارش فنی می‌تواند زمان نفوذ، نشانی دستگاه، تغییرات داده و دامنه دسترسی را ثبت نماید؛ اما مرجع باید از آن نتیجه بگیرد که آیا فرصت دفاع از بین رفته، ابلاغ معتبر بوده یا دلیل نیازمند بررسی بیشتر است. این تبدیل داده فنی به نتیجه آیینی، نیازمند حضور کارشناس مستقل و امکان پرسش طرفین است. کارشناس نباید درباره اصل حق یا نتیجه دعوا تصمیم بگیرد، بلکه باید روش تولید و قابلیت اعتماد داده را توضیح دهد. چنین تفکیکی، هم از فنی‌سازی افراطی رسیدگی جلوگیری می‌نماید و هم اجازه نمی‌دهد تصمیم حقوقی بر برداشت نادرست از گزارش سامانه‌ای استوار گردد.

نتیجه‌گیری

پژوهش حاضر با هدف بررسی نقش سامانه‌های الکترونیکی و امنیت سایبری در فرایندهای مرجع حل اختلافات فیفا انجام گردید. پرسش اصلی پژوهش آن بود که سامانه‌های الکترونیکی و الزامات امنیت سایبری چگونه بر تضمین دادرسی منصفانه و اعتبار تصمیمات این نهاد اثر می‌گذارند.

نخستین یافته آن است که سامانه‌های الکترونیکی در مرجع حل اختلافات فیفا، نقش زیرساخت حقوقی پیدا نموده‌اند. ثبت دعوا، ارسال لایحه، بارگذاری دلیل، دریافت ابلاغ، محاسبه مهلت و پیگیری پرونده از طریق سامانه انجام می‌پذیرد. بنابراین، نقص سامانه می‌تواند بر حق دسترسی به رسیدگی و فرصت دفاع اثر بگذارد.

دومین یافته، ضرورت تفکیک میان وجود داده و اعتبار داده است. درج اطلاعات در سامانه ارزش اثباتی دارد، اما این ارزش مطلق نیست و باید با منشأ، زمان ایجاد، هویت ثبت‌کننده، سابقه تغییر و سایر اسناد پرونده تطبیق داده گردد.

سومین یافته آن است که امنیت سایبری بخشی از تضمین‌های دادرسی منصفانه محسوب می‌گردد. محرمانگی پرونده، تمامیت اسناد، دسترسی‌پذیری سامانه و قابلیت انتساب اقدامات کاربران، همگی با حق دفاع و برابری طرفین ارتباط دارند. چهارمین یافته به خلأهای مقرراتی مربوط است. قواعد فیفا استفاده از بسترهای الکترونیکی و ابلاغ دیجیتال را پذیرفته‌اند، اما درباره آثار دقیق رخدادهای امنیتی، تعلیق مهلت، حفظ سوابق فنی، مسئولیت پیمانکار و جبران زیان، نظام تفصیلی و جامعی ایجاد ننموده‌اند.

بر اساس یافته‌های پژوهش، فرضیه مقاله تأیید مشروط می‌گردد. سامانه‌های الکترونیکی می‌توانند سرعت، شفافیت و قابلیت اعتماد رسیدگی را افزایش دهند، اما تحقق این آثار به وجود تدابیر امنیتی، قواعد جبرانی و نظارت حقوقی وابسته است. پیشنهاد می‌گردد قواعد آیینی فیفا تعریف مستقلی از رخداد امنیتی ارائه نمایند، شیوه اعلام حادثه و حفظ سوابق فنی را مشخص سازند، امکان تمدید مهلت در صورت تأثیر اختلال بر حق دفاع را پیش‌بینی نمایند و برای داده‌های سامانه‌ای گواهی ثبت، مهر زمانی و سابقه تغییر ایجاد کنند. همچنین استفاده از احراز هویت چندمرحله‌ای، کنترل دسترسی مبتنی بر نقش، رمزگذاری، ثبت وقایع، نسخه پشتیبان مستقل و ممیزی دوره‌ای باید به الزامات حداقلی سامانه تبدیل گردد.

اجرای این پیشنهادها نیازمند یک دستورالعمل واحد برای کاربران، اعضای مرجع، دبیرخانه و پیمانکاران فنی است. در این دستورالعمل باید سطح‌بندی داده، روش ثبت و تحویل دلیل، زمان نگهداری سوابق، نحوه اعلام اختلال، مرجع تصمیم‌گیری درباره تمدید مهلت و شیوه دسترسی به گزارش فنی تعیین گردد. آموزش دوره‌ای نیز اهمیت دارد؛ زیرا بخشی از رخدادهای امنیتی از خطای انسانی، استفاده از گذرواژه تکراری یا ارسال سند به نشانی نادرست ناشی می‌گردد. آموزش، جایگزین کنترل فنی نیست، اما موجب می‌گردد کاربران آثار حقوقی اقدام دیجیتال را بهتر درک نمایند و در صورت بروز حادثه، گزارش دقیق‌تری ارائه دهند. در کنار آن، ارزیابی مستقل سالانه باید به‌عنوان شرط استمرار سامانه در نظر گرفته گردد تا اصلاحات امنیتی به واکنشی موردی پس از حادثه محدود نماند.

افزون بر الزامات درون سازمانی، فیفا باید در قراردادهای فنی خود نیز ضمانت اجراهای روشن پیش‌بینی نماید. تعهد پیمانکار به قابلیت دسترسی، پشتیبان‌گیری، اعلام فوری رخداد و همکاری در استخراج سوابق، باید با معیار قابل سنجش و مسئولیت متناسب همراه باشد. گزارش ممیزی، برنامه آزمون بازیابی و نتیجه بررسی رخدادهای باید در دوره‌های معین به دبیرخانه ارائه گردد. در صورت قصور مؤثر، واکنش نباید فقط به اصلاح فنی محدود گردد؛ بلکه آثار آن بر پرونده‌های

مشخص باید بررسی گردد و در صورت لزوم، طرفین از امکان جبران برخوردار شوند. چنین سازوکاری، امنیت را از یک وعده کلی به تعهد قابل ارزیابی تبدیل می‌نماید و اعتماد کاربران حرفه‌ای و نهادهای عضو را افزایش می‌دهد. از دیدگاه سیاست‌گذاری، این اصلاحات باید به تدریج و با اولویت پرونده‌های حساس اجرا گردند. نخست می‌توان ثبت دقیق زمان، صدور رسید، احراز هویت چندمرحله‌ای و مسیر ارتباط اضطراری را الزامی نمود؛ سپس نظام نگهداری داده، ممیزی مستقل و سازوکار جبران را توسعه داد. اجرای مرحله‌ای، هزینه تغییر را مدیریت می‌نماید و امکان دریافت بازخورد از کاربران را فراهم می‌سازد. در هر مرحله، نتیجه ارزیابی باید در دستورالعمل‌های بعدی انعکاس یابد تا قواعد سامانه با تجربه واقعی پرونده‌ها هماهنگ بماند.

در نهایت، مشروعیت رسیدگی دیجیتال فقط از سرعت و کاهش هزینه ناشی نمی‌گردد. رسیدگی الکترونیکی هنگامی اعتماد حقوقی طرفین را جلب می‌نماید که هویت آنان از حمایت کافی برخوردار باشد، اسناد قابلیت اعتماد داشته باشند، اطلاعات محرمانه باقی بمانند، مهلت‌های آیینی برای طرفین قابل پیش‌بینی باشند و در صورت بروز اختلال، راهکار جبران مؤثر در اختیار آنان قرار گیرد. بر این اساس، امنیت سایبری در مرجع حل اختلافات فیفا باید از سطح یک اقدام فنی فراتر رود و به عنوان یک اصل حقوقی و آیینی شناخته شود.

منابع فارسی

مقاله‌ها

- شریف‌زاده خرم، امیرحسین. (۱۴۰۴). بررسی اعتبار و قابلیت استناد ادله الکترونیک تولیدشده توسط الگوریتم‌ها در نظام دادرسی و حقوق سایبری. حقوق سایبری، ۲(۱)، ۳۴-۴۹.
- شعاعی، مرتضی، و اعراب شیانی، حجت. (۱۴۰۱). درآمدی بر حل و فصل اختلافات ورزش فوتبال در نظام ایران و بین‌الملل. تحقیقات حقوقی بین‌المللی، ۵۵(۱۵)، ۳۸۱-۳۶۳.
- صادقی‌نشاط، امیر. (۱۳۹۳). اعتبارسنجی اسناد الکترونیک. پژوهش حقوق خصوصی، ۲(۷)، ۶۴-۶۱.
- قرایی، تکتّم، هدایی، علیرضا، و اسحاقی، محمد. (۱۴۰۰). امکان‌سنجی استنادپذیری ادله الکترونیک در فقه، با نگاهی به قانون تجارت الکترونیک ایران. فقه و مبانی حقوق اسلامی، ۵۴(۲۱)، ۶۱-۴۶.
- قوانین
- قانون تجارت الکترونیک. (۱۳۸۲). جمهوری اسلامی ایران.

References

Books

- Blackaby, N., Partasides, C., Redfern, A., & Hunter, M. (2022). Redfern and Hunter on international arbitration (7th ed.). Oxford University Press.
- Born, G. B. (2021). International commercial arbitration (3rd ed., 3 vols.). Kluwer Law International.
- Katsh, E., & Rabinovich-Einy, O. (2017). Digital justice: Technology and the internet of disputes. Oxford University Press. doi: 10.1093/acprof:oso/9780190464585.001.0001
- Susskind, R. (2019). Online courts and the future of justice. Oxford University Press.

Articles

- Chatterjee, P., Singhanian, A., & Sharma, Y. S. (2024). Cybersecurity in arbitration: Balancing protection, privacy and regulation in the digital age. Asian Dispute Review, 26(1), 29–36.
- Chen, L. (2024). Will virtual hearings remain in post-pandemic international arbitration? International Journal for the Semiotics of Law, 37(3), 829–849. doi: 10.1007/s11196-023-10054-7
- Ferreira, D. B., & Gromova, E. A. (2023). Electronic evidence in arbitration proceedings: Empirical analysis and recommendations. Digital Evidence and Electronic Signature Law Review, 20, 30–39.
- Ferreira, D. B., & Gromova, E. A. (2024). Digital evidence: The admissibility of leaked and hacked evidence in arbitration proceedings. International Journal for the Semiotics of Law, 37(3), 903–922. doi: 10.1007/s11196-023-10014-1
- Gómez-Moreno, J. P. (2024). Advocacy for online proceedings: Features of the digital world and their role in how communication is shaped in remote international arbitration. International Journal for the Semiotics of Law, 37(3), 865–885. doi: 10.1007/s11196-023-10041-y
- Łagiewska, M., & Bhatia, V. K. (2024a). International arbitration in the digital world. International Journal for the Semiotics of Law, 37, 821–827. doi: 10.1007/s11196-024-10135-1
- Łagiewska, M. (2024b). New technologies in international arbitration: A game-changer in dispute resolution? International Journal for the Semiotics of Law, 37(3), 851–864. doi: 10.1007/s11196-023-10070-7
- Latifah, E., Bajrektarevic, A. H., & Imanullah, M. N. (2019). The shifting of alternative dispute resolution: From traditional form to the online dispute resolution. Brawijaya Law Journal, 6(1), 27–37. doi: 10.21776/ub.blj.2019.006.01.02
- Moreira, J. I., & Zhang, L. (2024). Assessing credibility in online arbitration hearings: Determining facts and justice by Zoom. International Journal for the Semiotics of Law, 37(3), 887–901. doi: 10.1007/s11196-023-10046-7
- Rabinovich-Einy, O., & Katsh, E. (2014). Digital justice: Reshaping boundaries in an online dispute resolution environment. International Journal of Online Dispute Resolution, 1(1), 5–36.

- Teramura, N., & Trakman, L. (2024). Confidentiality and privacy of arbitration in the digital era: Pies in the sky? *Arbitration International*, 40(3), 277–306. doi: 10.1093/arbint/aiae017
- Laws, Regulations, and Related Instruments
- Court of Arbitration for Sport. (2025). Code of sports-related arbitration.
- Fédération Internationale de Football Association. (2026). Procedural rules governing the Football Tribunal: January 2026 edition.
- International Council for Commercial Arbitration, New York City Bar Association, & CPR Institute. (2022). Protocol on cybersecurity in international arbitration.
- Reports and Frameworks
- Fédération Internationale de Football Association, & Court of Arbitration for Sport. (2026). CAS & Football annual report 2025.
- Fédération Internationale de Football Association. (2025). Football Tribunal report 2024/25.
- National Institute of Standards and Technology. (2024). The NIST cybersecurity framework 2.0.
- OECD. (2024). Online dispute resolution framework.
- Awards and Judicial Decisions
- Court of Arbitration for Sport (CAS). (2025, May 23). CAS 2024/A/10427: Right to Dream FC v. Fédération Internationale de Football Association (FIFA), arbitral award. Sole Arbitrator: Mark Andrew Hovell. Lausanne, Switzerland: Court of Arbitration for Sport.
- Court of Arbitration for Sport (CAS). (2025, April 17). CAS 2024/A/10551: Espérance Sportive Troyes Aube Champagne (ESTAC) v. Torino Football Club S.P.A. & Fédération Internationale de Football Association (FIFA), arbitral award. Sole Arbitrator: Manfred Nan. Lausanne, Switzerland: Court of Arbitration for Sport.
- Swiss Federal Supreme Court, First Civil Law Court. (2013, August 5). X. SA v. Y. SA, Judgment 4A_214/2013. Subject: Internal arbitration; right to be heard; arbitrariness. Lausanne, Switzerland.