Rasanch \ A Quarterly Journal of Media Studies and Research
http//qjmn.farhang.gov.ir DOI: 10.22034/bmsp.2025.509695.2130
Research paper Received: 1/3/2025
Vol. 37, No. 1, Spring 2026, Issue 4 Accepted: 27/4/2025

The Role of Media Literacy in Cybersecurity and Digital Identity in the Age of Artificial Intelligence

Ali Jafari: Assistant Professor, Institute for Educational Studies, Organization for Educational Research and Planning (OERP), Tehran, Iran. **email:** alijafari@oerp.ir

This study was conducted to examine the role of media literacy in cybersecurity and digital identity in the age of artificial intelligence. The research method was survey-based, and the statistical population included all users of cyberspace and social networking platforms in Iran who are actively present in digital environments. The sample size was determined as 384 participants using Cochran's formula for an unlimited population. Stratified random sampling was employed. Data collection tools consisted of standard questionnaires on digital identity, cybersecurity, and media literacy.

The findings showed that there is a positive and significant correlation between media literacy, cybersecurity, and digital identity. Media literacy has both a direct and indirect positive effect (through cybersecurity) on digital identity. Cybersecurity had the greatest effect on digital identity. Women demonstrated higher levels of media literacy compared to men.

The results indicate that media literacy, as a key skill, plays an important role in strengthening cybersecurity and protecting digital identity in the age of artificial intelligence. Digital identity, as a valuable asset, requires protection; cybersecurity provides the tools for this protection, while media literacy empowers users to use these tools effectively. Increasing users' awareness through media literacy education can help reduce cyber threats and improve digital security. Together, these three concepts contribute to creating a secure and trustworthy digital environment.

Keywords: Cybersecurity, media literacy, digital identity, artificial intelligence.

How to cite this paper: Jafari, A. (2026). The Role of Media Literacy in Cybersecurity and Digital Identity in the Age of Artificial Intelligence. *Rasaneh*, 37(1), 53-72. **[In persian]**

رسانه / فصلنامه مطالعاتی و تحقیقاتی وسایل ارتباط جمعی
Rasanch
نوع مقاله: پژوهشی
DOI: 10.22034/bmsp.2025.509695.2130
http//qjmn.farhang.gov.ir
Vol. 37, No. 1, Spring 2026, Issue 4

نقش سواد رسانه‌ای در امنیت سایبری و هویت دیجیتال در عصر هوش مصنوعی

نوشتهٔ
علی جعفری*

تاریخ دریافت: ۱۴۰۳/۱۲/۱۱
تاریخ پذیرش: ۱۴۰۴/۰۲/۰۷

چکیده

این پژوهش با هدف بررسی نقش سواد رسانه‌ای در امنیت سایبری و هویت دیجیتال در عصر هوش مصنوعی انجام شـده است. روش تحقیق از نوع پیمایشـی و جامعهٔ آماری پژوهش شامل تمام کاربران فضای مجازی و شـبکه‌های اجتماعی در ایران اسـت که به‌صورت فعال در محیط‌های دیجیتال حضور دارند. حجم نمونه با اسـتفاده از فرمول کوکران برای جامعهٔ نامحدود، ۳۸۴ نفر تعیین شـد. روش نمونه‌گیری تصادفی طبقه‌ای بود. ابزار جمع‌آوری داده‌ها پرسشـنامه‌های استاندارد هویت دیجیتال، امنیت سایبری و سواد رسانه‌ای بود. یافته‌های پژوهش نشان داد که همبستگی مثبت و معنادار بین سواد رسانه‌ای، امنیت سایبری و هویت دیجیتال وجود دارد. سواد رسانه‌ای به‌طور مستقیم و غیرمستقیم (از طریق امنیت سایبری) بر هویت دیجیتال تأثیر مثبت دارد. امنیت سـایبری بیشـترین تأثیر را بر هویت دیجیتال دارد. زنان نسبت به مردان از سطح سواد رسانه‌ای بالاتری برخوردار بودند. نتایج پژوهش نشـان داد که سواد رسانه‌ای به‌عنوان یک مهارت کلیدی، نقش مهمی در تقویت امنیت سـایبری و حفاظت از هویت دیجیتال در عصر هوش مصنوعی ایفا می‌کند. هویت دیجیتال به‌عنوان یک دارایی ارزشمند نیازمند حفاظت است، امنیت سایبری ابزارهای این حفاظت را فراهم می‌کند، و سواد رسانه‌ای کاربران را توانمند می‌سازد تا از این ابزارها به‌طور مؤثر استفاده کنند. افزایش آگاهی کاربران از طریق آموزش سـواد رسـانه‌ای می‌تواند به کاهش تهدیدات سایبری و بهبود امنیت دیجیتال کمک کند. در کنار هم، این سه مفهوم به ایجاد یک محیط دیجیتال امن و قابل‌اعتماد کمک می‌کنند.

کلیدواژه: امنیت سایبری، سواد رسانه‌ای، هویت دیجیتال، هوش مصنوعی.

---

* اسـتادیار گروه مشارکت‌ها ارتباطات، پژوهشـگاه مطالعات آموزش و پرورش، سازمان پژوهش و برنامه‌ریزی آموزشی، تهران، ایران alijafari@oerp.ir

نحوهٔ استناد به این مقاله: جعفری، علی (۱۴۰۵). نقش سواد رسانه ای در امنیت سایبری و هویت دیجیتال در عصر هوش مصنوعی. رسانه، ۳۷(۱)، ۵۳-۷۲ .

مقدمه

با گسترش فناوری‌های دیجیتال و هوش مصنوعی[1]، مفاهیم هویت دیجیتال، امنیت سایبری و سواد رسانه‌ای به موضوعات کلیدی در عصر حاضر تبدیل شده‌اند. این مفاهیم نه‌تنها به‌صورت جداگانه اهمیت دارند، بلکه ارتباط تنگاتنگی با یکدیگر دارند.

در عصر هوش مصنوعی، هویت دیجیتال و امنیت سایبری به‌عنوان دو مؤلفهٔ حیاتی در فضای مجازی مطرح هستند. هویت دیجیتال[2] به مجموعه‌ای از اطلاعات دیجیتالی اشاره دارد که یک فرد یا سازمان را به‌گونه‌ای منحصربه‌فرد شناسایی می‌کند. این اطلاعات می‌توانند شامل نام، آدرس، شماره‌های شناسایی، داده‌های بیومتریک (مانند اثر انگشت یا تشخیص چهره) و حتی رفتارهای برخط (مانند تاریخچهٔ جست‌وجو یا تراکنش‌ها) باشند. هویت دیجیتال به‌عنوان نمایندهٔ دیجیتالی یک فرد، نقش اساسی در دسترسی به خدمات برخط، احراز هویت و تعاملات دیجیتال ایفا می‌کند (سازمان همکاری و توسعه اقتصادی، ۲۰۱۹).

هویت دیجیتال، هدف اصلی بسیاری از حملات سایبری است. حملاتی مانند فیشینگ، کلاهبرداری‌های برخط و جعل هویت[3] می‌توانند به سرقت یا سوءاستفاده از هویت دیجیتال منجر شوند. امنیت سایبری با ارائهٔ ابزارها و روش‌های محافظتی مانند رمزنگاری، احراز هویت دو مرحله‌ای و سیستم‌های تشخیص نفوذ، از هویت دیجیتال در برابر این تهدیدات محافظت می‌کند (چزنی و سیترون[4]، ۲۰۱۹).

امنیت سایبری[5] به مجموعه‌ای از روش‌ها، فناوری‌ها و فرایندها اشاره دارد که برای محافظت از سیستم‌های رایانه‌ای، شبکه‌ها، داده‌ها و اطلاعات دیجیتال در برابر حملات سایبری، دسترسی غیرمجاز و سوءاستفاده طراحی شده‌اند. امنیت سایبری به‌دنبال تضمین محرمانگی، یکپارچگی و دسترس‌پذیری اطلاعات است (مؤسسه ملی استاندارد و فناوری[6]، ۲۰۲۰).

در عصر دیجیتال، هویت فردی نه‌تنها در فضای فیزیکی، بلکه در فضای مجازی نیز تعریف می‌شود. توسعهٔ فناوری‌های نوین، به‌ویژه هوش مصنوعی، چالش‌های جدیدی در حوزهٔ هویت دیجیتال و امنیت سایبری ایجاد کرده است. در این میان، سواد رسانه‌ای به‌عنوان عاملی کلیدی در افزایش آگاهی کاربران و تقویت رفتارهای محافظتی در فضای دیجیتال شناخته می‌شود (لیوینگستون و هلپسر[7]، ۲۰۰۷).

یکی از چالش‌های اساسی در عصر هوش مصنوعی، تغییر ماهیت هویت از قالبی ثابت

1. Artificial Intelligence (AI)
2. Digital Identity
3. Identity Theft
4. Chesney & Citron
5. Cybersecurity
6. NIST
7. Livingstone & Helsper

و مبتنی‌بر منابع سنتی به هویتی چندپاره، سیال و شبکه‌ای است. در این گذار، رسانه‌های اجتماعی با فراهم آوردن امکان خوداظهاری و بازنمایی‌های متعدد، نقشی کلیدی در بازتعریف هویت کاربران ایفا می‌کنند. جعفری و فرج‌زاده (۱۴۰۳) در پژوهش خود با تأکید بر این تمایز، نشان می‌دهند نوجوانانی که رسانهٔ غالب آن‌ها از نوع اجتماعی است، خود را به نفع هویتی جهانی یا جهان‌وطنی بازنمایی می‌کنند؛ در حالی که مصرف‌کنندگان غالب رسانه‌های جمعی در پی پاسداشت منابع سنتی هویت ملی هستند. این یافته نشان می‌دهد که شکل‌گیری هویت دیجیتال در بستر رسانه‌های نوین، تابع منطق متفاوتی نسبت به هویت‌های شکل‌گرفته در رسانه‌های جریان اصلی است.

سواد رسانه‌ای[1] به توانایی افراد در درک، تحلیل، ارزیابی و ایجاد محتوای رسانه‌ای اشاره دارد. این مفهوم شامل مهارت‌های تفکر انتقادی در مواجههٔ با اطلاعات دیجیتال، تشخیص منابع معتبر و درک تأثیرات رسانه‌ها بر افکار و رفتارها می‌شود. در عصر دیجیتال، سواد رسانه‌ای به‌عنوان یک مهارت ضروری برای مقابله با اطلاعات نادرست، محتوای جعلی و تهدیدات سایبری مطرح می‌شود (یونسکو[2]، ۲۰۲۱).

سواد رسانه‌ای به افراد کمک می‌کند تا تهدیدات سایبری را شناسایی کنند و از خود در برابر آن‌ها محافظت کنند. برای مثال، توانایی تشخیص ایمیل‌های فیشینگ، شناسایی محتوای جعلی مانند دیپ‌فیک[3] و درک خطرات اشتراک‌گذاری اطلاعات شخصی برخط، همگی بخشی از سواد رسانه‌ای هستند. این مهارت‌ها به‌طور مستقیم به امنیت سایبری مرتبط هستند؛ زیرا کاربران آگاه می‌توانند از وقوع بسیاری از حملات سایبری جلوگیری کنند (لیوینگستون[4]، ۲۰۱۸).

بنابراین، تقویت سواد رسانه‌ای در جامعه می‌تواند نقش مؤثری در افزایش آگاهی کاربران نسبت به تهدیدات سایبری و حفاظت از هویت دیجیتال آن‌ها داشته باشد. آموزش مهارت‌های لازم برای تشخیص محتوای جعلی، ارزیابی منابع اطلاعاتی و درک تأثیرات رسانه‌ها از جمله اقداماتی است که می‌تواند به بهبود امنیت سایبری در عصر هوش مصنوعی کمک کند.

با ظهور هوش مصنوعی، تهدیدات سایبری پیچیده‌تر شده‌اند. برای نمونه، فناوری‌هایی مانند دیپ‌فیک می‌توانند هویت دیجیتال افراد را جعل کنند و اعتماد عمومی را تحت‌تأثیر قرار دهند. در این زمینه سواد رسانه‌ای به افراد کمک می‌کند تا محتوای تولیدشده توسط هوش مصنوعی را تشخیص دهند و از تأثیرات منفی آن جلوگیری کنند. از سوی دیگر، امنیت سایبری با استفاده از هوش مصنوعی برای تشخیص و مقابله با این تهدیدات، به حفاظت از هویت دیجیتال کمک می‌کند (زوبوف[5]، ۲۰۱۹).

1. Media Literacy
2. UNESCO
3. Deepfakes
4. Livingstone
5. Zuboff

براساس گزارش آی‌بی‌ام سکیوریتی[1] (۲۰۲۲)، هزینهٔ متوسط یک نقض داده در سال ۲۰۲۱ به چهار میلیون و بیست و چهار هزار دلار رسیده که بالاترین رقم در تاریخ این گزارش است. این گزارش نشان می‌دهد حملات سایبری به هویت دیجیتال و داده‌های شخصی به یک تهدید جدی تبدیل شده‌اند.

گزارش یونسکو (۲۰۲۱) نشان داد کشورهایی که برنامه‌های آموزش سواد رسانه‌ای را در مدارس و جامعه اجرا کرده‌اند، کاهش چشمگیری در میزان کلاهبرداری‌های برخط و انتشار اطلاعات جعلی تجربه کرده‌اند. مطالعه‌ای توسط چزنی و سیترون[2] (۲۰۱۹) نشان داد فناوری دیپ‌فیک به‌عنوان یک تهدید جدی برای هویت دیجیتال و امنیت سایبری مطرح است. این مطالعه پیش‌بینی کرد که تا سال ۲۰۲۵، بیش از ۹۰ درصد از محتوای برخط ممکن است توسط هوش مصنوعی تولید یا دستکاری شود.

گزارش مک‌آفی[3] (۲۰۲۰) نیز نشان داد ۶۰ درصد از کاربران اینترنت در تشخیص محتوای جعلی تولیدشده توسط هوش مصنوعی مشکل دارند که این موضوع اهمیت سواد رسانه‌ای را بیش از پیش آشکار می‌کند.

براساس شواهد موجود، سؤال اصلی پژوهش حاضر این است که سواد رسانه‌ای چه نقشی در امنیت سایبری و هویت دیجیتال در عصر هوش مصنوعی دارد؟

پیشینهٔ پژوهش

عزیزی‌نیا و فیاض (۱۴۰۳) در پژوهشی با عنوان "نقش مؤثر سواد رسانه‌ای در امنیت فضای مجازی" به این نتیجه رسیدند که ارتقای سواد رسانه‌ای کاربران فضای مجازی موجب تمایل به تفکر و تأمل بیشتر در ارائهٔ اطلاعات شخصی و دریافت اطلاعاتی شده که مخاطب را احاطه کرده است. این امر بر افزایش سطح مهارت استفاده و کم شدن آسیب‌های بمباران اطلاعاتی شبکه‌های مجازی مؤثر است. فضای مجازی حفظ حریم خصوصی کاربر را به چالش می‌کشد. حریم خصوصی اطلاعات یکی از مهم‌ترین مسائل و چالش‌های افراد برای قرارگیری در فضای مجازی است. در صورتی که مراقب نباشند، ممکن است قربانی از دست دادن یا انتشار اطلاعات شوند. سواد رسانه‌ای توانایی فرد را در کنترل شخصی اطلاعات تقویت می‌کند.

تندرو و همکاران (۱۴۰۲) در پژوهشی با عنوان "بررسی اهمیت آموزش سواد رسانه‌ای و نقش آن در کاهش آسیب‌های فضای مجازی" به این نتیجه رسیدند که آموزش سواد رسانه‌ای می‌تواند به افزایش امنیت دیجیتال و محافظت از حریم خصوصی در فضای مجازی کمک کند. نتایج پژوهش نشان می‌دهد که آگاهی از خطرات فضای مجازی و آموزش روش‌های صحیح

1. IBM Security
2. Chesney & Citron
3. McAfee

اســتفادهٔ از آن، به‌ویژه در میان نوجوانان و جوانان، می‌تواند از بســیاری از آسیب‌ها جلوگیری کرده و افراد را قادر سازد تا از فضای مجازی به‌طور مؤثر و سالم بهره‌برداری کنند.

محمدی و دانایی (۱۴۰۱) با استفاده از روش نظریهٔ داده‌بنیاد، الگویی برای پدافند غیرعامل رســانه‌ای در ایران ارائه داده‌اند که شــامل ســه بعد اصلی زمان اجرای اقدامات (پیش، حین و پس از جنگ روانی)، مجریان اقدامات (جمعی و فردی) و نوع اقدامات (رســانه‌ای، فرهنگی، اجتماعی، سیاســی) اســت. در این الگو، "افزایش سواد رســانه‌ای در جامعه به‌عنوان یکی از مفاهیم کلیدی در بعد زمان اجرا (پیش از جنگ روانی) و نیز در بعد مجریان (اقدامات فردی) شناسایی شده است.

رسولی و همکاران (۱۴۰۰) در پژوهشی با عنوان "ارائهٔ چارچوب مدیریت هویت دیجیتال در فضای سایبر با رویکرد آمیخته" به این نتیجه رسیدند که عامل "برنامه‌ریزی راهبردی" تأثیرگذارترین عامل در مدیریت هویت دیجیتال اســت. در حل مســئله به روش ترکیبی فرآیند تحلیل شــبکه و دیمتل نیز مدیریت دسترســی در عوامل اصلی و کنترل دسترســی به کلیهٔ منابع و اطلاعات تنها از طریق سیستم مدیریت هویت دیجیتال در عوامل فرعی اولویت اول را کسب کردند.

خاکسار ازغندی (۱۳۹۸) در پژوهشی با عنوان "بررسی رابطهٔ بین سواد رسانه‌ای و قربانی سایبری" به این نتیجه رسید که سواد رسانهٔ دانش‌آموزان دختر بیشتر از سواد رسانهٔ دانش‌آموزان پســر است و همچنین قربانی ســایبری دانش‌آموزان پسر بیشتر از قربانی سایبری دانش‌آموزان دختر اســت. همچنین نتایج نشان می‌دهد که بین سواد رسانهٔ دختران و پسران رابطهٔ معناداری وجود دارد و این‌که بین قربانی سایبری دختران و پسران رابطهٔ معناداری وجود ندارد.

چن[1] و همکاران (۲۰۲۲) در پژوهش "اطلاعات نادرســت مبتنی‌بر هوش مصنوعی و سواد دیجیتال"، به بررسی تأثیر هوش مصنوعی در گسترش اطلاعات نادرست و نقش سواد رسانه‌ای در کاهش تأثیرات منفی آن پرداخته‌اند. یافته‌های این مطالعه نشــان می‌دهد که کاربران با سواد رســانه‌ای بالا، توانایی بهتری در تشــخیص اخبــار جعلی دارند و کمتــر تحت‌تأثیر اطلاعات دستکاری‌شده قرار می‌گیرند.

نگویــن[2] و همــکاران (۲۰۲۱) در مطالعــهٔ "هــوش مصنوعی و امنیت ســایبری: تهدیدها و فرصت‌ها"، تأثیر هوش مصنوعی بر امنیت ســایبری را بررســی کرده‌اند. آن‌ها بیان می‌کنند که در حالــی که هوش مصنوعی می‌تواند ابزارهای امنیتی قدرتمنــدی ایجاد کند، اما هم‌زمان می‌تواند برای حملات پیشرفتهٔ سایبــری مانند فیشینگ مبتنی‌بر یادگیری ماشین نیز مورد استفاده قرار گیرد.

گوئــس[3] و همکاران (۲۰۲۰) در مقاله‌ای با عنوان "مواجههٔ با اطلاعات نادرســت و اتخاذ شــیوه‌های امنیت دیجیتال"، نشــان داده‌اند که سواد رســانه‌ای بالا باعث کاهش آسیب‌پذیری

1. Chen
2. Nguyen
3. Guess

کاربران در برابر تهدیدات سـایبری می‌شـود و کاربران آگاه‌تر، بیشتر از ابزارهای امنیتی مانند احراز هویت دو مرحله‌ای استفاده می‌کنند.

بوچانـان[1] و همکاران (۲۰۱۷) در مطالعه‌ای با عنوان "نقش سـواد دیجیتال در حفاظت از حریم خصوصی آنلاین"، به بررسـی رابطهٔ بین سـواد دیجیتال و رفتارهای امنیتی پرداخته‌اند. یافته‌های این پژوهش نشان می‌دهد که کاربران با سطح بالای سواد رسانه‌ای، بیشتر از رمزهای قوی استفاده می‌کنند و کمتر اطلاعات حساس خود را در اینترنت به اشتراک می‌گذارند.

ون‌دایک[2] (۲۰۱۴) در مقاله‌ای با عنوان "داده‌محورسـازی، داده‌گرایی و نظارت داده‌محور" بـه چالش‌های مرتبـط با هویت دیجیتال در دنیـای داده‌محور پرداخته و نقـش کلان‌داده‌ها و الگوریتم‌های هوش مصنوعی در تغییر درک کاربران از خود و محیط دیجیتال را بررسی می‌کند.

لیوینگستون و هلسپر (۲۰۰۷) در مقالهٔ "درجات شمول دیجیتال: کودکان، جوانان و شکاف دیجیتال"، نشـان داده‌اند که سـواد رسـانه‌ای یکی از مهم‌ترین عوامل در حفاظت از اطلاعات شخصی در فضای برخط است. کاربران با سطح بالای سواد رسانه‌ای، کمتر در معرض حملات سایبری قرار می‌گیرند.

با بررسـی پیشینه‌های پژوهشی مرتبط با هویت دیجیتال، امنیت سایبری، سواد رسانه‌ای و هوش مصنوعی، مشـخص شـد که بسیاری از مطالعات پیشین به بررسی این مفاهیم به‌صورت جداگانه پرداخته‌اند. نوآوری پژوهش حاضر در چند بعد کلیدی قابل مشاهده است:

بسـیاری از پژوهش‌های قبلی مانند مطالعات ون‌دایک (۲۰۱۴) به بررسی هویت دیجیتال به‌عنـوان یک مفهوم مسـتقل پرداخته‌اند، اما این پژوهش تلاش می‌کنـد هویت دیجیتال را در ارتباط با امنیت سـایبری و سواد رسـانه‌ای بررسی کند. برخی پژوهش‌های پیشین دربارهٔ تأثیر هوش مصنوعی بیشتر بر روی مسائل امنیت سایبری و حریم خصوصی متمرکز بوده‌اند (نگوین و همـکاران، ۲۰۲۱؛ زوبـوف، ۲۰۱۹). اما کمتر به این پرداخته شـده اسـت که چگونه هوش مصنوعی می‌تواند بر هویت دیجیتال و سواد رسانه‌ای کاربران تأثیر بگذارد.

چارچوب نظری پژوهش

نظریهٔ هویت اجتماعی: این نظریه بیان می‌کند که افراد براساس عضویت در گروه‌های اجتماعی، هویـت خود را شـکل می‌دهند. در فضـای دیجیتال، تعاملات برخط و حضور در شـبکه‌های اجتماعی نقش مهمی در شـکل‌گیری هویت دیجیتال افـراد دارند (رینگولد[3]، ۲۰۰۰؛ تاجفل و ترنر[4]، ۲۰۰۴). ارتباط این نظریه با موضوع مقاله در این است که کاربران فضای مجازی هویت

1. Buchanan
2. Van Dijck
3. Rheingold
4. Tajfel & Turner

دیجیتـــال خود را از طریق تعاملات برخط، شـــبکه‌های اجتماعی و سیســـتم‌های احراز هویت دیجیتال تعریف می‌کنند و امنیت سایبری از این هویت محافظت می‌کند تا افراد قربانی سرقت هویت، فیشینگ و جعل هویت دیجیتال نشوند.

نظریهٔ خودپنداره دیجیتال: بلک[1] مفهوم "خودگسترش‌یافته[2]" را مطرح می‌کند که بیانگر تأثیر فناوری بر درک افراد از هویت شـــخصی آن‌ها است. طبق این نظریه، کاربران با اشتراک‌گذاری اطلاعات شـــخصی در فضای برخط، بخشـــی از هویت خود را در دنیای دیجیتال می‌ســـازند (بلک، ۲۰۱۳). ارتباط این نظریه با موضوع مقاله در این اســـت که ســـواد رسانه‌ای نقش مهمی در چگونگـــی مدیریت و نمایش هویـــت دیجیتال دارد. کاربران بایـــد توانایی تحلیل محتوای رسانه‌ای را داشته باشند تا از هویت دیجیتال خود در برابر دستکاری اطلاعات و جعل هویت محافظت کنند.

نظریهٔ رفتار برنامه‌ریزی‌شده: این نظریه بر تأثیر نگرش، هنجارهای اجتماعی و کنترل رفتاری ادراک‌شده بر تصمیمات کاربران در امنیت سایبری تأکید دارد. افراد با آگاهی بیشتر، رفتارهای ایمن‌تری در فضای دیجیتال نشـــان می‌دهند (یون[3]، ۲۰۱۱؛ آجزن[4]، ۱۹۹۱). ارتباط این نظریه با موضوع مقاله در این اســـت که افراد با سواد رسانه‌ای بالاتر، نگرش مثبت‌تری نسبت به‌رعایت امنیت ســـایبری دارند و رفتارهای محافظتی بیشتری نشـــان می‌دهند. هنجارهای اجتماعی در فضای دیجیتال (مانند توصیه به استفاده از رمزهای قوی و احراز هویت دو مرحله‌ای) بر رفتار کاربران تأثیر می‌گذارد. کنترل رفتاری ادراک‌شـــده نیز بر اســـتفاده از ابزارهای امنیت ســـایبری تأثیر دارد.

نظریهٔ اعتماد الکترونیکی: در این نظریه، امنیت ســـایبری وابســـته به میزان اعتماد کاربران به سیســـتم‌های دیجیتال و اقدامات حفاظتی اســـت. این اعتماد زمانی افزایش می‌یابد که کاربران از تهدیدات آگاهی داشته و راهکارهای ایمنی را رعایت کنند (مک‌نایت[5] و همکاران، ۲۰۰۲). ارتبـــاط این نظریه با موضوع مقاله در این اســـت که کاربرانی که به سیســـتم‌های احراز هویت دیجیتال و پروتکل‌های امنیت ســـایبری اعتماد دارنـــد، هویت دیجیتال خود را امن‌تر مدیریت می‌کنند. ســـواد رســـانه‌ای به کاربران کمک می‌کند تا منابع معتبر را شناسایی کنند و کمتر قربانی حملات فیشینگ شوند.

نظریهٔ ســـواد رســـانه‌ای انتقادی: این نظریه بیـــان می‌کند که کاربران بایـــد مهارت‌های تفکر انتقادی را برای تحلیل اطلاعات دیجیتال و تشخیص اخبار جعلی تقویت کنند. سواد رسانه‌ای نقش مهمی در پیشـــگیری از فریب‌های دیجیتال و تقویت امنیت ســـایبری دارد (لیوینگستون،

1. Belk
2. Extended Self
3. Yoon
4. Ajzen
5. McKnight

۲۰۱۸؛ کلنر و شـر[1]، ۲۰۰۵). ارتباط این نظریه با موضوع مقاله در این اسـت که سواد رسانه‌ای نقش مهمی در پیشـگیری از مهندسـی اجتماعی و حملات سـایبری دارد. افراد آگاه‌تر، کمتر قربانی اطلاعات نادرست و محتوای جعلی می‌شوند.

نظریهٔ پردازش اطلاعات دوگانه: یکی از نظریات بنیادین در روان‌شناسـی شـناختی اسـت که چگونگی پردازش اطلاعات توسـط انسـان را تبیین می‌کند. این نظریه ابتدا توسط شلایینی چایکن و یاکوف تروپ در سال ۱۹۹۹ مطرح شد. این نظریه بیان می‌کند که کاربران از دو روش برای پردازش اطلاعات اسـتفاده می‌کنند: پردازش سـطحی (مبتنی‌بر شهود) و پردازش عمیق (مبتنی‌بر تحلیل) (چایکن و تروپ[2]، ۱۹۹۹).

پردازش سـطحی بر سـرعت، خودکار بودن و اسـتفاده از میانبرهای ذهنی متکی اسـت. افراد بدون بررسی عمیق اطلاعات، براساس احساسات، باورهای پیشین و نشانه‌های سطحی مانند شـهرت منبع یا جذابیـت بصری، تصمیم‌گیـری می‌کنند (تورسـکی و کانمن[3]، ۱۹۷۴). ویژگی‌های پردازش سـطحی عبارتند از: سـریع و کم‌هزینه از نظر شناختی، مبتنی‌بر میانبرهای ذهنی و اطلاعات سطحی، بیشتر تحت‌تأثیر هیجانات و سوگیری‌های شناختی و مستعد پذیرش اطلاعات نادرست و تبلیغات فریبنده.

در پـردازش عمیـق، افراد اطلاعات را به‌صورت دقیق، آگاهانه و با تفکر انتقادی بررسـی می‌کنند. تصمیم‌گیری در این حالت زمان‌برتر اسـت اما احتمال خطای شـناختی کمتر خواهد بود (کانمن[4]، ۲۰۱۱). ویژگی‌های پردازش عمیق عبارتند از: نیاز به تمرکز و تلاش ذهنی بیشتر، مبتنی‌بر اسـتدلال منطقی و تحلیل دقیق اطلاعات، کمتر تحت‌تأثیر سـوگیری‌های شـناختی و توانایی تشخیص اخبار جعلی و تبلیغات گمراه‌کننده.

در دنیای دیجیتال که پر از اطلاعات نادرسـت، اخبار جعلی و تهدیدات سـایبری اسـت، پردازش عمیق اهمیت دوچندانی دارد (لواندوسکی[5] و همکاران، ۲۰۱۷). سواد رسانه‌ای کمک می‌کند تا کاربران از پردازش سطحی به سمت پردازش عمیق حرکت کرده و در برابر تهدیدات سـایبری آگاهانه‌تر رفتار کنند (چایکن و تروپ، ۱۹۹۹). ارتباط این نظریه با موضوع مقاله در این اسـت که سواد رسـانه‌ای به کاربران کمک می‌کند تا به‌جای پردازش سطحی، اطلاعات را عمیق‌تر بررسی کنند و در برابر اخبار جعلی، تبلیغات گمراه‌کننده و تهدیدات سایبری آگاهانه‌تر رفتـار کنند. کاربران با پردازش عمیق می‌توانند تفـاوت بین منابع معتبر و منابع غیرقابل‌اعتماد را تشخیص دهند.

چارچوب نظری پژوهش براسـاس ترکیـب نظریه‌های مرتبط با هویـت دیجیتال، امنیت

1. Kellner & Share
2. Chaiken & Trope
3. Tversky & Kahneman
4. Kahneman
5. Lewandowsky

سـایبری و سـواد رسانه‌ای شکل گرفته است و می‌تواند در تحقیقات آینده نیز توسعه یابد. این چارچـوب نظری، مبنای محکمی برای تحلیل داده‌هـای پژوهش فراهم می‌کند و نقش کلیدی سواد رسانه‌ای در حفظ امنیت و هویت دیجیتال را تبیین می‌کند. این نظریه‌ها همگی در ارتباط با مدیریت هویت دیجیتال، امنیت سایبری و سواد رسانه‌ای هستند:

- نظریه‌هـای هویـت (هویت اجتماعی و خودپنـدارهٔ دیجیتال): نشـان می‌دهند که چگونه هویت دیجیتال افراد شکل می‌گیرد.
- نظریه‌های رفتار (رفتار برنامه‌ریزی‌شده و اعتماد الکترونیکی): تبیین می‌کنند که چرا برخی افراد از امنیت سایبری استفاده می‌کنند و برخی خیر؟
- نظریه‌های پردازش اطلاعات (پردازش دوگانه و سواد رسانه‌ای انتقادی): تأکید می‌کنند که چرا برخی کاربران اخبار جعلی را باور کرده و امنیت دیجیتال خود را به خطر می‌اندازند.

روش پژوهش

این پژوهش از نظر هدف، کاربردی و از نظر شـیوهٔ گردآوری اطلاعات از نوع پیمایشـی بود. جامعـهٔ آماری ایـن پژوهش تمامی کاربران فضای مجازی و شـبکه‌های اجتماعی در ایران را شـامل می‌شـود که به‌صورت فعال در محیط‌های دیجیتال حضور دارند و در معرض تهدیدات سایبری قرار می‌گیرند. برای تعیین حجم نمونه، از فرمول کوکران برای جامعهٔ نامحدود استفاده شد و نمونه شامل ۳۸۴ نفر بود که با روش نمونه‌گیری تصادفی طبقه‌ای (بر حسب جنس، سن، تحصیلات و میزان استفاده از اینترنت) انتخاب شدند.

ابزار اصلی پژوهش، پرسشـنامهٔ استاندارد در سـه بخش است: پرسشنامهٔ هویت دیجیتال (براسـاس شـاخص‌های تعامل برخط، حضور دیجیتـال و حفاظت از اطلاعات شـخصی)، پرسشـنامهٔ امنیت سـایبری (براساس شـاخص‌های آگاهی از تهدیدات، رعایت اصول ایمنی و اسـتفاده از ابزارهای محافظتی) و پرسشنامهٔ سواد رسانه‌ای (براساس شاخص‌های ارزیابی انتقادی اطلاعات، آگاهی از اخبار جعلی و توانایی تحلیل محتوای دیجیتال). روایی پرسشنامه با استفاده از نظر خبرگان و تحلیل عاملی تأییدی تأیید شد. پایایی آن نیز از طریق آلفای کرونباخ بررسـی شد؛ مقدار آلفای کرونباخ برای کل پرسشنامه ۰/۸۶ است که از پایایی بالا و قابل قبول ابـزار اندازه‌گیری حکایت می‌کند. ضریب آلفای کرونبـاخ متغیرهای تحقیق در جدول ۱ آمده است.

جدول ۱. آلفای کرونباخ برای بررسی پایایی پرسشنامه

متغیر	تعداد گویه‌ها	آلفای کرونباخ (α)
هویت دیجیتال	۸	۰/۸۲
امنیت سایبری	۱۰	۰/۸۵
سواد رسانه‌ای	۱۲	۰/۸۸
کل پرسشنامه	۳۰	۰/۸۶

بـــرای تجزیه‌وتحلیل داده‌ها، از روش‌های آمـــار توصیفی (میانگین، انحراف معیار، فراوانی) و آمار استنباطی (آزمون رگرسیون، تحلیل مسیر، مدل‌سازی معادلات ساختاری) با نرم‌افزارهای AMOS استفاده شد.

یافته‌ها

جدول ۲. متغیرهای جمعیت‌شناختی نمونهٔ پژوهش

متغیر	دسته‌بندی	فراوانی (N)	درصد
جنسیت	زن	۱۸۰	۴۶/۹
	مرد	۲۰۴	۵۳/۱
سن	۱۸ تا ۲۵ سال	۱۲۰	۳۱/۳
	۲۶ تا ۳۵ سال	۱۴۰	۳۶/۵
	۳۶ تا ۴۵ سال	۸۰	۲۰/۸
	۴۶ سال و بالاتر	۴۴	۱۱/۴
تحصیلات	دیپلم و کمتر	۵۰	۱۳/۰
	کارشناسی	۱۸۰	۴۶/۹
	کارشناسی‌ارشد	۱۲۰	۳۱/۳
	دکتری و بالاتر	۳۴	۸/۹

متغیر	دسته‌بندی	فراوانی (N)	درصد
میزان استفاده از اینترنت در روز	کمتر از ۲ ساعت	۴۵	۱۱/۷
	۲ تا ۴ ساعت	۱۲۰	۳۱/۳
	۴ تا ۶ ساعت	۱۴۰	۳۶/۵
	بیش از ۶ ساعت	۷۹	۲۰/۵

نتایج جدول ۲ نشـــان می‌دهد که مردان (۵۳/۱ درصد) ســـهم بیشتری در نمونه دارند. بیشترین گروه سنی در بین پاسخ‌دهندگان ۲۶ تا ۳۵ سال (۳۶/۵ درصد) است. بیشتر پاسخ‌دهندگان دارای تحصیلات کارشناســـی (۴۶/۹ درصد) هستند. بیشـــترین افراد بین ۴ تا ۶ ساعت در روز (۳۶/۵ درصد) از اینترنت استفاده می‌کنند.

جدول ۳. آمار توصیفی متغیرهای پژوهش

متغیر	میانگین	انحراف معیار	کمترین مقدار	بیشترین مقدار
هویت دیجیتال	۳/۷۵	۰/۶۸	۲/۱۰	۴/۹۰
امنیت سایبری	۳/۹۰	۰/۷۲	۲/۳۰	۵/۰۰
سواد رسانه‌ای	۴/۱۰	۰/۶۵	۲/۵۰	۵/۰۰

با توجه به داده‌های جدول ۳، میانگین ۳/۷۵ نشـــان می‌دهد که افراد در حد متوسط به بالایی از هویت دیجیتال خود آگاه هستند. امنیت سایبری با میانگین ۳/۹۰، نشان می‌دهد که افراد تا حد خوبی نکات امنیتی را رعایت می‌کنند، اما هم‌چنان نیاز به بهبود دارند. سواد رسانه‌ای بیشترین میانگین (۴/۱۰) را دارد که از آگاهی به نســـبت بالای افراد در تحلیل محتوای رسانه‌ها حکایت می‌کند.

جدول ۴. آزمون همبستگی پیرسون بین متغیرها

متغیرها	هویت دیجیتال	امنیت سایبری	سواد رسانه‌ای
هویت دیجیتال	۱	۰/۶۵	۰/۵۸
امنیت سایبری	۰/۶۵	۱	۰/۷۲
سواد رسانه‌ای	۰/۵۸	۰/۷۲	۱

جدول ۴ نشان می‌دهد که بین هویت دیجیتال و امنیت سایبری همبستگی مثبت معنادار (۰/۶۵) وجود دارد. بین سواد رسانه‌ای و امنیت سایبری قوی‌ترین رابطه (۰/۷۲) مشاهده می‌شود که نشان می‌دهد افراد دارای سواد رسانه‌ای بالاتر، امنیت سایبری بهتری دارند.

آزمون رگرسیون چندگانه (تأثیر سواد رسانه‌ای و امنیت سایبری بر هویت دیجیتال)

جدول ۵. ضرایب رگرسیون

متغیر مستقل	ضریب استاندارد (β)	مقدار t	سطح معناداری
امنیت سایبری	۰/۵۲	۸/۴۲	۰/۰۰۰
سواد رسانه‌ای	۰/۳۹	۶/۷۸	۰/۰۰۰
R^2 = ۰/۴۸	F = ۳۵/۷۲	P = ۰/۰۰۰	

نتایج جدول ۵ نشان می‌دهد که امنیت سایبری بیشترین تأثیر را بر هویت دیجیتال دارد. (β = ۰/۵۲) سواد رسانه‌ای نیز تأثیر معناداری بر هویت دیجیتال دارد (β = ۰/۳۹)، اما نسبت به امنیت سایبری اثر کمتری دارد. ضریب تعیین (R^2 = ۰/۴۸) نشان می‌دهد که ۴۸٪ تغییرات در هویت دیجیتال توسط این دو متغیر قابل توضیح است.

جدول ۶. آزمون T مستقل (مقایسهٔ سواد رسانه‌ای بین مردان و زنان)

گروه	میانگین	انحراف معیار	مقدار t	درجهٔ آزادی (df)	سطح معناداری (Sig)
مردان	۴/۰۲	۰/۷۰	۲/۳۴	۳۸۲	۰/۰۲۱
زنان	۴/۱۸	۰/۶۰			

مطابق با داده‌های جدول فوق، زنان دارای میانگین سواد رسانه‌ای بالاتری نسبت به مردان هستند (۴/۱۸ در مقابل ۴/۰۲). مقدار t معنادار (p = ۰/۰۲۱) است، بنابراین تفاوت بین دو گروه از نظر آماری تأیید می‌شود.

مدل‌سازی معادلات ساختاری[1] و تحلیل مسیر

در پژوهش حاضر برای بررسی روابط بین سواد رسانه‌ای، امنیت سایبری و هویت دیجیتال از مدل‌سازی معادلات ساختاری و تحلیل مسیر استفاده شده است. در ادامه، فرآیند اجرای این روش‌ها و چگونگی استفاده از آن‌ها در پژوهش توضیح داده می‌شود.

1. SEM

مراحل اجرای مدل‌سازی معادلات ساختاری در پژوهش

مرحلهٔ ۱. تدوین مدل مفهومی

در ابتدا، براســاس مبانی نظری و پژوهش‌های پیشین، یک مدل مفهومی طراحی شد که روابط بین متغیرها را مشــخص می‌کند. در این مدل، ســواد رســانه‌ای به‌عنوان متغیر مســتقل، امنیت سایبری به‌عنوان متغیر میانجی و هویت دیجیتال به‌عنوان متغیر وابسته در نظر گرفته شد.

مرحلهٔ ۲. طراحی مدل اندازه‌گیری

مدل اندازه‌گیری مشــخص می‌کند که چگونه متغیرهای مشاهده‌شــده (گویه‌های پرسشــنامه) به متغیرهای پنهان (ســواد رســانه‌ای، امنیت ســایبری، هویت دیجیتال) مرتبط هستند. در این پژوهش:

- ســواد رسانه‌ای از طریق شــاخص‌هایی مانند ارزیابی انتقادی اطلاعات و آگاهی از اخبار جعلی اندازه‌گیری شد.
- امنیت سایبری براساس رعایت اصول ایمنی و آگاهی از تهدیدات سایبری سنجیده شد.
- هویت دیجیتال نیز براساس حفظ حریم خصوصی و تعامل برخط ایمن اندازه‌گیری شد.

روایی این مدل با استفاده از تحلیل عاملی تأییدی بررسی شد.

مرحلهٔ ۳. تدوین مدل ساختاری

مدل ســاختاری نشــان‌دهندهٔ روابط بین متغیرهای پنهان است. در این پژوهش، مسیرهای علی زیر در مدل بررسی شدند:

۱. تأثیر سواد رسانه‌ای بر امنیت سایبری.
۲. تأثیر امنیت سایبری بر هویت دیجیتال.
۳. تأثیر سواد رسانه‌ای بر هویت دیجیتال (مستقیم و غیرمستقیم از طریق امنیت سایبری).

اجرای تحلیل مسیر

تحلیل مسیر برای بررسی ضرایب تأثیر متغیرها بر یکدیگر به‌کار رفت. نرم‌افزار AMOS برای تحلیل داده‌ها مورد استفاده قرار گرفت.

جدول ۷. ضرایب مسیر در مدل تحلیل مسیر

مسیر علی	ضریب استاندارد (β)	مقدار t	سطح معناداری (p-value)	نتیجه
سواد رسانه‌ای ← هویت دیجیتال	۰/۳۶	۷/۲۴	۰/۰۰۰	معنادار
امنیت سایبری ← هویت دیجیتال	۰/۴۸	۸/۹۲	۰/۰۰۰	معنادار
سواد رسانه‌ای ← امنیت سایبری	۰/۶۳	۱۰/۱۵	۰/۰۰۰	معنادار

یافته‌های جدول ۷ بیانگر آن است که سواد رسانه‌ای تأثیر مستقیم و قوی بر امنیت سایبری دارد (β = ۰/۶۳). یعنی افرادی که از سواد رسانه‌ای بالاتری برخوردارند، امنیت سایبری بهتری دارند. امنیت سایبری بیشترین تأثیر را بر هویت دیجیتال دارد (β = ۰/۴۸)؛ یعنی رعایت اصول امنیتی تأثیر زیادی بر حفاظت از هویت دیجیتال کاربران دارد. سواد رسانه‌ای تأثیر مستقیمی بر هویت دیجیتال دارد (β = ۰/۳۶)، اما این تأثیر کمتر از تأثیر امنیت سایبری است.

همچنین، اثر غیرمستقیم سواد رسانه‌ای بر هویت دیجیتال از طریق امنیت سایبری مثبت و معنادار بود که نشان می‌دهد آموزش سواد رسانه‌ای می‌تواند امنیت سایبری را تقویت کرده و در نتیجه از هویت دیجیتال محافظت کند.

بررسی شاخص‌های برازش مدل SEM

برای ارزیابی میزان تطابق مدل با داده‌های پژوهش، از شاخص‌های برازش مدل استفاده شد.

جدول ۸. شاخص‌های برازش مدل تحلیل مسیر

شاخص	مقدار به‌دست‌آمده	مقدار مطلوب	نتیجه
شاخص برازش تطبیقی[1]	۰/۹۴	>۰/۹۰	مناسب
شاخص تاکر ـ لوئیس[2]	۰/۹۱	۰>/۹۰	مناسب
ریشهٔ میانگین مربعات خطای تقریب[3]	۰/۰۵۶	<۰/۰۸	مناسب
کای ـ دو بر درجه آزادی[4]	۲/۸۹	<۳/۰۰	مناسب

جدول ۸ نشان می‌دهد که تمامی شاخص‌های برازش مدل در محدودهٔ مقادیر مطلوب قرار

1. CFI
2. TLI
3. RMSEA
4. χ^2/df

دارند که از برازش مناسب مدل با داده‌ها حکایت می‌کند. مدل از برازش مناسبی برخوردار است و روابط بین متغیرها به‌درستی تبیین شده‌اند.

در مورد محدودیت‌های روش‌های آماری استفاده شده و چگونگی غلبه بر این محدودیت‌ها اقدامات زیر انجام شد:

- روش مدل‌سازی معادلات ساختاری (SEM) بیشتر به حجم نمونه بزرگی نیاز دارد تا نتایج آن پایدار و قابل تعمیم باشد. در پژوهش حاضر، حجم نمونه ۳۸۴ نفر بود که با استفاده از فرمول کوکران محاسبه شد. برای رفع این محدودیت از افزایش حجم نمونه با استفاده از نمونه‌گیری تصادفی طبقه‌ای به‌جای روش نمونه‌گیری در دسترس استفاده شد.
- روش SEM فرض می‌کند که توزیع داده‌ها نرمال است، اما در بسیاری از موارد داده‌های واقعی دارای چولگی و کشیدگی بالا هستند. نرمال نبودن داده‌ها می‌تواند باعث خطا در محاسبهٔ ضرایب مسیر و آزمون معناداری شود. برای رفع این محدودیت از بررسی نرمال بودن داده‌ها با استفاده از آزمون کولموگروف ـ اسمیرنوف استفاده شد.

مدل SEM باید شاخص‌های برازش RMSEA، TLI، CFI و df/χ^2 را برآورده کند. اگر مدل برازش مناسبی نداشته باشد، ممکن است از مشکلاتی مانند روابط نادرست بین متغیرها یا عدم کفایت شاخص‌های اندازه‌گیری حکایت کند. برای رفع این محدودیت، اصلاح مدل با حذف مسیرهای غیرمعنادار و افزودن مسیرهای مناسب براساس تحلیل اصلاحی انجام شد.

بحث و نتیجه‌گیری

پژوهش حاضر با هدف بررسی نقش سواد رسانه‌ای در امنیت سایبری و هویت دیجیتال در عصر هوش مصنوعی انجام شده است. در این مطالعه، روابط بین سواد رسانه‌ای، امنیت سایبری و هویت دیجیتال با استفاده از مدل‌سازی معادلات ساختاری و تحلیل مسیر مورد بررسی قرار گرفت. یافته‌های پژوهش نشان داد که:

- سواد رسانه‌ای تأثیر مستقیم و غیرمستقیم (از طریق امنیت سایبری) بر هویت دیجیتال دارد.
- امنیت سایبری بیشترین تأثیر را بر هویت دیجیتال دارد.
- زنان نسبت به مردان از سطح سواد رسانه‌ای بالاتری برخوردار هستند.

این نتایج تأکید می‌کند که سواد رسانه‌ای نه‌تنها یک مهارت کلیدی در دنیای دیجیتال است، بلکه نقش مهمی در حفاظت از هویت دیجیتال و امنیت کاربران ایفا می‌کند. استفاده از مدل‌سازی معادلات ساختاری و تحلیل مسیر در این پژوهش نشان داد که امنیت سایبری قوی‌ترین عامل در حفاظت از هویت دیجیتال است. همچنین استفاده از این روش‌ها به درک بهتر روابط بین

متغیرها کمک کرده و نشـان داده است که سواد رسانه‌ای به‌عنوان یک مهارت کلیدی، می‌تواند امنیت سایبری و هویت دیجیتال کاربران را تقویت کند. مدل از برازش خوبی برخوردار است و نتایج از لحاظ آماری معنادار هستند. افزایش سواد رسانه‌ای کاربران می‌تواند به بهبود امنیت سایبری و در نهایت تقویت هویت دیجیتال منجر شود.

تفسیر یافته‌ها براساس چارچوب نظری پژوهش

طبـق نظریهٔ تاجفل و ترنر، هویـت اجتماعی کاربران در فضای دیجیتـال تحت‌تأثیر تعاملات برخط آن‌ها قرار دارد. یافته‌های پژوهش نشان داد که امنیت سایبری نقش کلیدی در محافظت از این هویت دارد. در تبیین این یافته با استفاده از نظریهٔ هویت اجتماعی می‌توان گفت کاربران با سواد رسانه‌ای بالاتر، بهتر می‌توانند از هویت دیجیتال خود در برابر جعل هویت، فیشینگ و کلاهبرداری‌های برخط محافظت کنند.

بلک در نظریهٔ خودپندارهٔ دیجیتال مطرح می‌کند که کاربران هویت خود را از طریق محتوای دیجیتالی که به اشـتراک می‌گذارند، شـکل می‌دهند. یافته‌های پژوهش نیز تأیید کرد که کاربران با سـواد رسانه‌ای بالا، هویت دیجیتال خود را با آگاهی بیشتری مدیریت می‌کنند. در تبیین این یافته با اسـتفاده از نظریهٔ خودپندارهٔ دیجیتال می‌توان گفت که سواد رسانه‌ای از طریق افزایش آگاهی کاربران، به کاهش آسیب‌پذیری آن‌ها در برابر تهدیدات سایبری کمک می‌کند.

طبق نظریهٔ رفتار برنامه‌ریزی‌شـدهٔ آجزن، رفتارهـای کاربران در فضای مجازی تحت‌تأثیر نگرش‌ها، هنجارهای اجتماعی و کنترل رفتاری ادراک‌شـده اسـت. نتایج پژوهش نشان داد که افراد با سواد رسانه‌ای بالاتر، نگرش مثبت‌تری نسبت به رعایت امنیت سایبری دارند. در تبیین این یافته با اسـتفاده از این نظریه می‌توان گفت سـواد رسانه‌ای باعث افزایش آگاهی امنیتی و کاهش رفتارهای پرخطر در فضای مجازی می‌شود.

نظریـهٔ پردازش اطلاعـات دوگانه بیان می‌کند کـه کاربران از دو نوع پـردازش اطلاعات استفاده می‌کنند: پردازش سطحی (شهودی) و پردازش عمیق (تحلیلی). با استفاده از این نظریه در تحلیل یافته‌های پژوهش می‌توان گفت سـواد رسـانه‌ای کاربران را از پردازش سـطحی به سـمت پردازش عمیق هدایت می‌کند و باعث افزایش دقت آن‌ها در تشـخیص اخبار جعلی و تهدیدات سایبری می‌شود.

مقایسهٔ یافته‌ها با پژوهش‌های پیشین

یافته‌های این پژوهش هم‌سـو با مطالعات پیشـین است و بر اهمیت سواد رسانه‌ای در تقویت امنیت سایبری و حفاظت از هویت دیجیتال تأکید دارد:

یافته‌های این پژوهش نشـان می‌دهد که هوش مصنوعی مولد و الگوریتم‌های شخصی‌ساز

محتوا، نه‌تنها بر امنیت سایبری کاربران تأثیر می‌گذارند، بلکه به‌تدریج هویت دیجیتال آنان را نیز دستخوش تغییر می‌کنند. این یافته با نتایج پژوهش جعفری و فرج‌زاده (۱۴۰۳) همخوانی دارد که براساس تجربهٔ زیسته نوجوانان، شکاف میان دانش، نگرش و رفتار آنان نسبت به هویت ملی در رسانه‌های جمعی و اجتماعی را آشکار ساخته‌اند. به بیان دیگر، کاربران در عصر هوش مصنوعی، با تکثر منابع هویت‌بخش و پیام‌های متناقض مواجه هستند و آنچه ضرورت می‌یابد، نه‌فقط دسترسی به اطلاعات، بلکه توانایی تحلیل و ارزیابی انتقادی محتوا و آگاهی از سازوکارهای بازنمایی هویت در بسترهای گوناگون رسانه‌ای است؛ توانمندی‌ای که از آن به سواد رسانه‌ای تعبیر می‌شود.

یافته‌های این پژوهش با مطالعهٔ لیوینگستون و هلسپر (۲۰۰۷) هم‌سو است. نتایج این پژوهش نیز تأیید می‌کند که سواد رسانه‌ای به‌طور مستقیم بر امنیت سایبری تأثیر مثبت دارد و از این طریق، هویت دیجیتال کاربران را تقویت می‌کند. نتایج این پژوهش با یافته‌های چسنی و سیترون (۲۰۱۹) همخوانی دارد. این پژوهش نیز تأیید می‌کند که امنیت سایبری مهم‌ترین عامل تأثیرگذار بر هویت دیجیتال است. این پژوهش با مطالعهٔ نگوین و همکاران (۲۰۲۱) هم‌سو است. این پژوهش نیز تأکید می‌کند فناوری‌های مبتنی‌بر هوش مصنوعی می‌توانند هویت دیجیتال کاربران را تحت‌تأثیر قرار دهند و چالش‌های جدیدی در زمینهٔ امنیت سایبری ایجاد کنند.

یافته‌های این پژوهش نشان می‌دهد که امنیت سایبری و حفاظت از هویت دیجیتال، به هیچ وجه تنها با اقدامات فنی و دولتی تأمین نمی‌شود، بلکه نیازمند مشارکت فعال تمامی اقشار جامعه است. این یافته با الگوی ارائه‌شده توسط محمدی و دانایی (۱۴۰۱) همخوانی دارد که مجریان پدافند غیرعامل رسانه‌ای را به دو دسته "جمعی" (شامل دانشگاه‌ها، مطبوعات و مسئولان) و "فردی" (شامل والدین، معلمان و هر شهروند) تقسیم می‌کنند. در این میان، نقش والدین و معلمان در آموزش تفکر انتقادی و سواد رسانه‌ای به کودکان و نوجوانان به‌عنوان "اقدام‌های فردی" برجسته می‌شود.

نتیجه‌گیری نهایی

نتایج این پژوهش نشان داد که سواد رسانه‌ای به‌عنوان یک مهارت کلیدی، نقش مهمی در تقویت امنیت سایبری و حفاظت از هویت دیجیتال در عصر هوش مصنوعی ایفا می‌کند. هویت دیجیتال، امنیت سایبری و سواد رسانه‌ای سه مفهوم به‌هم‌پیوسته هستند که در عصر هوش مصنوعی اهمیت بیشتری یافته‌اند. هویت دیجیتال به‌عنوان یک دارایی ارزشمند نیازمند حفاظت است؛ امنیت سایبری ابزارهای این حفاظت را فراهم می‌آورد و سواد رسانه‌ای کاربران را توانمند می‌سازد تا از این ابزارها به‌طور مؤثر استفاده کنند. در کنار هم، این سه

مفهوم به ایجاد یک محیط دیجیتال امن و قابل‌اعتماد کمک می‌کنند.

با توجه به یافته‌های این پژوهش و نقش کلیدی سواد رسانه‌ای در تقویت امنیت سایبری و حفاظت از هویت دیجیتال، پیشنهادهای کاربردی زیر ارائه می‌شود:

- آموزش سواد رسانه‌ای در مدارس و دانشگاه‌ها (طراحی دوره‌های آموزشی برای دانش‌آموزان و دانشجویان با هدف افزایش آگاهی آن‌ها دربارهٔ تهدیدات سایبری).
- گنجاندن دوره‌های سواد دیجیتالی در برنامهٔ درسی مدارس و دانشگاه‌ها.
- برگزاری کارگاه‌ها و وبینارهای رایگان برای افزایش آگاهی عمومی دربارهٔ امنیت سایبری و هویت دیجیتال.
- توسعهٔ برنامه‌های هوش مصنوعی برای تشخیص تهدیدات دیجیتال مانند فیشینگ، کلاهبرداری‌های برخط و جعل هویت.
- استفاده از هوش مصنوعی برای تشخیص محتوای جعلی و اخبار نادرست در فضای مجازی.
- تشویق همکاری بین دانشگاه‌ها، شرکت‌های فناوری و سازمان‌های دولتی برای توسعهٔ راهکارهای امنیتی.
- اجرای کمپین‌های تبلیغاتی در رسانه‌های اجتماعی و تلویزیون برای افزایش آگاهی کاربران دربارهٔ تهدیدات سایبری و راه‌های مقابله با آن‌ها.

منابع

تندرو، کوروش؛ رمضانی، محمدهادی، تندرو، ابراهیم و تندرو، جلال (۱۴۰۲). بررسی اهمیت آموزش سواد رسانه‌ای و نقش آن در کاهش آسیب‌های فضای مجازی. سومین همایش ملی ایده‌های کاربردی در علوم تربیتی، روان‌شناسی و مطالعات فرهنگی. بوشهر.

جعفری، علی و فرجزاده، غلامعلی (۱۴۰۳). نقش رسانه‌های جمعی و اجتماعی در برساخت هویت ملی دانش‌آموزان دوره متوسطه: یک مطالعه پدیدارشناسی. رسانه، ۳۵(۱)، ۸۳-۱۰۲.

doi: 10.22034/bmsp.2023.343626.1806

خاکسار ازغندی، عبدالله (۱۳۹۸). بررسی رابطه بین سواد رسانه‌ای و قربانی سایبری. پژوهش در آموزش راهنمایی و مشاوره، ۵(۱۰)، ۹۱-۱۰۵. dor: 20.1001.1.2783154.1398.1398.10.5.4

رسولی، هاتف؛ والمحمدی، چنگیز، آزاد، ناصر و عباس‌پور اسفدن، قنبر (۱۴۰۰). ارائه چارچوب مدیریت هویت دیجیتال در فضای سایبر با رویکرد آمیخته. امنیت ملی، ۱۱(۴۰)، ۱۲۱-۱۵۴

dor: 20.1001.1.33292538.1400.11.40.5.1

عزیزی‌نیا، مریم و فیاض، راضیه (۱۴۰۲). نقش مؤثر سواد رسانه‌ای در امنیت فضای مجازی. اولین کنگره ملی فضای مجازی و گوشی‌های هوشمند؛ چالش‌ها و فرصت‌ها. تهران.

محمدی، علیرضا و دانایی، ابوالفضل (۱۴۰۱). تدوین الگوی مطلوب پدافند غیرعامل رسانه‌ای در ایران. رسانه، ۳۳(۴)، ۱۸۱ - ۲۰۲. doi:10.22034/bmsp.2021.289073.1553

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179-211. https://doi.org/10.1016/0749-5978(91)90020-T

Azizinia, M., & Fayyaz, R. (2023). The Effective Role of Media Literacy in Cyber Space Security. The First National Congress on Cyber Space and Smartphones: Challenges and Opportunities, Tehran. **[In persian]**

Belk, R. W. (2013). Extended self in a digital world. *Consumer Research*, 40(3), 477-500. https://doi.org/10.1086/671052

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U. D. (2017). The role of digital literacy in protecting online privacy. *Computers in Human Behavior*, 70, 243-250. https://doi.org/10.1016/j.chb.2016.12.067

Chaiken, S., & Trope, Y. (1999). *Dual-process theories in social psychology*. Guilford Press.

Chen, X., Sin, S. C. J., Theng, Y. L., & Lee, C. S. (2022). AI-powered misinformation and digital literacy. *Association for Information Science and Technology*, 73(5), 763-777. https://doi.org/10.1002/asi.24589

Chesney, R., & Citron, D. (2019). Deepfakes and the New Disinformation War: The Coming Age of Post-Truth Geopolitics. *Foreign Affairs*, 98(1), 147-155.

Guess, A., Nyhan, B., & Reifler, J. (2020). Exposure to misinformation and the adoption of digital security practices. *Cybersecurity*, 6(1), 1-10. https://doi.org/10.1093/cybsec/tyaa001

IBM Security (2022). Cost of a Data Breach Report 2022.

Jafari, A., & Farajzadeh, G. A. (2024). The role of mass and social media in constructing the national identity of secondary school students: A phenomenological study. *Rasaneh*, 35(1), 83-102. **[In persian]** doi: 10.22034/bmsp.2023.343626.1806.

Kahneman, D. (2011). Thinking, Fast and Slow. *Statistical Papers*, 55(3). DOI:10.1007/s00362-013-0533-y

Kellner, D., & Share, J. (2005). Toward critical media literacy: Core concepts, debates, organizations, and policy. Discourse: Studies in the Cultural Politics of Education, 26(3), 369-386. https://doi.org/10.1080/01596300500200169

Khaksar Azghandi, A. (2019). Investigating the Relationship between Media Literacy and Cyber Victimization. Research in Guidance and Counseling Education, 5(10), pp. 91-105. Dor: 20.1001.1.2783154.1398.1398.10.5.4 **[In persian]**

Lewandowsky, S., Ecker, U. K. H., & Cook, J. (2017). Beyond misinformation: Understanding and coping with the "post-truth" era. *Applied Research in Memory and Cognition*, 6(4), 353–369. https://doi.org/10.1016/j.jarmac.2017.07.008

Livingstone, S. (2018). Audiences in an age of datafication: Critical questions for media research. *Television & New Media*, 19(1), 15-25. DOI:10.1177/1527476418811118

Livingstone, S., & Helsper, E. J. (2007). Gradations in digital inclusion: Children, young people and the digital divide. *New Media & Society*, 9(4), 671-696. https://doi.org/10.1177/1461444807080335

McAfee (2020). The State of Deepfakes: A Threat to Trust and Security.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research*, 13(3), 334-359. https://doi.org/10.1287/isre.13.3.334.81

Mohammadi, A., & Danaei, A. (2022). Developing an optimal model of media passive defense in Iran .*Rasaneh*, 33(4), 181-202. **[In persian]** doi:10.22034/bmsp.2021.289073.1553

Nguyen, T. T., Hatua, A., & Sung, A. H. (2021). AI and cybersecurity: Threats and opportunities. *Cybersecurity and Privacy*, 1(2), 195-210. https://doi.org/10.3390/jcp1020012

NIST (2020). Cybersecurity Framework. National Institute of Standards and Technology.

OECD (2019). The Role of Digital Identity in the Digital Economy. OECD Publishing.

Rasouli, H., Valmohammadi, Ch., Azad, N., & Abbaspour Esfeden, Gh. (2021). Presenting a Digital Identity Management Framework in Cyber Space with a Mixed Approach. *National Security*, 11(40), 121-154. **[In persian]** Dor: 20.1001.1.33292538.1400.11.40.5.1

Rheingold, H. (2000). *The virtual community: Homesteading on the electronic frontier*. MIT press.

Tajfel, H., & Turner, J. C. (2004). *The Social Identity Theory of Intergroup Behavior*. In J. T. Jost & J. Sidanius (Eds.), *Political psychology: Key readings*, 276–293. Psychology Press. https://doi.org/10.4324/9780203505984-16.

Tondro, K., Ramezani, M., Tondro, E., & Tondro, J. (2023). Investigating the Importance of Media Literacy Education and Its Role in Reducing Cyber Space Harms. The Third National Conference on Applied Ideas in Educational Sciences, Psychology and Cultural Studies, Bushehr. **[In persian]**

Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. *Science*, 185(4157), 1124-1131. DOI: 10.1126/science.185.4157.1124

UNESCO (2021). *Media and Information Literacy: Reinforcing Human Rights and Countering Radicalization*. UNESCO Publishing.

Van Dijck, J. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society*, 12(2), 197-208. https://doi.org/10.24908/ss.v12i2.4776

Yoon, C. (2011). Theory of planned behavior and security awareness. *Computers in Human Behavior*, 27(1), 184-193. https://doi.org/10.1016/j.chb.2010.07.030

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.