VOL. 7 / Autumn 2025 and Winter 2026 / NO. 2 (Serial 14)
Jurisprudence and Legal Studies of Media Journal

Protecting Children's Digital Identity in Islamic Jurisprudence and case Law

Mohaddeseh Moeinifar[1] 0000-0003-1964-9347

Abstract

An individual's distinctiveness, a cornerstone of human existence since its inception, has evolved alongside historical, economic, social, and technological advancements in communication, gaining new dimensions. An individual's identity has effectively entered the digital realm, mirroring its real-world aspects. The presentation has evolved through novel tools that incorporate new dimensions enabled by technological advancements. In this transition, children have not been left behind; in fact, they often enter the digital world even before birth. Therefore, this paper employs descriptive and analytical methods and gathers data through library research, aiming to identify the dimensions of children's digital identity, along with the justifications for its legitimacy and the guarantees for its enforcement in Islamic jurisprudence and Iran's law. There is no consensus among experts on the concept of digital identity; definitions focus on individual characteristics and traits, data collections, and the financial aspects of data. Accordingly, children's digital identity can be summarized in three dimensions: characteristics or representation, data, and, finally, the economic dimension. Although the third dimension may not seem practical for children's digital identity, it strengthens it in other ways, namely by verifying their identity in non-financial matters. The foundations for the legitimacy of children's digital identity dimensions in Islamic jurisprudence can be found in certain Quranic verses. The foundations for civil enforcement guarantees for heretical children's digital identity can be found under jurisprudential rules such as "no harm," preserving order, respecting a Muslim's property, and the rule of authority. The foundations for criminal enforcement guarantees can be found in "discretionary punishment for every forbidden act" and "discretionary punishment as the ruler sees fit". Furthermore, in Iran's legal system, compensation for damages in this area may be based on Article 1 of the Civil Liability Law, and criminal liability for it may be derived from certain articles of the Computer Crimes Law.

Keywords: Identity, Digital Identity, Child, Data, Islamic Jurisprudence, Iran's Law.

1- Assistant professor of Theology and Islamic thought, Faculty of Islamic Sciences and Researches, Imam Khomeini International University, Qazvin, Iran moeinifar@isr.ikiu.ac.ir

دوفصلنامه
مطالعات فقه و حقوق رسانه
دانشکده غیردولتی – غیرانتفاعی رفاه

دوره ۷، شماره ۲(پیاپی ۱٤)
پاییز و زمستان ۱٤۰٤
صص: ۳۲۳-۳٦۰

حمایت از هویت دیجیتال کودکان در فقه و حقوق موضوعه

نوع مقاله: ترویجی
تاریخ دریافت: ۱٤۰٤/۰٤/۱٦
تاریخ پذیرش: ۱٤۰٤/۰۷/۲۱

محدثه معینی‌فر[۱]

چکیده

تشخص هر فرد از دیگری که رکن اساسی زندگی بشر از ابتدا تاکنون بوده، در گذر زمان و با تحولات تاریخی، اقتصادی و اجتماعی و توسعه فناوری‌های ارتباطی، ابعاد جدیدی یافته است؛ به‌این‌ترتیب که هویت هر فرد تقریباً با همان ابعاد واقعی وارد دنیای مجازی شده و با ابزارهای جدید، شکل عرضه آن متفاوت گشته و برخی ابعاد ناشی از توسعه فناوری نیز به آن افزوده شده است. در این گذار، کودکان نیز از این حرکت و تحول بازنمانده بلکه چه‌بسا پیش از تولد نیز وارد این دنیای مجازی شده‌اند. ازاین‌رو، این پژوهش با روش توصیفی و تحلیلی و گردآوری داده‌ها به روش کتابخانه‌ای در پی پاسخ به این پرسش است که ابعاد هویت دیجیتال کودکان، ادله مشروعیت و ضمانت اجرای آن، در فقه و حقوق ایران شامل چه مواردی است؟ درباره مفهوم هویت دیجیتال میان صاحب‌نظران اتفاق‌نظری وجود ندارد و تعاریف بر محور مشخصات و ممیزات فردی، مجموعه‌ای از داده‌ها و بُعد مالی داده‌ها عرضه شده‌اند و برهمین‌اساس، می‌توان هویت دیجیتال کودکان را در سه بُعد ویژگی‌ها یا نمایش، داده‌ها و درنهایت، بُعد مالی خلاصه کرد. هر چند بُعد سوم، در مورد هویت دیجیتال کودکان کاربردی به‌نظر نمی‌رسد؛ اما از جهات دیگر، یعنی احراز هویت دیجیتال آنان در موضوعات غیرمالی، هویت دیجیتال آنان را تقویت می‌کند. مبانی مشروعیت ابعاد هویت دیجیتال کودک در فقه را می‌توان در برخی آیات قرآن یافت و همچنین مبانی ضمانت اجرای مدنی نقض هویت دیجیتال کودکان را ذیل قواعد فقهی چون لاضرر، حفظ نظام، احترام مال مسلمان و قاعده تسلیط و مبانی ضمانت اجرای کیفری آن را در «التعزیر لکل عمل محرم» و «التعزیر بما یراه الحاکم» خلاصه کرد. به‌علاوه، در حقوق ایران نیز می‌توان جبران خسارت‌ها در این زمینه را مستند به ماده یک قانون مسئولیت مدنی کرد و مسئولیت کیفری در قبال آن را در برخی مواد قانون جرائم رایانه‌ای به‌دست آورد.

---

۱. استادیار گروه فقه و حقوق اسلامی، دانشکده علوم و تحقیقات اسلامی، دانشگاه بین‌المللی امام خمینی (ره)، قزوین، ایران moeinifar@isr.ikiu.ac.ir

کلیدواژه‌ها

هویت، هویت دیجیتال، کودک، داده، فقه، حقوق ایران.

مقدمه

هویت، اغلب با ویژگی‌های شخصیتی و ویژگی‌های بین‌فردی مانند نقش‌ها و روابطی فرد در تعاملات مختلف، مهارت‌های او و ارزش‌های شخصی یا باورهای اخلاقی فرد تمایز می‌یابد. توضیح چگونگی تمایز یک فرد از دیگران، بدون استفاده از هویت دشوار خواهد بود. هر چند وحدت ذاتی انسان به‌عنوان بدن، با یک هویت خاص در برون‌خط مطابقت دارد و تحت‌تأثیر بسیاری از عوامل خارج از مدیریت انسان مانند سن، نژاد و جنسیت است؛ اما اینترنت به دلیل ناشناس بودن و انعطاف‌پذیری، عرصه جدیدی را برای کاوش هویت فراهم کرده است. هویتی که به‌صورت برخط ایجاد شده است، لزوماً با هویت برون‌خط یا واقعی همان شخص مرتبط نیست؛ به‌عنوان‌مثال، یک فرد می‌تواند هویت بسیار فعال و شادی را در برخط داشته باشد، درحالی‌که مشخصه هویت متفاوت او در برون‌خط، خجالتی بودن است.

علاوه‌براین، ایجاد و تغییر هویت در برخط آسان است؛ درحالی‌که ایجاد و تغییر هویت در برون‌خط بسیار دشوار است. همچنین، زمان و تلاش کمتری برای بیان و اظهار هویت در برخط صرف می‌شود، درحالی‌که زمان و تلاش زیادی برای بیان و اظهار هویت در برون‌خط لازم است. برهمین‌اساس، هویت ایجاد شده در برخط را می‌توان هویت دیجیتال دانست که نه‌تنها درباره مفهوم آن در میان متخصصان رشته‌های مرتبط وفاقی وجود ندارد بلکه نسبت آن با کودک به‌عنوان موضوع داده یا صاحب داده، مباحث در این حوزه را پیچیده‌تر کرده است؛ زیرا کودکان به جهت آسیب‌پذیربودن بیشتر در معرض نقض هویت دیجیتال یا سرقت آن قرار دارند. به‌علاوه، تلاش کودکان برای عرضه شخصیتی متفاوت از خود در دنیای مجازی می‌تواند آسیب‌های دیگری چون قلدری سایبری، تحریک به خودکشی و مشکلات دیگری را برای آنان رقم بزند؛ بنابراین لازم است تا ابعاد هویت دیجیتال کودکان در فقه و حقوق ایران شناسایی شود و ادله مشروعیت و ضمانت اجرای مدنی و کیفری نقض آن نیز طرح شوند.

هویت دیجیتال مفهومی است که بر بستر اینترنت در شبکه‌های اجتماعی و رسانه‌های اجتماعی کاربرد دارد و می‌تواند در ارتباط با خود، آثار و تبعات مختلفی را برای فرد و

جامعه در پی داشته باشد. در سطح بین‌المللی، چهارچوب‌های حقوقی گوناگونی برای مقابله با چالش‌های مرتبط با سامانه‌های هویت دیجیتال ایجاد شده‌اند. نمونه برجسته، مقررات عمومی حفاظت از داده‌ها[1] است که چهارچوب نظارتی سخت‌گیرانه‌ای برای حفاظت از داده‌های شخصی در سراسر اتحادیه اروپا عرضه می‌کند. مقررات عمومی حفاظت از داده‌ها، دستورالعمل‌های روشنی در مورد جمع‌آوری، پردازش، ذخیره‌سازی و به‌اشتراک‌گذاری داده‌های شخصی تعیین می‌کند و اطمینان می‌دهد که افراد مدیریت اطلاعات شخصی خود را حفظ می‌کنند و در برابر سوءاستفاده محافظت می‌شوند. رویکرد این قانون به هویت دیجیتال بر اهمیت اخذ رضایت آگاهانه از افراد برای پردازش داده‌هایشان تأکید می‌کند که به‌ویژه با هویت‌های دیجیتال مرتبط است که اطلاعات حساس در آن دخیل هستند. یکی دیگر از چهارچوب‌های مهم بین‌المللی، دستورالعمل‌های سازمان ملل متحد در مورد هویت دیجیتال است که از گنجاندن ملاحظات حقوق بشری در طراحی و اجرای سامانه‌های هویت دیجیتال حمایت می‌کند. این دستورالعمل‌ها تأکید می‌کنند که سامانه‌های هویت دیجیتال باید به حق حریم خصوصی احترام بگذارند، عدم تبعیض را تضمین کنند و تسهیل‌کننده شمول اجتماعی باشند. دستورالعمل‌های سازمان ملل بر اهمیت اطمینان از دسترسی همه افراد، به‌ویژه گروه‌های به‌حاشیه‌رانده‌شده، به سامانه‌های هویت دیجیتال تأکید می‌کنند تا دسترسی برابر به خدمات دولتی، مزایای اجتماعی و سایر منابع حیاتی تضمین شود. آنها همچنین توصیه می‌کنند که سامانه‌های هویت در سرتاسر مرزها قابلیت همکاری داشته باشند تا همکاری بین‌المللی تسهیل شود و تحرک برای افرادی افزایش یابد که نیاز به دسترسی به خدمات در کشورهای مختلف دارند. رویکرد سازمان ملل به هویت دیجیتال بر نیاز به همکاری بین‌المللی برای ایجاد یک چهارچوب حقوقی مشترک تأکید دارد که به پیچیدگی‌های جریان داده‌های فرامرزی و تأیید هویت می‌پردازد *(Amini and Javidnejad, 2023, p. 51)*. در بررسی پیشینه حقوقی موضوع لازم به ذکر است که در این قوانین به موضوع هویت دیجیتال کودکان توجه ویژه شده است. برای نمونه، طبق قوانین اتحادیه اروپا، به‌ویژه مقررات عمومی حفاظت از داده، در این موضوع، کودکان زیر

1. GDPR

۱۶ سال نیاز به کسب رضایت قانونی والدین یا سرپرستان قانونی خود دارند؛ اما کشورهای عضو مجاز به کاهش این سن به ۱۳ سال نیز هستند. به‌علاوه، در ضرورت پژوهش حاضر می‌توان ادعا کرد که هر چند پژوهش کاملاً مرتبطی درباره آن وجود ندارد؛ اما برخی پژوهش‌های نسبتاً مرتبط شامل موارد زیر است:

لطیف‌زاده، مهدیه و قبولی درافشان، سیدمحمدمهدی (۱۴۰۲). معرفی هویت دیجیتال در متاورس، شناسایی چالش‌های حقوقی مربوط به آن و جست‌وجوی راه‌حل. مطالعات حقوق خصوصی، ۵۳(۲)، ۳۴۹-۳۷۲.

تمرکز این پژوهش بر موضوع هویت دیجیتال در فضای متاورس است و «سعی کرده است ضمن تعریف هویت دیجیتال در متاورس به چالش‌های حقوقی مربوط به هویت‌های مجازی در این محیط و ارائه راه‌حلی جهت پاسخ به معضلات پیش‌رو بپردازد. به‌موجب برآمد پژوهش، استفاده موردی از برخی قوانین و مقررات خاص مانند مقررات اروپایی حفاظت از داده و قانون هوش مصنوعی اتحادیه اروپا در کنار بهره‌مندی از فناوری بلاک‌چین باتوجه‌به استفاده از نوع متناسب آن، می‌تواند در خصوص حمایت‌های مؤثر از هویت‌های دیجیتال کارآمد باشد». تفاوت عمده این پژوهش با پژوهش حاضر آن است که هویت دیجیتال در پژوهش حاضر بسیار گسترده‌تر از آن است و تلاش کرده است فقه و حقوق ایران را به‌عنوان ساحت و کودک را به‌عنوان موضوع مدنظر قرار دهد. ازهمین‌رو، پرسش اساسی این پژوهش آن است که ابعاد هویت دیجیتال کودکان و ادله مشروعیت و ضمانت اجرای آن، در فقه و حقوق ایران شامل چه مواردی است؟ این پژوهش بر این فرض استوار است که هویت دیجیتال کودکان دامنه بسیار گسترده‌ای دارد که می‌تواند شامل ابعادی باشد که قائم به ویژگی‌های شخصی و بین‌فردی فرد است و ویژگی‌های دیگری را دربرمی‌گیرد که بخش مهمی از زندگی فرد را تشکیل می‌دهند و با استناد به ادله‌ای محکم می‌توان هویت دیجیتال کودکان را به‌رسمیت شناخت.

۱. مفهوم هویت دیجیتال

برای تبیین مفهوم هویت دیجیتال، تعاریف در جدول شماره ۱ تقسیم و بررسی شدند:

جدول شماره ۱: مفهوم هویت دیجیتال

انواع تعاریف	مرجع حقوقی یا فنی تعریف	عناصر تعریف	تحلیل تعریف
تعریف تک‌عنصری متمرکز بر ویژگی‌ها	قانون «نظام هویت معتبر در فضای مجازی کشور» ایران	مجموعه‌ای از اطلاعات پایه هویتی و صفت‌های معرف یک موجودیت واحد شامل هر شخص، گروه، شیء، خدمت، محتوا و مکان قابل‌شناسایی و مستقل	این تعریف بیشتر بر خود داده‌ها و اطلاعات با ویژگی وابستگی به هویت و صفات موجودیت تأکید دارد و تعریف به‌دور است.
تعریف دوعنصری از ویژگی‌ها و رابطه برخط	پروژه راهبرد ملی دولت آمریکا برای مدیریت هویت در فضای مجازی[۲]	مجموعه‌ای از ویژگی‌های یک موضوع در رابطه‌ای برخط (*Friedman, 2015, p.41; Ghadge, 2024:1*)	تعریف به‌دور است و تصویر روشنی از هویت دیجیتال نشان نمی‌دهد. هر چند اشاره کلی به این ویژگی‌ها کرده؛ اما روشن نساخته است که منظور از این ویژگی‌ها، چه ویژگی‌هایی است.
تعریف دوعنصری از نمایش و محیط دیجیتال	شورای فدرال مدیریت اطلاعات ایالات متحده	نمایش هویت در محیط دیجیتال (*Friedman, 2015, p.41; Ghadge, 2024:1*)	تعریف به‌دور است و تصویر روشنی از هویت دیجیتال نشان نمی‌دهد و تعریفی عام است که به ابعاد هویت دیجیتال اشاره‌ای ندارد. به‌علاوه، اگر تعبیر از هویت، تمایزهای فردی باشد، بازهم ابهام در مسئله قابل‌حل نیست؛ زیرا محور این تمایز روشن نیست.
	مایکروسافت	نمایش دیجیتال مجموعه‌ای از مطالبات یک موضوع دیجیتال درباره خودش یا	تعریف به‌دور است و تصویر روشنی از هویت دیجیتال نشان نمی‌دهد. مطالبه یا ادعا

2. The National Strategy on Trusted Identities in Cyberspace (NSTIC)

انواع تعاریف	مرجع حقوقی یا فنی تعریف	عناصر تعریف	تحلیل تعریف
		موضوع دیجیتال دیگر است (Holt and Malčić, 2015, p.159)	به‌عنوان اظهار صدق امری، معمولاً مورد مناقشه یا تردید است و هویت دیجیتال برای احراز هویت کاربران و پایگاه‌های اینترنتی در «چهارچوب سازگار و جامع» موردنظر مایکروسافت ملاحظه شده است.
	ــــــــــــ	هویت شخصی برخط[3] مفهومی است که بر این امر دلالت می‌کند که فرد چگونه خود را در فضای مجازی نشان می‌دهد (Levin & Mamlok, 2021, p.8).	
تعریف سه‌عنصری از هویت، صاحبان هویت و فضای مجازی	ــــــــــــ	هویتی برخط یا شبکه‌ای که توسط فرد، سازمان یا دستگاه الکترونیک در فضای مجازی ایجاد شده است. براین‌اساس، ممکن است کاربران بیش از یک هویت دیجیتال را در چندین سکو داشته باشند (Friedman, 2015, p.42)	این تعریف، گرفتار همان ابهام تعاریف قبلی است. به‌علاوه، این تعریف نیز مرز روشنی میان شخصیت دیجیتال و هویت دیجیتال قائل نیست و میان این دو مفهوم خلط کرده است.
تعریف سه‌عنصری از نمایش، صاحبان هویت و اینترنت	ــــــــــــ	نمایش فردی کاربر از خود در اینترنت که قابل‌گسترش به نهادهای بزرگ‌تری مانند شرکت‌ها است (Virginia	این تعریف نیز بر نمایش یا اظهار هویت یا ویژگی‌های هر شخص در فضای مجازی تأکید دارد و در نتیجه، گرفتار

3- Personal Identity Online (PIO)

انواع تعاریف	مرجع حقوقی یا فنی تعریف	عناصر تعریف	تحلیل تعریف
		(Phelan et al., 2013, p.251)	همان ابهام تعاریف قبلی است. به‌علاوه، این تعریف نیز مرز روشنی میان شخصیت دیجیتال و هویت دیجیتال قائل نیست و میان این دو مفهوم خلط کرده است.
تعریف چند عنصری از داده‌ها و سایر ویژگی‌های مربوط به داده‌ها و حرکت از توصیف یک فرد به‌سوی منشأ این تفاوت؛ یعنی داده‌ها	ــــــــــــ	مجموعه‌ای از داده‌ها است که شخص یا امری را به طور منحصربه‌فرد توصیف می‌کند (گاهی اوقات به‌عنوان موضوع یا موجودیت شناخته می‌شود) و حاوی اطلاعاتی در مورد روابط این موضوع با نهادهای دیگر است (Friedman, 2015, p.42). برخی نیز به این تعریف قیود دیگری چون «قابلیت اضافه‌کردن، به‌روزرسانی و حتی فراموش‌کردن داده‌ها» را افزوده‌اند و علاوه بر داده، آن را «مجموعه‌ای از کدها برای تعامل با آن داده‌ها و دنیای واقعی می‌دانند که بیش از پاسخ‌دهی خودکار و ساده مانند ربات توییتر هستند» (Savin-Baden, 2017, p.184)	مساوی دانستن هویت و شخصیت دیجیتال با داده، ناشی از نگاه فناورانه به این موضوعات است که از معایب آن می‌توان به تقلیل هویت و شخصیت دیجیتال در حد مجموعه‌ای از اطلاعات هر چند مهم دانست که ویژگی خاص دیگری ندارد؛ درحالی‌که بسیاری از این داده‌ها، قائم به وجود و شخصیت فرد هستند و حتی می‌توان ادعا کرد که از وجود و هستی فرد جدایی‌ناپذیر هستند و زندگی فرد بر محور آنها می‌چرخد.

انواع تعاریف	مرجع حقوقی یا فنی تعریف	عناصر تعریف	تحلیل تعریف
تعاریف تجاری از هویت دیجیتال	ــــــــــــ	هویت دیجیتال نمایانگر حضور منحصربه‌فرد و احراز هویت یک فرد یا نهاد در فضای برخط است. این هویت، شالوده‌ای برای امنیت برخط محسوب شده و دسترسی مجاز به خدمات دیجیتال را تضمین می‌کند. علاوه‌براین، هویت‌های دیجیتال تعاملات سفارشی و آسان را در فضای برخط امکان‌پذیر ساخته و انجام اموری مانند بانکداری برخط و تجارت الکترونیک را تسهیل می‌نمایند. مهم‌تر از همه، آنها با تسهیل ارتباطات و تراکنش‌های دیجیتال امن، اعتماد را تقویت کرده و به ایجاد یک زیست‌بوم دیجیتال ایمن، کارآمد و قابل‌اعتماد کمک می‌کنند» *(Hamid et al., 2023: 89)*	این تعریف علاوه بر تمرکز بر حضور منحصربه‌فرد، به موضوع احراز هویت نیز توجه دارد و درعین‌حال، بعد اقتصادی و تجاری هویت دیجیتال را مدنظر قرار داده و ازاین‌جهت، نسبت به تعاریف قبل و بعد خود کامل‌تر است.
	ــــــــــــ	اعتباری است که به فرد امکان می‌دهد اطلاعات شخصی، حق‌ها (استحقاق) و مجوزهای خود را به‌سرعت تأیید کند *(Hanson, 2018, p.11)* یا بیان مفهوم یک توکن منحصربه‌فرد	هرچند این تعاریف بر بعد اقتصادی و تجاری هویت دیجیتال تأکید دارند؛ اما به‌خوبی اهمیت این نوع از هویت را برای تداوم زندگی بشر کنونی نشان می‌دهند.

انواع تعاریف	مرجع حقوقی یا فنی تعریف	عناصر تعریف	تحلیل تعریف
		متقابل در هر سامانه یا مجموعه‌ای از سامانه‌های یکپارچه است که در فرایندی تجاری استفاده می‌شود؛ زیرا تعیین هویت دقیق عامل انسانی در آن سامانه یا زیرمجموعه‌ای از آن حیاتی است. هنگام استفاده از داده‌های ساخته شده در شبکه اجتماعی، داشتن دانش خاص در مورد اینکه چه کسی آن داده‌ها را ایجاد کرده است، از طریق یک نشانه یا هویت دیجیتال منحصربه‌فرد، به یک فرایند اجازه می‌دهد تا عاملی انسانی را به یک مجموعه خاص از کار یا تخصص مرتبط کند (*Jennings & Finkelstein, 2009, p.688*).	تعریف دوم از این گروه، ضمن تأکید بر جنبه تجاری هویت دیجیتال، بیشتر بر ایجاد هویت از سوی سازمان‌ها و دولت تأکید دارد.
	ــــــــــــ	هویت دیجیتال خوب، هویت تحت اختیار کاربر است که استفاده از آن، ساده و در همه‌جا قابل‌قبول و بسیار شبیه به کارت اعتباری یا تلفن همراه و برای مشاغل، قابل‌اعتماد و مقرون‌به‌صرفه است و قدرت انتخاب، تسلط و راحتی بیشتری را برای	

انواع تعاریف	مرجع حقوقی یا فنی تعریف	عناصر تعریف	تحلیل تعریف
		کاربران فراهم می‌کند. مصرف‌کنندگان با الگوهای نوظهور دیجیتال مثل شبکه هویت دیجیتال، می‌توانند حساب مؤسسه مالی خود را با تلفن همراه و کد ملی خود ترکیب کنند تا هویت دیجیتالی را ایجاد کنند که هنوز فیزیکی است (با سیم‌کارت در دستگاه تلفن همراه آنها) و در همه‌جا به‌آسانی قابل‌استفاده است (*Boysen, 2019, p.40*).	
	ــــــــــــ	مجموعه‌ای از اطلاعات است که به شکل دیجیتال برای اهداف طرح‌های خاص مالی ذخیره می‌شود. این مجموعه از اطلاعات که در ثبت هویت و سایر پایگاه‌های اطلاعاتی قابل‌دسترسی تحت این طرح موجود است، هویت پایگاه داده یک فرد است (*Sullivan, 2011, p.38*).	

یکی از موانع اصلی ایجاد یک‌لایه هویتی قابل‌دوام، این است که مفهوم توافق‌شده و واحدی برای هویت دیجیتال وجود ندارد و بهتر است مجموعه‌ای از انواع هویت دیجیتال را مدنظر قرار داد که هر کدام منحصر به ملت، شبکه، سکو یا فرهنگ خود هستند. علی‌رغم

وضوح نسبی مفهوم هویت دیجیتال، این هویت باید از نظر مادی برای کار در عرصه‌های خاص با فرهنگ‌های نظارتی ویژه سازگار شود. درمجموع، در ارزیابی این تعاریف باید اذعان کرد که هر یک از این تعاریف از منظر خود به موضوع هویت دیجیتال پرداخته‌اند. برخی به هویت یا منحصربه‌فرد بودن انسان در فضای مجازی اشاره داشته‌اند؛ درحالی‌که برخی به داده‌ها به‌عنوان مهم‌ترین بخش هویت دیجیتال نظر دارند و درنهایت، برخی به ویژگی‌های ثانویه مثل کاربرد این داده‌ها در معاملات برخط توجه کرده‌اند. به‌نظر می‌رسد باید تمامی ابعاد فوق را در تعریف هویت دیجیتال در نظر گرفت؛ اما آنچه هویت دیجیتال را متمایز می‌سازد منحصربه‌فرد بودن ویژگی‌های هر فرد در اینترنت و شبکه‌ها و رسانه‌های اجتماعی است که می‌تواند از دو نوع داده متفاوت از جهت ایجادکننده و جنس داده حاصل شود. برخی داده‌ها توسط خود فرد در فضای مجازی بارگذاری می‌شود و برخی نیز توسط سازمان‌ها و دولت برای فرد در فضای مجازی ملاحظه می‌شود. جنس داده‌ها نیز متفاوت است؛ برخی داده‌ها، صرفاً اطلاعات هویتی فرد هستند؛ اما برخی دیگر شامل فیلم‌ها یا عکس‌ها یا پیام‌های یک فرد در فضای مجازی‌اند که هویت فردی وی را در این فضا بازنمایی می‌کنند. داده‌های نوع نخست، معمولاً در معاملات برخط استفاده می‌شوند؛ درحالی‌که داده‌های نوع دوم بیشتر در شبکه‌ها و رسانه‌های اجتماعی استفاده می‌شوند و حتی اطلاعات هویتی فرد ممکن است در این شبکه‌ها و رسانه‌های اجتماعی پنهان باشد.

۲. ابعاد هویت دیجیتال کودک

هرچند همه ابعاد مدنظر در تعاریف فوق برای بزرگسالان قابل‌قبول است؛ اما برخی از این ابعاد برای کودکان از نظر حقوقی و فقهی قابل‌شناسایی است. برهمین‌اساس، باید ابتدا ابعاد هویت دیجیتال کودکان را مشخص کرد تا بتوان مباحث حقوقی و فقهی مرتبط را طرح کرد:

۲-۱. ابعاد هویت دیجیتال کودکان بر اساس تعاریف متمرکز بر ویژگی‌ها یا نمایش و محیط دیجیتال یا رابطه برخط

بخشی از تعاریف درباره مفهوم هویت دیجیتال، متمرکز بر نمایش ویژگی‌ها و صفات خاصی از یک فرد در فضای دیجیتال یا برخط است. براین‌اساس، هویت شخصی برخط، سبکی از رفتار فرد را در شبکه مشخص می‌کند که به فرد اجازه می‌دهد هویت خود را متفاوت از واقعیت، شکل و سپس نشان دهد. شخصیت امری است که شخص خودش آن را ایجاد می‌کند، الگویی که در ذهن او توسعه می‌یابد و هویت فردی او را شکل می‌دهد. این الگو در مکان‌های خاصی تکامل‌یافته است: جامعه، خانواده و فرهنگ. زندگی در شبکه مجازی به‌عنوان بخش جدایی‌ناپذیر زندگی واقعی در شکل‌گیری شخصیت افراد مهم است؛ زیرا صمیمانه‌ترین امری که یک فرد می‌تواند داشته باشد- خودش- به‌طور قابل‌توجهی، تحت‌تأثیر فناوری‌های دیجیتال است *(Levin and Mamlok, 2021, p.8)*. این نوع از هویت دیجیتال برای کودکان با هویت در معنای عام خود در ارتباط است که محل بحث نظریات بسیاری در علوم اجتماعی است و قابل تقسیم به هویت فردی، ملی، دینی، قومی و غیره است و در قالب حق بر هویت، فارغ از بستر عرضه آن، پیش‌ازاین از ابتدای تولد در معاهده حقوق کودک به‌رسمیت شناخته شده که ایران نیز به‌موجب ماده‌واحده الحاق اجازه دولت جمهوری اسلامی ایران در اسفند ۱۳۷۲ به صورت مشروط به این معاهده پیوسته است. پس آنچه در این میان تغییر کرده، تنها ساحت عرضه این حق است که از فضای واقعی به‌سوی فضای مجازی حرکت کرده و به‌دلیل حضور بر بستر اینترنت و ویژگی‌های خاص آن، مشخصات تمایزدهنده افراد از هم نیز ابعاد جدیدی یافته‌اند؛ البته آنچه در هویت دیجیتال با تأکید بر این ابعاد مدنظر است، بیشتر همان هویت فردی است و برهمین‌اساس، این تقسیمات از آن عرضه می‌شود:

الف- هویت‌های فضایی[۴]: هویت‌های متحرک و چندظرفیتی که توسط افراد در فضاهای رسانه‌ای مختلف، اعم از توییتر، فیس‌بوک، وبلاگ‌ها یا پست الکترونیک ایجاد می‌شوند و توسعه می‌یابند و در هر اجرا تمایل به ایجاد نوع متفاوتی از عملکرد وجود دارد که همواره به‌واسطه هنجارها، فرهنگ‌ها و ظرفیت‌های نرم‌افزار و کاربران آن فضاها هدایت می‌شود *(Savin-Baden, 2017, p.183)*.

4. Spatial identities

ب- هویت‌های شبکه‌ای[5]: هویت‌های شبکه‌ای به روش‌های چندبعدی و پیچیده در سراسر شبکه‌های برخط و برون‌خط مشترک در مدرسه، محل کار و اوقات فراغت ساخته می‌شوند و از این طریق هویت‌های فردی وجود می‌یابند. هویت‌های شبکه‌ای به‌طورخاص در شبکه‌های معین قرار دارند و در ارتباط با آنها هستند، نه مناطق فضایی وسیع‌تری که هویت‌های فضایی در آنها قرار دارند *(Savin-Baden, 2017, p.183)*.

ج- هویت‌های در سفر[6]: اغلب با این نوع هویت‌ها، حس بازی وجود دارد، مانند گردشگری هویت. این هویت‌ها هر چند ثابت نیستند؛ اما هیچ امر نادرست و گمراه‌کننده‌ای در مورد آنها وجود ندارد. درمقابل، آنها پویا هستند و هدف و دیدگاه مسافر محور دارند *(Savin-Baden, 2017, p.183)*.

د- هویت‌های پیوندی[7]: هویت‌هایی هستند که برای پیوند با جهان‌های بیرونی دیگر مانند دنیای مجازی، انجمن‌های گفتگو و دنیای بازی ایجاد می‌شوند. چنین هویت‌هایی ممکن است از طریق ایجاد آواتارها[8] یا هویت آواتارها برای بازی ایجاد شوند *(Savin-Baden, 2017, p.184)*.

هـ- هویت‌های کنار گذاشته شده[9]: وقتی افراد هویت‌های خود را در برخط جابه‌جا می‌کنند، به‌جای حذف هویت‌های زائد، به‌دنبال کنارگذاشتن آنها هستند. چنین هویت‌هایی به بخشی از فضاهای متروک اینترنت تبدیل می‌شوند، مانند آواتارهای فراموش‌شده، وبلاگ‌ها یا نمایه‌های فیس‌بوک رهاشده و هویت‌هایی که پس از مرگ اشخاص باقی می‌مانند *(Savin-Baden, 2017, p.184)*.

دامنه رفتار کاربر نسبت به هویت‌های دیجیتال خود می‌تواند از عملیات ایجاد، توسعه و گسترش و حرکت آن از یک محیط دیجیتال به محیط دیگر شروع شود و تا کنارگذاشتن آن هویت پیش رود. ویژگی بارز این هویت‌ها، موقتی بودن آنها است، هر چند در برخی از آنها تداوم مدنظر است. آنچه مسلم است، این است که این تقسیم مربوط به نوع نخست

---

5. Networked identities
6. Identities on tour
7. Bridged identities
۸. نماد مجازی یا نمایش گرافیکی از یک کاربر در محیط مجازی است.
9. Discarded identities

تعاریف است و در ارتباط با کودکان نیز معنا می‌یابد.

نوع دیگری که از این تعاریف به‌دست می‌آید، هویت اجتماعی دیجیتال است که در ذیل به آن اشاره شده است:

الف- هویت شخصی دیجیتال: هویت شخصی دیجیتال، دستاوردها، ویژگی‌ها و خصوصیات منحصربه‌فرد انسان است که برای بیان و اظهار آن ممکن است یک فرد نیاز به استفاده از هر یک از رسانه‌هایی (به‌عنوان‌مثال، وبلاگ و تابلوی پیام) داشته باشد که نشان‌دهنده آن است *(Kim and Que, 2007, p.98)*.

ب- هویت اجتماعی دیجیتال: باتوجه‌به بیان و اظهار هویت دیجیتال اجتماعی، آن را می‌توان با گروه‌های برخطی تعریف کرد که فرد به آنها تعلق دارد و شامل علائم و نمادهای دیجیتالی می‌شود که به یک هویت وابسته مانند لوگو یا رنگ تیم ورزشی اشاره می‌کنند *(Kim and Que, 2007, p.98)*. این دو تقسیم بر محور تعامل فرد با دیگران استوار است؛ زیرا در نوع نخست، صرفاً به عرضه خود برای دیگران می‌اندیشد؛ درحالی‌که در نوع دوم، از عرضه فراتر رفته و تعامل دوسویه را مدنظر قرار می‌دهد.

به نظر می‌رسد بیشتر این تعاریف، رخ‌نمای هر یک از افراد به‌ویژه کودکان را در سکوهای مختلف مدنظر قرار داده است که متمایزکننده او در هر سکو از دیگران است؛ برای نمونه، به نتایج یک پژوهش درباره حضور کودکان در فیس‌بوک و داشتن رخ‌نما در آن اشاره می‌شود: «اکثریت قریب‌به‌اتفاق کودکان پاسخ‌دهنده، در فیس‌بوک حساب کاربری دارند و هر چه سن کودک بیشتر باشد، احتمال‌داشتن رخ‌نمای شخصی برای او بیشتر است. دختران نسبت به پسران دوستان و عکس‌های بیشتری در رخ‌نمای فیس‌بوک خود دارند و تعداد دوستان با افزایش سن کاربران افزایش می‌یابد» *(Huk, 2016, p. 17)*. در این پژوهش، به‌خوبی وجه تمایز میان حضور دختران و پسران در فیس‌بوک به تصویر کشیده شده است. علاوه بر فیس‌بوک، سایر سکوها نیز محل حضور کودکان است و در ایران نیز کودکان علاوه بر سکوهای خارجی، در سکوهای داخلی نیز رخ‌نما دارند و به‌اصطلاح دارای هویت دیجیتال متمایزی هستند. گاهی هم والدین برای کودکان خود صفحه رخ‌نما در یک سکو را ایجاد و مدیریت می‌کنند. نکته مهم درباره این بعد آن است که این بُعد در دسترس

کودکان است و خود آنها می‌توانند آن را شکل دهند.

پس بر اساس این دیدگاه، هویت دیجیتال شامل ویژگی‌های منحصربه‌فردی است که افراد در اینترنت و بالتبع آن، شبکه‌ها و رسانه‌های اجتماعی از خود به منصه ظهور می‌رسانند. در این‌صورت، هویت دیجیتال کودک، تمامی اطلاعات موجود در اینترنت را دربرمی‌گیرد که اعم از آنچه است که خود کودک یا والدین او در شبکه‌ها یا رسانه‌های اجتماعی بارگذاری می‌کند یا دولت یا سازمان‌ها جمع‌آوری می‌کنند. این اطلاعات می‌تواند شامل ساده‌ترین اطلاعات مانند نام، جنسیت، تاریخ و محل تولد (و تاریخ مرگ)، یک قطعه عکس، امضا، آدرس محل سکونت و سایر اطلاعات زیست‌سنجی تا فیلم‌ها، ویدئوها، تصاویر، پیام‌های صوتی، پیام‌های متنی، اسناد و فایل‌های پی.دی.اف، پادکست‌ها، اخبار، زندگی‌نامه‌های مختصر (بیو)، آواتارها[۱۰]، روایت‌ها، آگهی‌ها یا اطلاعیه‌ها، بنرهای تبلیغاتی، اطلاع‌نگاشت یا گرافیک اطلاع‌رسان، نظرسنجی‌ها، گیف‌ها، برندها و نمایه‌های مختلف ساخته‌شده توسط خود فرد در شبکه‌ها و رسانه‌های اجتماعی با محتوای خانوادگی، آموزشی، کسب‌وکار و غیره البته با محوریت خود فرد حقیقی یا حقوقی باشد. پس هرگونه محتوای تعاملی و غیرتعاملی که ابرازکننده ویژگی‌های منحصربه‌فرد هر شخص باشد، می‌تواند به فراخور در شبکه‌ها و رسانه‌های اجتماعی به‌عنوان هویت دیجیتال فرد شناخته شود؛ زیرا محتوای تعاملی به شبکه‌های اجتماعی تعلق دارد، هرچند خالی از محتوای غیرتعاملی نیستند و محتوای غیرتعاملی در رسانه‌های اجتماعی منتشر می‌شوند.

۲-۲. ابعاد هویت دیجیتال کودکان بر اساس تعریف مبتنی بر داده‌ها و سایر ویژگی‌های مربوط به داده‌ها

برخی موضوع حق‌ها در فضای دیجیتال را داده‌ها می‌دانند (*Livingstone and Third, 2017, P 666.*) و ازاین‌رو، در تعریف هویت دیجیتال نیز، جنس تعریف را داده قرار داده و منظور از آن را هر نوع از داده می‌دانند که در ارتباط با یک فرد حقیقی یا حقوقی در اینترنت موجود است و درنتیجه، نتوانسته‌اند تمامی ابعاد هویت دیجیتال را در نظر بگیرند. این در حالی

۱۰. تصاویری هستند که کاربران در اینترنت و به‌خصوص در تالار گفتگو برای رخ‌نمای خود استفاده می‌کنند.

است که هویت دیجیتال فراتر از صرف داده است بلکه حاوی تلاش‌های فرد برای بازنمایی خود در شبکه‌ها و رسانه‌های اجتماعی است و حتی گاهی با هدف تأثیرگذاری بیشتر برای انتقال پیام‌ها، این بازنمایی در چند رسانه یا شبکه اجتماعی به نحو یکسان یا متفاوت تکرار می‌شود. در این تعریف، موضوع داده که کودک یا فرد بزرگسال است، منفعل ملاحظه شده است و هیچ نقشی برای او در این زمینه قائل نیست. این تعریف درواقع، حائل میان دو تعریف گروه نخست و گروه سوم است؛ زیرا داده‌ها در هر سه گروه تعاریف، نقش دارند؛ اما در تعاریف گروه نخست، کودک خود داده‌هایی را در سکوها بارگذاری می‌کند؛ اما در گروه سوم، این سازمان‌های دولتی یا خصوصی هستند که داده‌هایی را برای شناسایی افراد از همدیگر در نظر می‌گیرند.

۲-۳. ابعاد هویت دیجیتال کودکان بر اساس تعاریف تجاری از آن

هر چند تعریف چند عنصری از نمایش دیجیتال، احراز هویت، صاحبان هویت و تضمین خدمات دیجیتال مانند بانکداری دیجیتال در این تعاریف دیده می‌شود؛ اما این نوع از تعاریف بیشتر بر بعد تجاری و آثار مالی تأکید دارند و اقسامی را برای آن بر می‌شمارند:

الف- هویت تراکنش: هویت تراکنش فرد، بخشی از مجموعه اطلاعاتی است که هویت پایگاه‌داده یا هویت دیجیتال او را تشکیل می‌دهد و در زمان تراکنش عرضه می‌شود. هویت تراکنش فقط یک فرد را شناسایی نمی‌کند بلکه هویت تراکنش یک هویت را از بقیه افراد جامعه جدا می‌کند که دارای هویت ثبت شده هستند و پس از تأیید به سامانه اجازه می‌دهد تا با آن هویت ثبت شده تعامل کند. هویت پایگاه‌داده از طریق هویت تراکنش به یک فرد مرتبط می‌شود. هویت تراکنش علاوه بر اینکه سامانه را قادر می‌سازد تا با یک هویت ثبت‌شده خاص سروکار داشته باشد، دروازه ورود به هویت پایگاه‌داده را فراهم می‌کند. اطلاعات هویت پایگاه‌داده یک فرد مانند هویت تراکنش برای شناسایی او استفاده می‌شود، اما هویت پایگاه‌داده فعالیت‌هایی را نشان می‌دهد که داستانی را در مورد فرد مرتبط با هویت دیجیتال بیان می‌کند که می‌تواند بر نحوه تلقی افراد توسط افراد دیگر و سامانه تأثیر بگذارد *(Sullivan, 2011, p.38)*. هویت تراکنش همچنین ارتباط بین یک فرد و اطلاعاتی را که

هویت پایگاه‌داده او را تشکیل می‌دهد، از طریق «اطلاعات شناسایی»؛ یعنی امضای دست‌نویس، عکس و اطلاعات زیست‌سنجی فراهم می‌کند و حداقل اطلاعات موردنیاز برای انجام یک تراکنش، شامل نام، جنسیت، تاریخ و محل تولد است *(Sullivan, 2011, p.43)*.

ب- هویت معامله: هویت معامله، هویتی است که فرد برای معاملات استفاده می‌کند *(Sullivan, 2011, p.71)*.

ج- هویت تجاری: یکی از مهم‌ترین مؤلفه‌های هویت دیجیتال یک سازمان، هویت تجاری[11] است که ارتباط تنگاتنگی با شخصیت حقوقی دارد. هویت تجاری کیفیت درک مشتریان از آن نشان (برند) است؛ به‌عنوان‌مثال، ممکن است مشتریان برخی برندها را باکیفیت یا قابل‌اعتماد بدانند. شرکت این ویژگی‌ها را باید در محیط برخط به نمایش بگذارد تا هویت دیجیتال یک شرکت تقویت شود *(Virginia Phelan et al., 2013, p.251)*. هر چند این سه نوع هویت بر اساس بعد اقتصادی یا تجاری هویت دیجیتال مدنظر قرار دارند؛ اما تفاوت عمده‌ای میان آنها وجود دارد؛ زیرا هویت تراکنش و هویت معاملی مربوط به اشخاص حقیقی است؛ درحالی‌که هویت تجاری مربوط به اشخاص حقوقی است.

البته تأکید بر بُعد مالی، بدان‌معنا نیست که این نوع از تعاریف در مجال‌های دیگر نیز قابل‌طرح نیستند؛ زیرا «یکی از اهداف اصلی هویت دیجیتال، امکان تمایز یک موجودیت از سایر موجودیت‌ها است. هر نظام فناوری اطلاعات[12]، ابزارهای منحصربه‌فرد شناسایی و تمایز موجودیت‌ها را لازم دارد؛ به‌عنوان‌مثال، نشانی پست الکترونیک می‌تواند هویت دیجیتال منحصربه‌فرد یا شناسه قابل‌اعتماد برای کارمندان در یک شرکت باشد؛ هرچند چندان فایده‌ای برای احراز هویت دیجیتال ندارد» *(Friedman, 2015, p.42)* و آثار مالی برای آن متصور نیست. ازهمین‌رو، عناصر این بُعد از هویت دیجیتال را علی‌رغم عدم وجود مطالبی درباره آن در مکتوبات، می‌توان شامل موارد زیر دانست:

الف- رمزهای عبور: امروزه آنچه بر هویت دیجیتال تأثیرگذار است، رمزهای عبور هستند که تنها مانع دسترسی به سامانه‌ها و داده‌های حساس به‌شمار می‌روند. بااین‌حال،

11. Brand identity
12. IT

صرف‌نظر از اینکه گذرواژه‌ها طولانی هستند، چندین‌بار در دقیقه تغییر می‌کنند یا از نویسه‌های تصادفی تشکیل شده‌اند؛ اما به‌اندازه کافی امن نیستند تا داده‌ها را حفظ کنند *(Boysen, 2019, p.37)*.

ب- شبکه یا نظام هویت دیجیتال: هویت دیجیتال شباهت زیادی به شبکه برق دارد. هر سازمان عرضه‌کننده خدمات برخط در اینترنت، مولد هویت دیجیتال خود را اجرا می‌کند. فیس‌بوک، آمازون، نتفلیکس، گوگل، دولت‌ها، مدارس، بیمارستان‌ها، مؤسسات مالی و عرضه‌کنندگان ارتباطات راه دور، همگی گروه‌های خدمات هویتی خود را اجرا می‌کنند. امروزه، نخستین شبکه‌های هویت دیجیتال ظهور کرده‌اند که می‌تواند مصرف‌کنندگان را به فراتر از محدودیت رمزهای عبور سوق دهند تا بتوانند کارهای بیشتری را به‌صورت برخط انجام دهند و درعین‌حال، سازمان‌های ارائه‌دهنده خدمات نیز دیگر مجبور نیستند تولیدکننده‌های هویت دیجیتال خود را اجرا کنند و می‌توانند از مدیریت خدمات رمزهای عبورِ مخاطره‌آمیزِ تحتِ مالکیت و مدیریتِ خود خارج شوند. به‌علاوه، استفاده از سیستم فعلی برای مصرف‌کنندگان بسیار دشوار و هزینه‌های آن متغیر است. کسب‌وکارها، دولت‌ها، مؤسسات آموزشی و سازمان‌های مراقبت‌های بهداشتی در سرتاسر جهان مرتباً با نقض امنیت یا سرقت داده‌ها مواجه می‌شوند؛ زیرا هیچ سازمانی نمی‌تواند سرمایه‌گذاری هنگفت و موردنیاز را برای حفاظت، سهولت و خصوصی کردن هویت دیجیتال انجام دهد *(Boysen, 2019, p.39)*.

ج- خدمات تأیید تصویر[۱۳] **و تشخیص تصویر**[۱۴]: قابلیت تطبیق زیست‌سنجی ملی چهره افراد، پایه و اساس هویت دیجیتال است که بر اساس آن، این پایگاه‌داده‌های عکس‌های ملی و ایالتی را از طریق یک تبادل به هم متصل می‌کند و دارای دو جز کلیدی است: نخست، خدمات تأیید تصویر است که از تبادل برای تأیید هویت دیجیتال استفاده می‌کند و راستی‌آزمایی مبتنی بر تصویر است که عکس یک فرد را با تصویری که در یکی از سوابق دولتی آنها (مانند عکس پاسپورت) وجود دارد، مطابقت می‌دهد تا به تأیید هویت او کمک کند. جز دوم، خدمات تشخیص تصویر است که شناسایی مبتنی بر تصویر یک به چند

13. The Face Verification Service/FVS
14. FIS/ the Face Identification Service

است که عکس یک فرد ناشناس را با چند سوابق دولتی تطبیق می‌دهد تا به شناسایی هویت آنها کمک کند *(Hanson, 2018, p.4)*.

د- مجوز دسترسی: بنا بر نظر برخی، هویت دیجیتال از نظر فنی، به دو بخش «احراز هویت» (شما چه کسی هستید؟) و «مجوز دسترسی» (چه کارهایی می‌توانید انجام دهید؟) تقسیم می‌شود. این اصطلاح به طور متناوب هم برای فناوری‌های شناسایی و هم مدیریت شناسایی به‌کاررفته است؛ درحالی‌که مورد نخست، به‌طورکلی، به رویه‌ها و ابزارهای فناوری مورداستفاده برای شناسایی شخص اشاره دارد و مورد دوم، تمام فرایندهای فنی و سازمانی را توصیف می‌کند که تضمین می‌کنند تنها کاربران مجاز و احراز هویت شده به خدمات ارائه شده دسترسی داشته باشند *(Giannopoulou, 2023: 18)*.

هر چند برخی بر این باورند که بین هویت و تشخیص یا شناسایی هویت تفاوت وجود دارد و شناسایی تنها بخشی از دو فرایند مورداستفاده برای ایجاد هویت؛ یعنی احراز هویت اولیه در زمان ثبت‌نام و دوم تأیید هویت است که در زمان معامله انجام می‌شود *(Sullivan, 2011, p.44)*؛ اما در یک جمع‌بندی می‌توان دریافت که محور ملاحظه این عناصر، همان موضوع شناسایی هویت افراد از یکدیگر است؛ ازهمین‌رو، رمزهای عبور یا نظام هویت دیجیتال و خدمات تأیید و تشخیص تصویر در اینجا مدنظر قرار گرفته‌اند و این موارد، عناصری هستند که می‌توانند در احراز هویت فرد مؤثر باشند؛ زیرا آنچه سبب تمایز می‌شود صرف وجود داده‌ها نیست بلکه مسیر احراز هویت بسیار مهم‌تر از داده‌هایی است که در شبکه‌ها و رسانه‌های اجتماعی وجود دارد؛ بنابراین، به نظر می‌رسد توجه به ابعاد مالی و اقتصادی هویت دیجیتال سبب شده است تا تمایز بین‌فردی در فضای مجازی حائز اهمیت باشد و بدون احراز این شاخصه‌ها، تفاوت در هویت دیجیتال معنایی ندارد.

نکته مهم این است که علی‌رغم بُعد تجاری و مالی این تعاریف و همچنین، رویکرد فقه و حقوق ایران نسبت به معاملات یا انواع دیگر تعاملات مالی کودک که این بُعد از هویت دیجیتال را در قبال کودکان فاقد کارکرد می‌کند، می‌توان از عناصر هویت دیجیتال بهره برد و این بُعد را به ترتیب دیگری برای کودکان ملاحظه کرد. این بُعد از هویت دیجیتال که به‌شدت وابسته به فرایند احراز است، منحصراً در امور مالی انجام نمی‌شود. بسیاری از

امور است که منوط به احراز هویت دیجیتال هستند، مانند پایگاه‌های داده کودکان که مربوط به خدمات دولت الکترونیک است و شامل محتوایی چون نام، نام خانوادگی، جنسیت، تاریخ و محل تولد (و تاریخ مرگ)، یک قطعه عکس، امضا، نام پدر، شماره ملی، شماره شناسنامه، نشانی محل سکونت و سایر اطلاعات زیست‌سنجی است که نقش اساسی در احراز هویت برای انجام تراکنش‌های بانکی و معاملات را دارد. پس بر اساس این دیدگاه، دامنه اطلاعات وارد شده توسط فرد یا گردآوری شده توسط دولت‌ها یا سازمان‌های مرتبط محدودتر خواهد شد. درنهایت باید دانست که با به‌روزرسانی اطلاعات و جمع‌آوری اطلاعات جدید، محتوای هویت دیجیتال، ثابت نیست بلکه طی فرایند زمانی این داده‌ها دائماً در حال تغییر هستند. برخی داده‌ها به‌حسب شرایط حذف می‌شوند؛ درحالی‌که داده‌های دیگری به هویت پایگاه‌داده فرد اضافه می‌شوند؛ بنابراین، متعلقات هویت دیجیتال می‌تواند از پیش از تولد تا پس از مرگ، محل توجه و حمایت قانون‌گذار باشند.

۳. مبانی مشروعیت ابعاد هویت دیجیتال کودک در فقه

در تعلق برخی اطلاعات در پایگاه‌داده یا مربوط به هویت دیجیتال شامل جنسیت، تاریخ و محل تولد (و تاریخ مرگ) و معمولاً حداقل یک قطعه عکس، امضا و سایر اطلاعات زیست‌سنجی که کاملاً مختص به هر فرد اعم از کودک و بالغ است و فقط به شکلی خاص و در فضایی خاص ثبت و ضبط می‌شوند، تردیدی وجود ندارد. چه‌بسا بتوان با استناد به آیاتی خاص بتوان تعلق آنها به فرد و سپس مشروعیت این تعلق را اثبات کرد:

آیه نخست: «وَمِنْ آيَاتِهِ خَلْقُ السَّمَاوَاتِ وَالْأَرْضِ وَاخْتِلَافُ أَلْسِنَتِكُمْ وَأَلْوَانِكُمْ إِنَّ فِي ذَٰلِكَ لَآيَاتٍ لِلْعَالِمِينَ؛ و از نشانه‌های [قدرت و ربوبیت] او آفرینش آسمان‌ها و زمین و اختلاف و گوناگونی زبان‌ها و رنگ‌های شماست؛ بی‌تردید در این [واقعیات] نشانه‌هایی است برای دانایان» *(سوره روم: آیه ۲۲)*.

در برخی تفاسیر، دلیل این اختلاف زبان و رنگ را این‌گونه بیان کرده‌اند: «اگر این نوع اختلاف نمی‌بود، هر آینه به سبب تشاکل، اختلال در نظام نوع بشر و تنظیم امور عالم واقع می‌گردید» *(حسینی شاه‌عبدالعظیمی، ۱۳۶۳، ج۱۰، ص.۲۸۵؛ ثقفی تهرانی، ۱۳۹۸، ج٤، ص.۲۵۲)*. اشاره به

اختلال نظام در تفسیر این آیه خود می‌تواند ثابت کند که شناسایی هر شخص به‌واسطه هویت به‌طورکلی و هویت دیجیتال به طور اخص امری ضروری برای هر جامعه است.

آیه دوم: «بَلَى قَادِرِينَ عَلَى أَنْ نُسَوِّيَ بَنَانَهُ؛ چرا درحالی‌که تواناییم که [خطوط] سر انگشتانش را درست و نیکو بازسازی کنیم» *(سوره قیامت: آیه ٤)*.

این آیه ضمن نشان‌دادن قدرت حق‌تعالی در بازگرداندن اثر انگشت انسان‌ها، به تعبیر برخی مفسران «می‌تواند اشاره لطیفی به خطوط سرانگشت انسان‌ها باشد که می‌گویند کمتر انسانی در روی زمین پیدا می‌شود که خطوط سرانگشت او با دیگری یکسان باشد. به‌تعبیردیگر، خطوط ظریف و پیچیده‌ای که در سرانگشتان هر انسانی نقش بسته، معرّف شخص او است. به‌همین‌دلیل در عصر ما «انگشت‌نگاری» به‌عنوان راهی برای شناسایی اشخاص و به‌ویژه مُجرمان مطرح است» *(مکارم شیرازی، ١٣٧٤، ج٢٥، صص.٢٧٨– ٢٧٩)*. این اشاره لطیف بر لزوم تمایز انسان‌ها از همدیگر به‌عنوان یک اصل اساسی در آفرینش الهی اشاره دارد که می‌تواند در موضوع هویت دیجیتال نیز کاربرد داشته باشد؛ زیرا یکی از مواردی که می‌تواند همچون تمایز چهره افراد از همدیگر، احراز هویت در فضای دیجیتال را تسریع کند، وجود اثر انگشت فرد به‌عنوان یکی از داده‌های هویت دیجیتال است. این ویژگی که مانند چهره و موارد مشابه قائم به شخص اعم از کودک و بالغ است، نقش اساسی در شکل‌گیری هویت فردی و سپس هویت دیجیتال دارد؛ زیرا هر کسی قطعاً نسبت به این نوع از داده حق مسلم دارد تا مانع نقض هویت دیجیتال خود شود.

آیه سوم: «وَمِنَ النَّاسِ وَالدَّوَابِّ وَالْأَنْعَامِ مُخْتَلِفٌ أَلْوَانُهُ كَذَلِكَ إِنَّمَا يَخْشَى اللَّهَ مِنْ عِبَادِهِ الْعُلَمَاءُ إِنَّ اللَّهَ عَزِيزٌ غَفُورٌ؛ و نیز از انسان‌ها و جنبدگان و چهارپایان [مانند میوه‌ها و راه‌های کوهستانی] رنگ‌های گوناگون وجود دارد. از بندگان خدا فقط دانشمندان از او می‌ترسند؛ یقیناً خدا توانای شکست‌ناپذیر و بسیار آمرزنده است» *(سوره فاطر: آیه ٢٨)*.

برخی در تفسیر این آیه بیان می‌کنند: «بعضی سفیدرنگ، بعضی سیاه‌رنگ، بعضی موی سرسیاه، بعضی زرد، به‌علاوه اختلاف شکلی از زیبایی و بدگلی و از حیث اخلاق و ذکاوت از حیث عقل و شعور و کند فهمی و جهات دیگر و از غرائب است که اینکه افراد بشر با اینکه اعضا و جوارح آنها به‌جا و به‌موقع است، بسیار کم اتفاق می‌افتد که دو نفر

از جمیع جهات شبیه هم باشند» *(طیب، ۱۳۷۸، ج۱۵، ص۲۵)*. این عبارات به‌خوبی نشان‌دهنده تفاوت انسان‌ها در آفرینش است و درعین‌حال، لزوم آن را نیز اثبات می‌کند. هویت در معنای اعم و هویت دیجیتال نیز خود نوعی از این تفاوت‌گذاری است. به‌علاوه، اگر لزوم تفاوت میان انسان‌ها به دلیل مانعیت از اختلال نظام به‌عنوان مناط حکم (شرعی بودن شناسایی هویت دیجیتال) اثبات شود، به قیاس اولویت می‌توان اثبات کرد که این مناط در هویت دیجیتال نسبت به هویت فردی شدیدتر است و به‌طریق‌اولی، برای مشروعیت شناسایی هویت دیجیتال کاربرد بیشتری دارد. به‌ویژه با وجود موضوع دولت الکترونیک و طرح مفاهیمی چون شهروند الکترونیک، وجود هویت دیجیتال از ضروریات زندگی کنونی بشر است؛ البته ناگفته نماند آنچه در حوزه دولت الکترونیک و شهروندی الکترونیک مهم است، همان داده‌ها و اطلاعات قائم به شخص و نیازمند احراز است و بقیه ابعاد و احوالات مربوط به آن که در مطالب فوق به آنها اشاره شد، به‌ویژه آن ابعادی که بیشتر جنبه غیررسمی دارند، چندان در این حوزه جایگاهی ندارند و بیشتر توصیف‌کننده احوالات زندگی فرد هستند تا خود فرد؛ البته این نوع از داده‌ها نیز معمولاً موضوع تجارت داده هستند؛ زیرا در حوزه شناخت مذاق فرد و تبلیغات و فروش کالاها بسیار مؤثر هستند.

۴. ضمانت اجرای نقض هویت دیجیتال کودکان در فقه

هویت دیجیتال در برخی موارد بسیار فراتر از یک خوداظهاری در اینترنت است و با زندگی انسان پیوند خورده است. ازهمین‌رو، دو گروه از قواعد فقه در این موضوع قابل‌طرح هستند. گروه نخست، شامل مواردی چون قاعده لاضرر، حفظ نظام، قاعده احترام مال مسلمان و قاعده تسلیط هستند که مبانی ضمانت اجرای مدنی حفاظت از هویت دیجیتال کودک را دربرمی‌گیرند. گروه دوم، شامل «التعزیر لکل عمل محرم» و «التعزیر بما یراه الحاکم» است که مبانی ضمانت اجرای کیفری آن را اثبات می‌کند.

۴-۱. مبانی ضمانت اجرای مدنی نقض هویت دیجیتال کودکان در فقه

این قواعد شامل موارد ذیل است:

۴-۱-۱. قاعده لا ضرر

قاعده لاضرر که برگرفته از حدیث مشهور نبوی: «لا ضرر و لاضرار فی الاسلام» *(کلینی، ۱٤۰۷، ج۱۰، ص.٤۸۳)*، هر چند با نقل‌های متفاوت است که در ابواب مختلف عبادات و معاملات کاربرد دارد و در مسائل مستحدثه نیز راهگشا است. مستندات قاعده در آیات، روایات، عقل و سیره عقلا خلاصه می‌شود. هر چند نحوه استدلال فقیهان شیعه به آن متفاوت است؛ اما از مدلول و مفهوم کلی قاعده و برخی نظرها می‌توان نهی از رساندن ضرر به خود و دیگری و لزوم تدارک و جبران ضرر را استفاده کرد؛ زیرا طبق تفسیر امام خمینی(ره) «سلطه‌ای که موجب زیان رسانیدن و در تنگنا قرار دادن دیگری شود، جایز و نافذ نیست» *(سبحانی، بی‌تا، ج۳، ص.۱۲٦)*. پس بر این مبنا و مبنای نفی احکام ضرری، قاعده لاضرر قابل استناد در موضوع جبران خسارت ناشی از نقض هویت دیجیتال کودکان نخواهد بود؛ اما بر اساس تفاسیر «نفی ضرر بدون جبران آن» *(فاضل تونی، ۱٤۱۲ق، ص.۱۹٤)* و «حکمی فرعی تکلیفی؛ یعنی حرمت اضرار به غیر» *(شریعت اصفهانی، بی‌تا، صص.۱۸-۱۹؛ مکارم شیرازی، ۱۳۷۰، ج۱، ص.۵۹)* می‌توان از حرمت اضرار به دیگران و سپس لزوم تدارک آن سخن گفت.

۴-۱-۲. قاعده حفظ نظام

متقدمان شیعه به این قاعده اشاره نداشته؛ اما برخی فقیهان، «وجوب حفظ نظام» *(خویی، بی‌تا، ج۲، ص.۵)* «لزوم ما یتوقف علیه حفظ النظام» *(مکارم شیرازی، ۱٤۲۵ق، ج۱، ص.۵۰۳)* و «اختلال نظام» *(انصاری، ۱٤۱۵ق، ص.٦۸؛ آشتیانی، ۱٤۰٤ق، ص.۵۱)* را به‌عنوان قاعده فقهی مطرح کرده‌اند که شامل چهار معنای «منظم بودن زندگی بشر و رفع اختلال و هرج‌ومرج» *(حلی، ۱۳۸۷، ج ۱، صص.۳ و ۲۵۰؛ شهید ثانی، ۱٤۱۳، ج۱، ص.۱۱؛ سبزواری، ۱٤۲۳ق، ج۲، ص.٦٦۵)*، حفظ کشور اسلامی مسلمانان از هجوم دشمنان و حفظ موجودیت اسلام و مسلمانان در برابر کفار *(جزائری، بی‌تا، ص.۱۹۸؛ خمینی، ۱٤۲۱ق، ج۲، ص.٦۲۰)*، حفظ حکومت یا همان نظام سیاسی به‌ویژه نظام اسلامی *(بحرانی، بی‌تا، ج۹، ص.٤۲۸)* و حفظ نظام عالم و حفظ شرایع، ادیان و علم» *(اصفهانی (فاضل هندی)، ۱٤۱٦ق، ج۱۰، ص.۳۵۲؛ کاشف الغطا(الف)، بی‌تا، ج۱، ص.۳۰؛ صاحب جواهر، ۱۳٦۲، ج۲۱، ص.۳۸٤)* است. مدارک این قاعده، شامل عقل و روایات است و شرط جریان این قاعده

از دیدگاه صاحب‌نظران گروه نخست، احراز توقف حفظ نظام نوع مردم و اغلب آنان بر انجام فعلی است که با این قاعده برای آن استدلال می‌شود و اختلال نظام بر اثر ترک آن فعل یا بالعکس نیز باید اثبات شود. در غیر این صورت، تا زمانی که این احراز حاصل نشود، این قاعده جاری نمی‌شود؛ زیرا موضوع حکم عقل تحقق نمی‌یابد *(سیفی، ۱٤۲۵ق، ج۱، ص.۱۲)*. به‌علاوه، جریان این قاعده نباید در نظام‌های جزئی باشد بلکه جریان آن باید در نظام‌های کلی باشد *(سیفی، ۱٤۲۵ق، ج۱، صص.۲۰-۲۱)*.

باتوجه‌به سه معنای نخست، می‌توان بر شناسایی هویت دیجیتال برای کودکان صحه گذاشت. بر اساس معنای نخست، رفع اختلال از زندگی بشر که امروزه وابستگی شدیدی به اینترنت و فضای مجازی دارد، تنها با به‌رسمیت‌شناختن هویت دیجیتال برای هر فرد حتی کودکان نسبت به آن میسر می‌شود. سرقت یا جعل هویت دیجیتال فرد، نظام نوع بشر را با اختلال جدی روبه‌رو می‌کند؛ زیرا بسیاری از خدمات دولت الکترونیک مبتنی بر هویت دیجیتال افراد است و کودکان نیز نمی‌توانند از این خدمات بی‌بهره باشند؛ هر چند خود نتوانند به‌صورت مستقیم برای دریافت این خدمات اقدام کنند.

بر اساس معنای دوم نیز حفظ کشور اسلامی مسلمانان و موجودیت اسلام، منوط به ملزوماتی است که باید نسبت به اینترنت، فضای مجازی، شبکه‌ها و رسانه‌های اجتماعی وجود داشته باشد تا این هدف مهم تأمین شود. یکی از این ملزومات، توجه به هویت دیجیتال کودکان در اینترنت است؛ زیرا مخاطرات حضور کودکان در فضای مجازی بسیار زیاد است. بر اساس معنای سوم، حفظ حکومت اسلامی نیز درحال‌حاضر، در گرو حکمرانی صحیح و درست فضای مجازی با مشارکت خود مردم و با توجه ویژه به کودکان است.

۴-۱-۳. قاعده احترام مال مسلمان

منظور از احترام به مال مسلمان در اینجا، مصونیت آن از تصرف رایگان و تعدی به آن است؛ به این معنا که مال مسلمان محترم است و تجاوز و تعدی به آن جایز نیست. ادله حجیت این قاعده، روایات، تسالم و سیره متشرعه هستند *(طباطبایی یزدی، ۱۳۷۸، ج۲، ص.۱۷۳؛ مصطفوی، ۱٤۲۱ق، ج۱، صص.۲٤-۲۵)*. از این قاعده، به قیاس اولویت می‌توان حرمت‌گذاری

نسبت به سایر متعلقات انسان از جمله هویت دیجیتال را به‌دست آورد. هویت دیجیتال قطعاً از متعلقات انسان و تحت حمایت اسلام است؛ اما شاید در ابتدا به نظر برسد که کیفیت این رابطه را نمی‌توان از طریق این قاعده کشف کرد. بااین‌حال، از مقایسه این قاعده با قاعده اتلاف و قاعده ضمان ید به نظر می‌رسد استنباط تکلیف برای دیگران در این موضوع ثابت باشد؛ زیرا این قاعده در حال بیان تکلیف پیش از تصرف است؛ درحالی‌که قاعده اتلاف و ضمان ید تکلیف پس از تصرف را بیان می‌کنند. برای اثبات نظر فوق می‌توان به نظر برخی در تفاوت قاعده اتلاف و ضمان اشاره کرد: «نخست، قاعده احترام، حرمت مال مسلمان را ذاتاً بیان می‌کند و نتیجه آن، پرداخت عوض است. پس، حرمت را بالاصاله و جبران خسارت (عوض) را بالتبع افاده می‌کند. برخلاف قاعده اتلاف که صرفاً ضامن بودن به قیمت یا مثل را نتیجه می‌دهد» *(مصطفوی، ق۱٤۲۱، ج۱، صص.۲٤-۲۵)*.

دوم، قاعده احترام، عدم جواز تصرف در مال غیر را به لحاظ تکلیفی بیان می‌کند، درحالی‌که قاعده اتلاف، صرفاً حکم وضعی (ضمان) را نتیجه می‌دهد. مراد از کلمه «حرمت» در عبارت «حرمت ماله کحرمه دمه» (حرمت مال او مانند حرمت خون اوست)، مقابل «حل» است و لذا به حکم تکلیفی بازمی‌گردد» *(مصطفوی، ۱٤۲۱ق، ج۱، صص.۲٤-۲۵؛ ایروانی، ۱۳۸٤، ج۱، ص.۹٦)*. در مورد قاعده ضمان ید نیز چنین است. هر چند دو نظر درباره افاده حکم تکلیفی و وضعی از آن وجود دارد؛ اما حکم وضعی از قوت بیشتری برخوردار است؛ بنابراین، در اینجا قابل استفاده نیست.

به‌علاوه، «تلقیِ قاعده احترام به مال مسلمان به‌عنوان شاخه‌ای از قاعده سلطنت و تفسیر احترام به این معنا قابل‌پذیرش نیست که عبارت است از سلطه مالک بر منعِ دیگران از تصرف در مال او به‌نحوی‌که شایسته نیست؛ زیرا این دو، نزد عقلا و در شریعت، دو قاعده مستقل از نظر دلیل و ملاک هستند. قاعده سلطنت، قاعده‌ای عقلایی است و از احکام مالکیت نزد عقلا به‌شمار می‌رود؛ زیرا مالکِ یک شیء، به انحای مختلف نزد ایشان بر آن مسلط است و شارع نیز آن را امضا و با این سخن نبوی مشهور نافذ کرده است: «الناس مسلطون علی أموالهم» *(مجلسی، ۱٤۰۳ق، ج۲، ص.۲۷۲)* و قاعده حرمت مال، عبارت است از اینکه مال در حریم مملوکیت باشد و محترم بوده و تصرف در آن بدون اذن مالک جایز نباشد و در

صورت اتلاف، موجب ضمان است. این، غیر از سلطه مالک بر مال خود و جواز دفعِ دیگری از تصرف در آن است و این قاعده نیز قاعده‌ای عقلایی است که شارع آن را امضا کرده است» *(خمینی، ۱٤۱۰ق، ج۱، ص.٦۱)*. ازهمین‌رو، این قاعده برای اثبات ضمان در مورد نقض هویت دیجیتال نسبت به‌قاعده تسلیط بیشتر کاربرد دارد؛ زیرا طبق مفاد قاعده تسلیط در ابتدا باید مالکیت فرد اعم از کودک یا بزرگسال را نسبت به داده‌های هویتی اثبات کرد و اگر این مهم به اثبات نرسد، استناد به قاعده تسلیط مشکل می‌شود و همچنین، مفاد این قاعده باتوجه‌به حریم مملوکیت بیشتر با هویت دیجیتال تطبیق دارد.

علاوه بر استنباط حکم تکلیفی از این قاعده، استفاده برخی *(مامقانی، بی‌تا، ج۲، ص.۲۸۱)* از مفاد این قاعده در دو موضوع منافع استیفا شده و اعمالی که مسلمان برای دیگری انجام داده، نشان می‌دهد که برخلاف قاعده ید، موضوع حکم تکلیفی حرمت‌گذاری نیز محدود به عین نیست بلکه دامنه گسترده‌تری دارد و عمومیت آن شامل اعیان، منافع، اعمالی که اجاره داده شده‌اند و غیر آنها می‌شود و به بیان برخی، «احترام به مال، به دلیل ذات مالی آن و لزوم جبران و جلوگیری از هدررفتنش نیست بلکه به دلیل ارتباط آن با مالکیت مسلمان است. به این معنا که حکم مترتب بر شیء، بر اساس ظاهر آن، جنبه تقییدی دارد، نه تعلیلی؛ بنابراین، احترام به مال، ناظر به رعایت مالکیت و سلطه مسلمان بر آن مال است. رعایت مالکیت و سلطه نیز صرفاً مستلزم عدم تصرف در مال بدون رضایت اوست، نه جبران ارزش مالی آن؛ زیرا جبران ارزش مالی به ذات مالی مال مربوط است، نه به مالکیت مسلمان بر آن. به‌همین‌دلیل، تسلیط رایگان بر مال، هتک حرمت مال محسوب نمی‌شود» *(غروی اصفهانی، ۱٤۱۹ق، ج۱، ص.۳۲۲)*.

۴-۱-۴. قاعده تسلیط

قاعده «الناس مسلطون علی انفسهم و اموالهم»، از دو بخش تشکیل شده است که «اگرچه «الناس مسلطون علی انفسهم»، بر سر زبان‌ها مشهور است؛ اما در کتاب‌های حدیثی، نشانی ندارد و نمی‌توان به آن اعتماد کرد. قاعده «الناس مسلطون علی اموالهم» وجود دارد و چه‌بسا به اولویت، به آن برای اثبات سلطه بر نفس نیز استناد شود و این بعید نیست» *(حسینی شاهرودی، بی‌تا، ج٤، ص.١٦٥)*. به هر روی، قاعده «الناس مسلطون علی انفسهم و

اموالهم»، قاعده‌ای است که در ظاهر به انسان حق می‌دهد تا هر طور که می‌خواهد در نفس و مال خود تصرف کند؛ اما در مقابل ادله‌ای قرار می‌گیرد که دلالت بر حرمت تصرفاتی دارند که مستلزم ضرر رساندن به دیگران است. ازآنجاکه قاعده سلطنت خصلت اقتضا و ادله حرمت ضرر، خصلت مانع دارد، معمولاً مانع بر مقتضی مقدم می‌شود تا مانع، مقتضی را از تأثیر باز دارد؛ اما این تقدم، تنها در غیر حالات اضطراری است که شارع، مکلف را ملزم به رفع ضرر از خود در آن حالات کرده است؛ و در این هنگام، تزاحم بین دو حکم الزامی رخ می‌دهد و در این صورت، اهمّ آن دو از نظر شارع، مقدم می‌شود *(طباطبایی حکیم، ۱٤۲۹ق، ج۱، ص.۱٤۷)*. به‌عبارت‌دیگر، مردم بر اموال و املاک خویش مسلّط هستند، نه بر احکام شرعی آنها و می‌توانند تصرّفات مشروع در آنها بنمایند *(کاشف الغطا(ب)، بی‌تا، ج٤، ص.۷٤؛ موسوی گلپایگانی، بی‌تا، ج۲، ص.٤۱؛ ذهنی تهرانی، ۱۳٦۹، ج٥، ص.۲۱۸)* و در طرف‌دیگر، هیچ‌کس نمی‌تواند بدون اجازه آنها در آن تصرف کند، پس به‌طریق‌اولی بر سرنوشت خود نیز مسلط هستند و هیچ‌کس نمی‌تواند بدون اجازه آنها در امور و مقدراتشان دخالت کند *(فیاض، ۱٤۲٦ق، ج۱، ص.۲٤۳)*. برخی مدرک این قاعده را عقل و «آن را یک اصل عقلایی می‌دانند که شرع آن را منع نکرده، پس نزد شرع نافذ است» *(محسنی، ۱٤۲٦ق، ج۲، ص.۱۳؛ سبحانی، ۱٤۱٤ق، ص.٦٦٦)*. برخی نیز آیات ۲۹ و ٤ نسا و ۱۸۸ سوره بقره، روایات، اجماع و بنای عقلا را به دلیل عقل افزوده‌اند *(مکارم شیرازی، ۱۳۷۰، ج۲، صص.۱۹-۲۹)*.

فارغ از موضوع اعتبار این قاعده نسبت به نفس، این قاعده در صورت عدم وجود دلیلی که اقتضای خروج از مدلول قاعده را داشته باشد، می‌تواند دلیلی بر حرمت نقض هویت دیجیتال افراد اعم از کودک و بالغ باشد، نه دلیل؛ زیرا «تسلّط فرع بر ثبوت مال یا حق است که در حکم مال است، و اشکال در اصل ثبوت حق است، و حکمْ، اثباتِ موضوعِ خود را نمی‌کند، و عدم صحّت تمسّک به دلیلِ حکمی، بر فرض عدم تمامیّت موضوع آن، از بدیهیّات است» *(حسینی طهرانی، ۱٤۳٥ق، ج۷، ص.۲۰۸)*. پس از اثبات حرمت از طریق این قاعده، با استناد به قواعد دیگر که در ذیل می‌آیند، می‌توان مسئولیت کیفری نقض هویت دیجیتال کودکان را به‌دست آورد؛ زیرا در بخشی از هویت دیجیتال، گردش اطلاعات در اختیار اوست و در بخش دیگر نیز هرچند در اختیار او نیست؛ اما قائم به شخص اوست و بدون

آن انجام هرگونه فعالیت در دولت الکترونیک منتفی خواهد بود.

۴-۲. مبانی ضمانت اجرای کیفری نقض هویت دیجیتال کودکان در فقه

ذیل مبانی ضمانت اجرای کیفری نقض هویت دیجیتال می‌توان به قاعده «التعزیر لکل عمل محرم» و «التعزیر بما یراه الحاکم» اشاره کرد که به بیان‌های مختلف در کتب فقهی *(تبریزی، ق۱٤۰٤، ص.۷؛ طوسی، ۱۳۵۱، ج۸، ص.٦۹؛ حرعاملی، بی‌تا، ج۱۸، ص.۳۰۹)* مطرح شده‌اند. با استناد به قاعده حرمت مال مسلمان و قاعده تسلیط که پیش‌ازاین اشاره شد، می‌توان حکم تکلیفی تصرف عدوانی را به‌دست آورد و با اثبات حکم حرمت می‌توان در مرحله بعد با استناد به قاعده «التعزیر لکل عمل محرم» و سپس قاعده «التعزیر بما یراه الحاکم»، فارغ از اختلافات نظر درباره مفاد آن، لزوم تعیین مجازات را برای نقض هویت دیجیتال کودک را تحصیل کرد؛ زیرا قدر متیقن از این قاعده، اختیار حاکم در تعیین میزان مجازات است و بهترین مستند برای تعیین تعزیر یا به‌عبارتی مجازات برای این عمل در فقه این است که نخست، «هرچند هویت دیجیتال امکان اشتراک‌گذاری محدودتر اطلاعات شخصی را فراهم می‌کند یا تقلب و سرقت هویت را کاهش می‌دهد؛ اما بدون پادمان یا حفاظت[۱۵]، هویت دیجیتال امکان سوءاستفاده جدی را باز می‌کند؛ زیرا درحال‌حاضر، بیشتر بررسی‌های هویتی شامل اشتراک‌گذاری بیش‌ازحد اطلاعات شخصی است که به ثالث فروخته می‌شود که برای نمونه، بر حق بیمه یا بر پرداخت‌های کارت نقدی فرد تأثیر می‌گذارد. برهمین‌اساس، ایجاد مرجع نظارتی یا قوانین نظارتی یا هر دو باهدف پیشگیری از فروش بی‌رویه داده‌هایی توصیه می‌شود که جمع‌آوری آنها از طریق تأیید هویت دیجیتال تسهیل می‌شوند. اگر هویت دیجیتال تبدیل به‌روشی واقعی برای خرید، ورود به رسانه‌های اجتماعی و غیره شود، تمام داده‌هایی که آن تراکنش‌ها جمع‌آوری می‌کنند، مانند مکان فرد، مقدار هزینه‌کرد، کالای خریداری شده و غیره را می‌توان به یک هویت فردی مرتبط کرد و (از طریق توافق‌نامه با خود شخص در شرایط و ضوابط چاپ دقیق) به یک سازنده نمایه شخص ثالث فروخته شود» *(Hanson, 2018, p.11)*. دوم، «حفاظت از حق هویت، به‌ویژه باتوجه‌به

15- Safeguards

نقش‌محوری هویت تراکنش در امور مالی مهم است» *(Sullivan, 2011, p.72)*.

۵- ضمانت اجرای مدنی و کیفری نقض هویت دیجیتال کودکان در حقوق ایران

هر چند به‌صورت مستقیم از ضمانت اجرای مدنی و کیفری نقض هویت دیجیتال کودکان در حقوق ایران سخنی به میان نیامده است، اما می‌توان ردپایی را از این دو نوع ضمانت اجرا یافت:

۵-۱. ضمانت اجرای مدنی نقض هویت دیجیتال کودکان در حقوق ایران

قطعاً مهم‌ترین مستند و مستمسک قانونی برای جبران خسارات مادی و معنوی ناشی از نقض هویت دیجیتال کودکان، ماده ۱ قانون مسئولیت مدنی است که برای استناد به آن در این مورد باید رابطه میان انسان و داده‌ها را تبیین کرد. ازهمین‌رو، برقراری رابطه میان انسان و داده‌ها را می‌توان در قالب‌های مختلف در نظر گرفت؛ برای نمونه، چند نظریه در این زمینه مطرح هستند که بر اساس یکی، توصیف این رابطه در قالب «حق مالکیت غیرقابل واگذار فرد بر داده‌های شخصی‌اش» می‌گنجد؛ درحالی‌که از نظر طرف مخالف، «این حق مالکیت در تضاد با مفهوم اروپایی خود آیینی اطلاعاتی و پیشرفت فرد در محیط دیجیتال است و به‌طور جدایی‌ناپذیری با کرامت انسانی مرتبط است» *(Stoykovar, 2018, p.66)*.

درمقابل، برخی نیز آن را ذیل «حق انتقال داده‌ها» مطرح می‌کنند و برخی نیز از آن به «حق دسترسی به اطلاعات» تعبیر می‌کنند؛ اما «حق انتقال داده‌ها» برخلاف حق دسترسی، نه‌تنها حفاظت از داده‌های شخصی بلکه جریان آزاد داده‌ها را در مقیاس وسیع تسهیل می‌کند که نمی‌توان آن را (مستقیماً) در محیط‌های پردازشی نوین با حق دسترسی به دست آورد؛ زیرا حق دسترسی صرفاً مجموعه‌ای از اطلاعات متنی ساده را فراهم کند که قابل خواندن توسط ماشین یا ساختار دیگری نیستند» *(Stoykovar, 2018, p.66)*.

بااین‌حال و فارغ از همه نظرها، می‌توان این رابطه را در چهارچوب هویت دیجیتال فرد تبیین کرد؛ زیرا به نظر می‌رسد تبیین این رابطه در هیئت حق مالکیت یا حق انتقال داده یا حق دسترسی دارای آفت‌هایی است که بیشتر به حوزه تجاری‌سازی داده‌ها مرتبط است و راهکارهای پیشنهادی مانند «اعمال ممنوعیت بر تجارت داده، به‌جای اعمال محدودیت در

قابلیت انتقال» و «عدم محدودیت قانونی در تجارت داده‌ها» به یک اندازه به نفع افراد نیستند. به‌علاوه، تعلق و قائم بودن برخی اجزای هویت دیجیتال به شخص می‌تواند ارتباط محکم‌تری را میان فرد و هویت دیجیتال نسبت به سایر نظرات برقرار کند؛ زیرا «هویت در نشانه‌های مختلفی متجلی می‌شود که به‌وسیله آنها، آن شخص خاص را می‌توان شناخت. به‌عبارت‌دیگر، وجوهی از شخصیت او که مشخصه یا منحصربه‌فرد برای اوست، مانند تاریخچه زندگی، شخصیت، نام، اعتبار، صدا، خط، ظاهر (تصویر فیزیکی) و غیره. یک شخص علاقه قطعی دارد که منحصربه‌فرد بودن و رفتارش مورداحترام دیگران باشد؛ بنابراین، اگر هر یک از این نشانه‌ها بدون مجوز به‌گونه‌ای استفاده شود که با تصویر واقعی او سازگار نباشد، هویت فرد نقض می‌شود» *(Sullivan, 2011, p.76)*. برهمین‌اساس، شاید بتوان هویت دیجیتال را بیشتر در ارتباط با حیثیت یا مال در این ماده مرتبط دانست، هرچند ارتباط آن با برخی موارد دیگر نیز امکان تحقق دارد.

۵-۲. ضمانت اجرای کیفری نقض هویت دیجیتال کودکان در حقوق ایران

هرچند قانون‌گذار صراحتاً به هویت دیجیتال و مفهوم آن در این قانون اشاره‌ای نکرده؛ اما می‌توان با استناد به تبصره ۲ ماده ۳۲ قانون جرائم رایانه‌ای به تعریفی از هویت دیجیتال دست یافت: «هرگونه اطلاعات راجع به کاربر خدمات دسترسی از قبیل نوع خدمات، امکانات فنی مورد استفاده و مدت زمان آن، هویت، آدرس جغرافیایی یا پستی یا پروتکل اینترنتی(IP)، شماره تلفن و سایر مشخصات فردی اوست». به‌علاوه آنکه در این تبصره، قانون‌گذار به واژه «هویت» اشاره دارد که به‌عنوان بخشی از هویت دیجیتال فرد شناخته می‌شود. قانون‌گذار در بند «ب» و «پ» ماده ۱۵ طرح صیانت از فضای مجازی (ویرایش ۹ بهمن ۱٤۰۰) ذیل الزام تضمین حقوق کاربران توسط ارائه‌دهندگان خدمات فضای مجازی هم به دیدگاه خود درباره هویت دیجیتال اشاره کرده است که آن را برابر با داده‌ها و اطلاعات کاربران می‌داند و هم یکی از عناصر هویت دیجیتال؛ یعنی احراز هویت را مد نظر قرار داده است: «ب- احراز هویت معتبر کاربران و حفظ اطلاعات آنها مطابق قوانین موضوعه و سند هویت معتبر مصوب شورای عالی فضای مجازی؛ پ- عدم انتقال داده‌های

مرتبط با هویت کاربران ایرانی به خارج از کشور». به‌علاوه، در بند «پ» آن را «داده‌های مرتبط با هویت کاربران» خوانده است. همچنین، در بند «د» همین قانون، به «شناسه کاربری» و مالکیت بر آن بدین‌نحو اشاره کرده است: «حمایت از حق مالکیت بر شناسه کاربری وفق قانون ثبت اختراعات، طرح‌های صنعتی و علائم تجاری مصوب ۱۳۸٦ و اصلاحات بعدی آن». شناسه کاربری نیز در ارتباط وثیق با هویت دیجیتال است که در این قانون صحبت از حق مالکیت بر آن است؛ زیرا کاربرد آن، احراز هویت کاربران در سامانه‌های مختلف است و برای حفظ امنیت آن، بسیاری از سازمان‌ها اقدام به راه‌اندازی سامانه مدیریت شناسه کاربری در راستای یکپارچه‌سازی فرایند احراز هویت کاربران در سامانه‌های مختلف می‌کنند. به‌این‌ترتیب با ثبت نام و دریافت شناسه و رمز عبور در این سامانه، دیگر نیاز به استفاده از رمزهای مختلف نخواهد بود و تنها با یک شناسه کاربری و رمز عبور، کاربران می‌توانند به تمامی سامانه‌ها دسترسی پیدا کنند.

قانون‌گذار در بند «ب» ماده ۲۵ قانون جرائم رایانه‌ای نیز به یکی دیگر از عناصر آن؛ یعنی گذرواژه اشاره کرده است. به‌علاوه، در بند «الف» این ماده نیز می‌توان اشاره‌ای غیرمصرح به هویت دیجیتال را به‌دست آورد؛ زیرا طبق یکی از نظریات هویت دیجیتال مساوی با داده است. این موضوع به‌خوبی نشان می‌دهد که گذرواژه یا داده متعلق به فرد هستند و تحت حمایت قانون‌گذار است.

شدت این حمایت تا حدی است که دسترسی به این نوع از هویت دیجیتال نیز در ماده ۱۰ این قانون مدنظر قانونگذار بوده و به دو مورد از نقض آن؛ یعنی تغییر گذرواژه یا رمزنگاری داده‌ها اشاره کرده است. هرچند این ماده به سامانه‌های رایانه‌ای یا مخابراتی اشاره دارد که به‌نوعی مشعر به هویت دیجیتال اشخاص حقوقی مثل دولت و بخش‌های درونی آن است و موضوع ماده در خصوص افراد حقیقی نیست؛ اما می‌توان از فحوای ماده توسعه موضوع به افراد را به‌دست آورد: «هرکس به‌طور غیرمجاز با اعمالی از قبیل مخفی کردن داده‌ها، تغییر گذرواژه یا رمزنگاری داده‌ها مانع دسترسی اشخاص مجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی شود، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون (۵.۰۰۰.۰۰۰) ریال تا بیست میلیون (۲۰.۰۰۰.۰۰۰) ریال یا هر

دو مجازات محکوم خواهد شد»؛ البته ناگفته نماند که برخی سامانه‌های رایانه‌ای به‌ویژه با پررنگ شدن جایگاه دولت الکترونیک حاوی هویت دیجیتال افراد یا داده‌های هویتی خاص هستند که تغییر گذرواژه یا رمزنگاری داده‌ها مانع از دسترسی به آنها برای انجام امور مرتبط می‌شود.

به‌علاوه، قانونگذار در ماده ۱۲ قانون جرائم رایانه‌ای به ربایش یا سرقت داده‌ها اشاره کرده‌اند که به‌عنوان هویت دیجیتال طبق یک نظر شناخته می‌شد و درنتیجه، قانون‌گذار در مسیر حمایت از هویت دیجیتال فرد، یک مورد دیگر از نقض این حق را جرم‌انگاری کرده است: «هرکس به‌طور غیرمجاز داده‌های متعلق به دیگری را برباید، چنانچه عین داده‌ها در اختیار صاحب آن باشد، به جزای نقدی و در غیراین‌صورت به حبس از نودویک روز تا یک‌سال یا جزای نقدی یا هر دو مجازات محکوم خواهد شد».

همچنین، قانون‌گذار در ماده ۱۳ قانون جرائم رایانه‌ای، به جرائم مالی مرتبط با داده‌ها به‌عنوان هویت دیجیتال اشاره می‌کند و رکن مادی جرائم در قبال داده‌ها را به‌خوبی تبیین می‌کند: «هرکس به‌طور غیرمجاز از سامانه‌های رایانه‌ای یا مخابراتی با ارتکاب اعمالی از قبیل وارد کردن، تغییر، محو، ایجاد یا متوقف کردن داده‌ها یا مختل کردن سامانه، وجه یا مال یا منفعت یا خدمات یا امتیازات مالی برای خود یا دیگری تحصیل کند، علاوه بر رد مال به صاحب آن به حبس از یک تا پنج سال یا جزای نقدی از بیست میلیون (۲۰.۰۰۰.۰۰۰) ریال تا یکصد میلیون (۱۰۰.۰۰۰.۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد».

علاوه‌براین، قانون‌گذار به عنصر دیگری از هویت دیجیتال در ماده ۳۲ قانون جرائم رایانه‌ای اشاره می‌کند که همان احراز هویت دیجیتال است: «ارائه‌دهندگان خدمات دسترسی موظف‌اند داده‌های ترافیک را حداقل تا شش‌ماه پس از ایجاد و اطلاعات کاربران را حداقل تا شش‌ماه پس از خاتمه اشتراک نگه‌داری کنند. تبصره ۱ـ داده ترافیک هرگونه داده‌ای است که سامانه‌های رایانه‌ای در زنجیره ارتباطات رایانه‌ای و مخابراتی تولید می‌کنند تا امکان ردیابی آنها از مبدأ تا مقصد وجود داشته باشد. این داده‌ها شامل اطلاعاتی از قبیل مبدأ، مسیر، تاریخ، زمان، مدت و حجم ارتباط و نوع خدمات مربوطه می‌شود». قانون‌گذار پس از اشاره به احراز هویت دیجیتال، در ماده ۳۳ همین قانون، ارائه‌دهندگان

خدمات میزبانی داخلی را موظف می‌کند اطلاعات کاربران خود را حداقل تا شش‌ماه پس از خاتمه اشتراک و محتوای ذخیره شده و داده ترافیک حاصل از تغییرات ایجاد شده را حداقل تا پانزده روز نگه‌داری کنند. این بدان‌معناست که قانون‌گذار درباره حفظ هویت دیجیتال افراد حساسیت دارد و حتی پس از خاتمه فرایند بر حفظ و نگه‌داری آنها برای مدتی خاص توجه دارد.

همچنین، طبق بند «ب» ماده ٤ مصوبه شورای‌عالی فضای مجازی در خصوص صیانت از کودکان و نوجوانان در فضای مجازی با عنوان «اقدامات کلان و تقسیم کار ملی» به تکلیف دولت نسبت به «ایجاد زیرساخت و خدمات پایه و پیشران ویژه محیط‌های صیانت شده مجازی اعم از احراز هویت، امکان دسترسی طبقه‌بندی‌شده، امکان نظارت اولیا، گزارش‌دهی، خدمات پرداخت و مقررات‌گذاری برای ترغیب دارندگان پروانه‌های ارائه خدمات ارتباطی و فناوری اطلاعات به توسعه زیرساخت و خدمات پایه در این محیط توسط وزارت ارتباطات و فناوری اطلاعات با همکاری نهادهای ذی‌ربط ظرف مدت شش‌ماه» اشاره شده است که «عبارت احراز هویت» به‌خوبی مؤید شناسایی هویت دیجیتال افراد است؛ زیرا سامانه احراز هویت، با هدف حفظ هویت‌های دیجیتال افراد در مقابل هویت‌های دیجیتال جعلی است. به‌علاوه، این موضوع برای کودکان مدنظر قرار گرفته تا از آنان در فضای مجازی صیانت کند. پس به‌طریق‌اولی، هویت دیجیتال کودکان مدنظر قانون‌گذار بوده است.

همچنین، قانون‌گذار در قانون «نظام هویت معتبر در فضای مجازی کشور» با تعریف «تأمین‌کننده شناسه» به‌عنوان نهادی که برای انواع تعاملات، اطلاعات پایه هویتی قابل استنادی از موجودیت‌ها را گواهی می‌کند و مسئولیت ثبت و راستی‌آزمایی هویت واقعی موجودیت‌ها، تخصیص شناسه و صدور گواهی‌نامه هویت برای آنها و در برخی تراکنش‌ها، احراز هویت آنها را برعهده دارد»؛ بر شناسایی هویت دیجیتال برای هر فرد حقیقی و حقوقی تأکید دارد. سخن‌گفتن از احراز هویت و شناسایی تأمین‌کننده شناسه در کنار مالکیت بر شناسه نشان‌دهنده تصمیم قانون‌گذار بر به‌رسمیت‌شناختن هویت دیجیتال است. قانون‌گذار در قانون مذکور با تأکید بر الزامات زیست‌بوم هویت معتبر در فضای

مجازی به مواردی اشاره دارد که نظر فوق را تقویت می‌کند، مانند «تأمین سطوح اعتبار و اعتماد در تأمین اطلاعات هویت دیجیتالی به‌تناسب نوع تعامل؛ رعایت امنیت اطلاعات هویت دیجیتالی و تناسب آن با نوع تعامل از طریق ایجاد چهارچوب مبادله قابل‌اعتماد و اعطای گواهی موثق؛ مرتبط بودن اطلاعات هویتی پایه فضای مجازی با فضای فیزیکی؛ تضمین صحت، تمامیت، اعتبار، انکارناپذیری و استنادپذیری هویت موجودیت‌های فضای مجازی به‌تناسب نوع تعامل؛ ارتقا و استمرار فرایندهای احراز هویت در فضای مجازی و افزایش شفافیت و کاهش گمنامی در فضای مجازی».

نتیجه‌گیری

درباره مفهوم هویت دیجیتال میان صاحب‌نظران اتفاق‌نظری وجود ندارد. برخی آن را بر محور مشخصات و ممیزات فردی ملاحظه کرده و مفهوم هویت در عالم واقع را در فضای مجازی بازتعریف کرده‌اند. به‌نظر می‌رسد این گروه مبنا و اصل را خود هویت قرار دادند، نه شبکه‌ها و رسانه‌های اجتماعی؛ درحالی‌که گروه دوم با مبنا قراردادن فضای مجازی هویت را مجموعه‌ای از داده‌ها می‌دانند. گروه سوم نیز بیشتر تمرکز خود را بر ابعاد اقتصادی و مالی آن گذارده‌اند و برهمین‌اساس، می‌توان هویت دیجیتال کودکان را در سه بُعد ویژگی‌ها یا نمایش، داده‌ها و درنهایت، بُعد مالی خلاصه کرد. هر چند بُعد سوم، در مورد هویت دیجیتال کودکان کاربردی به‌نظر نمی‌رسد؛ اما از جهات‌دیگر؛ یعنی احراز هویت دیجیتال آنان در موضوعات غیرمالی، هویت دیجیتال آنان را تقویت می‌کند. به‌علاوه، در تعلق برخی اطلاعات در پایگاه‌داده یا مربوط به هویت دیجیتال شامل جنسیت، تاریخ و محل تولد (و تاریخ مرگ) و معمولاً حداقل یک قطعه عکس، امضا و سایر اطلاعات زیست‌سنجی که کاملاً مختص به هر فرد است و فقط به شکلی خاص و در فضایی خاص ثبت و ضبط می‌شوند، تردیدی وجود ندارد.

مبانی مشروعیت ابعاد هویت دیجیتال کودک را می‌توان در برخی آیات قرآن مانند آیات ۲۲ سوره روم، ٤ سوره قیامت و ۲۸ سوره فاطر یافت؛ زیرا در این آیات بر لزوم تفاوت میان انسان‌ها برای حفظ نظام زندگی نوع بشر و ممانعت از اختلال آن تأکید شده است.

مبانی ضمانت اجرای مدنی نقض هویت دیجیتال کودکان ذیل قواعد فقهی چون لاضرر، حفظ نظام، احترام مال مسلمان و قاعده تسلیط قابل تبیین است؛ زیرا از عمده این قواعد، حکم تکلیفی حرمت ضرر به دیگری و حکم وضعی جبران خسارت قابل برداشت است. مبانی ضمانت اجرای کیفری آن در ذیل قواعد «التعزیر لکل عمل محرم» و «التعزیر بما یراه الحاکم» قابل پذیرش خواهد بود؛ زیرا حرمت نقض هویت دیجیتال کودکان که مبنای استعمال این قواعد است، به‌واسطه قواعد فوق به اثبات رسیده است. به‌علاوه، در حقوق ایران نیز می‌توان جبران خسارت‌ها در این زمینه را مستند به ماده یک قانون مسئولیت مدنی کرد و مسئولیت کیفری در قبال آن را در برخی مواد قانون جرائم رایانه‌ای به‌دست آورد.

منابع

۱. قرآن کریم
۲. آشتیانی، محمدحسن (۱٤۰٤ق). *کتاب القضا*. قم: هجرت.
۳. اصفهانی(فاضل هندی)، محمد بن حسن (۱٤۱٦ق). *کشف اللثام عن القواعد الاحکام*. قم: اسلامی.
٤. انصاری، مرتضی (۱٤۱٥ق). *القضا و الشهادات*. قم: المؤتمرالعالمی.
٥. ایروانی، میرزاعلی (۱۳۸٤). *حاشیه المکاسب*. تهران: کیا.
٦. بحرانی، یوسف (بی‌تا). *الحدائق الناضره فی أحکام العتره الطاهره*. قم: اسلامی.
۷. تبریزی، محمد جواد (۱٤۰٤ق). *اسس الحدود و التعزیرات*. قم: انتشارات جامعه مدرسین.
۸. ثقفی تهرانی، محمد (۱۳۹۸). *تفسیر روان جاوید*. تهران: برهان.
۹. جزائری، سیدعبدالله (بی‌تا). *التحفه السنیه*. بی‌جا: بی‌نا.
۱۰. جواهری، محمدحسن (بی‌تا). *بحوث فی الفقه المعاصر*. بیروت: دار الذخائر.
۱۱. حرعاملی، محمد بن حسن (بی‌تا). *وسائل الشیعه الی تحصیل الشریعه*. بیروت: دار احیا التراث العربی.
۱۲. حسینی شاه‌عبدالعظیمی، حسین‌بن‌احمد (۱۳٦۳). *تفسیر اثنی‌عشری*. تهران: میقات.

۱۳. حسینی طهرانی، سیدمحمدحسین (۱٤۳۵ق). *مطلع انوار*. تهران: مکتب وحی.

۱۴. حسینی شاهرودی، سیدعلی (بی‌تا). *محاضرات فی فقه‌الجعفری*. قم: دارالکتاب الإسلامی.

۱۵. حلی، ابی‌طالب محمد بن حسن (۱۳۸۷). *ایضاح الفوائد فی شرح اشکالات القواعد*. قم: المطبعه العلمیه.

۱٦. خمینی، سیدروح‌الله (۱٤۱۰ق). *الرسائل*. قم: اسماعیلیان.

۱۷. خمینی، سیدروح‌الله (۱٤۲۱ق). *البیع*. تهران: مؤسسه تنظیم و نشر آثار امام خمینی(ره).

۱۸. خویی، سیدابوالقاسم (بی‌تا). *مصباح‌الفقاهه فی المعاملات*. محمدعلی توحیدی، قم: داوری.

۱۹. ذهنی تهرانی، سیدمحمدجواد (۱۳٦۹). *ترجمه و شرح مکاسب شیخ انصاری*. قم: حاذق.

۲۰. سبحانی، جعفر (۱٤۱٤ق). *المختار فی احکام الخیار*. بی‌جا: بی‌نا.

۲۱. سبحانی، جعفر (بی‌تا). *تهذیب الأُصول؛ تقریر بحث السید روح الله الخمینی*. بی‌جا: بی‌نا.

۲۲. سبزواری، محمدباقر (۱٤۲۳ق). *کفایه الاحکام*. قم: اسلامی.

۲۳. سیفی، علی‌اکبر (۱٤۲۵ق). *مبانی الفقه الفعال فی القواعد الفقهیه الأساسیه*. قم: اسلامی.

۲۴. شریعت اصفهانی، فتح‌الله بن محمدجواد (بی‌تا). *قاعدهٔ لا ضرر*. قم: اسلامی.

۲۵. شهید ثانی، زین‌الدین بن علی (۱٤۱۳ق). *مسالک الافهام الی تنقیح شرائع الاسلام*. قم: مؤسسه معارف اسلامی.

۲٦. صاحب جواهر، محمدحسن (۱۳٦۲ق). *جواهر الکلام فی شرح شرایع الاسلام*. بیروت: دارإحیاالتراث العربی.

۲۷. طباطبایی حکیم، سیدمحمدتقی (۱٤۲۹ق). *القواعد العامهٔ فی الفقه المقارن*. تهران: المجمع العالمی للتقریب.

۲۸. طباطبایی یزدی، سیدمحمدکاظم (۱۳۷۸). *تکملة العروة الوثقی*. تهران: الحیدری.

۲۹. طوسی، محمد بن حسن (۱۳۵۱). المبسوط فی الفقه الامامیه. تهران: المکتبه المرتضویه.

۳۰. طیب، سیدعبدالحسین (۱۳۷۸). *اطیب البیان فی تفسیر القرآن*. تهران: اسلام.

۳۱. غروی اصفهانی، محمدحسین (۱٤۱۹ق). *حاشیه کتاب المکاسب*. قم: دارالمصطفی صلی‌الله علیه وآله وسلم.

۳۲. فاضل تونی، محمدحسین (۱٤۱۲ق). *الوافیه فی اصول الفقه*. قم: مجمع الفکر الاسلامی.

۳۳. فیاض، محمداسحاق (۱٤۲٦ق). *المسائل المستحدثه*. کویت: موسسهٔ مرحوم محمدرفیع حسین معرفی.

۳٤. کاشف‌الغطا، جعفر (بی‌تا.الف). *کشف الغطا*. اصفهان: مهدوی.

۳٥. کلینی، محمّد بن یعقوب (۱٤۰۷ق). *الکافی*. تهران: دارالکتب الاسلامیه.

۳٦. کاشف‌الغطا، مهدی (بی‌تا.ب). *مورد الأنام فی شرح شرائع الإسلام*. بی‌جا: بی‌نا.

۳۷. لطیف‌زاده، مهدیه و قبولی درافشان، سیدمحمدمهدی (۱٤۰۲). معرفی هویت دیجیتال در متاورس، شناسایی چالش‌های حقوقی مربوط به آن و جست‌وجوی راه‌حل. مطالعات حقوق خصوصی، ٥۳(۲)، ۳٤۹-۳۷۲.

۳۸. مامقانی، محمدحسن (بی‌تا). *غایة الآمال فی شرح کتاب المکاسب*. قم: مجمع الذخائر الإسلامیه.

۳۹. مجلسی، محمدباقربن محمدتقی (۱٤۰۳ق). *بحارالأنوار*. بی‌جا: مؤسسهٔ الوفاء.

٤۰. محسنی، محمدآصف (۱٤۲٦ق). *الفقه و مسائل طبیه*. قم: بوستان کتاب.

٤۱. مصطفوی، سیدمحمدکاظم (۱٤۲۱ق). *القواعد: مائة قاعدة فقهیة معنی و مدرکا و موردا*. جلد۱. قم: اسلامی.

٤۲. مکارم شیرازی، ناصر (۱۳۷۰). *القواعد الفقهیه*. قم: مدرسه الامام علی‌بن‌ابی‌طالب علیه‌السلام.

٤۳. مکارم شیرازی، ناصر (۱۳۷٤). *تفسیر نمونه*. تهران: دارالکتب الاسلامیه.

٤٤. مکارم شیرازی، ناصر (١٤٢٥ق). *انوار الفقاهه*. قم: مدرسه الامام علی‌بن‌ابی‌طالب علیه‌السلام.

٤٥. موسوی گلپایگانی، سیدمحمدرضا (بی‌تا). *کتاب القضاء*. قم: دارالقرآن الکریم.

46. Amini, Mehrdad and Javidnejad, Laleh. (2023). Legal Frameworks for Digital Identity Systems in E-Governance: Privacy, Security, and Inclusion. *Legal Studies in Digital Age*, *2*(3), 49-63.
47. Boysen, Andre. (2019). The Need for a National Digital Identity Infrastructure. *Governing Cyberspace during a Crisis in Trust essay. Waterloo, ON: Centre for International Governance and Innovation. www. cigionline. org/articles/need-national-digital-identity-infrastructure*.
48. Giannopoulou, Alexandra. (2023). Digital identity infrastructures: A critical approach of self-sovereign identity. Digital Society, 2(2), 1-19.
49. Ghadge, Nikhil. (2024). Challenges with securing digital identity. International Journal on Cybernetics & Informatics (IJCI), 13(13), 1-8.
50. Hamid, Muhammad Abdullah et al. (2023). Digital Identity and Legal Rights: the EU's eIDAS Regulation as a Model for Global Digital Trust. Democracy, Rule of Law, and Protection of Human Rights in the European Union, U.S.A: Batumi Shota Rustaveli State University.
51. Hanson, Fergus. (2018). Preventing another Australia card fail. *Australian Strategic Policy Institute*, 18.
52. Holt, Jennifer, and Malčić, Steven. (2015). The privacy ecosystem: regulating digital identity in the United States and European Union. *Journal of Information Policy*, *5*, 155-178.
53. Huk, T. (2016). Use of Facebook by children aged 10-12. Presence in social media despite the prohibition. The New Educational Review, 46(1), 17-28.
54. Friedman, Arthur R., and Wagoner, Larry D. (2015). The need for digital identity in cyberspace operations. *Journal of Information Warfare*, 14(2), 41-51.
55. Jennings, Ben, and Finkelstein, Anthony. (2009). Digital identity and reputation in the context of a bounded social ecosystem. In *Business Process Management Workshops: BPM 2008 International Workshops, Milano, Italy, September 1-4, 2008. Revised Papers 6* (pp. 687-697). Springer Berlin Heidelberg.
56. Levin, Ilya, and Mamlok, Dan. (2021). Culture and society in the digital age. *Information*, *12*(2), 68.
57. Livingstone, Sonia and Third, Amanda(2017), "Children and young people's rights in the digital age: An emerging agenda", *New media & society*,19(5),657–670.
58. Kim, Hee-Woong, and Que, Eunice. (2007). Presentation desire of digital identity in virtual community. In *Online Communities and Social Computing: Second International Conference, OCSC 2007, Held as Part of HCI International 2007, Beijing, China, July 22-27, 2007. Proceedings 2* (pp. 96-105). Springer Berlin Heidelberg.
59. Savin-Baden, M., Burden, D., & Taylor, H. (2017). The ethics and impact of

digital immortality. *Knowledge Cultures*, *5*(2), 178-196.
60. Stoykovar, Radina. (2018). The Right to Data Portability: Data protection scope and technical feasibility. *Computer Law Review International*, *19*(3), 65-71.
61. Sullivan, Clare. (2011). *Digital identity: An emergent legal concept* (p. 178). University of Adelaide Press.
62. Virginia Phelan, K., Mills, J. E., Douglas, A. C., & Brian Aday, J. (2013). Digital personalities: an examination of the online identity of travel and tourism web sites. *Journal of Hospitality and Tourism Technology*, *4*(3), 248-262.