

<http://doi.org/10.22133/mtlj.2025.444138.1301>

Criminal Law Challenged by Crossing into Virtual Reality

Mahdi Karimi 

Assistant Prof., Department of Law, Faculty of Law and Social Sciences, Payam Noor University, Tehran, Iran.

Article Info

Abstract

Original Article

Received:

16-02-2024

Accepted:

03-07-2024

Keywords:

Virtual Reality

Criminal Law

Virtual Emotions

Artificial Intelligence

Avatar

This article examines the risks of using virtual reality technology to achieve criminal law objectives. In the first step, by reviewing scientific studies to determine the nature of virtual reality, it has been identified as a non-invasive neural technology that has high-risk artificial intelligence. At the same time, it introduces it as a transformational neural technology that can alter what people perceive as reality. This capability is referred to as "realism" which represents the emotional immersion of the user in a virtual experience. The implications of this capacity reveal three key risks, which are: (1) the ability to collect extensive data stored during its use; (2) the ability of virtual reality to mentally recreate the "physical" avatar experience in the user; and (3) its considerable capacity for manipulating individuals. In the second step, this article examines potential criminal activities in virtual environments, focusing on violations of mental privacy and manipulation of users. Ultimately, it is suggested that criminal law should intervene to define the "red line" of extensive use of virtual reality by citizens and outline a legal framework for criminalizing associated harms and dangers. Therefore, formulating a comprehensive criminal policy and prevention encompassing laws tailored to the evolving technology is imperative.

*Corresponding author

e-mail: m.karimi342@pnu.ac.ir

How to Cite:

Karimi, M. (2025). Criminal Law Challenged by Crossing into Virtual Reality . *Modern Technologies Law*, 6(11), 277-298.

Published by University of Science and Culture <https://www.usc.ac.ir>

Online ISSN: 2783-3836

1. Introduction

In the last quarter of the 20th century, significant changes occurred in the social, political, and economic fabric of most countries, which became known as the 'Risk Society' (Beck, 2006, p: 102). These changes brought with them new risks associated with industrial advancement, technological progress, and globalization. Unlike the domains that traditional criminal law protected, such as individual rights and private property, these new risks could create damage on a global scale, were systematic, and system-based. The consequences of these risks were unpredictable and undefined, and their effects would manifest in the medium or long term.

While criminal law had not yet fully adapted to the complexities and challenges arising from rapid social, technological, and cultural transformations of society, the risk society was also evolving simultaneously under the influence of factors such as the digital revolution and remarkable advances in neuroscience and artificial intelligence.

This social revolution could challenge the function of criminal law and have fundamental impacts and consequences on it. Therefore, the necessity for implementing fundamental changes in criminal law was felt so that it could continue to fulfill its role in society.

New changes in the digital space highlighted the need for criminal law adaptation to these changes. This adaptation includes updating and modifying criminal laws and regulations to cover cyberspace crimes and address data, computer systems, and network systems that require legal protection, as well as encompassing new forms of cyber attacks or electronic hacking in the digital domain.

Furthermore, due to the borderless nature of the internet, cybercrimes have an extensive scope that necessitated the development and regulation of a transnational and cross-border framework to counter these behaviors and pursue and punish the aforementioned crimes at an international level. At another stage, in the transition to Web 3.0, another factor was added, meaning that in addition to the internet, the interactive factor - namely the capability of social networks for users to interact and communicate with each other - also intervened, which led to new forms of crimes in social media. These latter criminal behaviors are either committed through the use of social networks such as Facebook, Twitter, and Instagram or are facilitated by using them.

2. Methodology

It can be stated that virtual reality (VR) is an advanced human-computer interface where users, through various devices and connections to a computer or platform, can immerse themselves in three-dimensional virtual experiences. Displays and lenses are used for stereoscopic 3D vision; headphones are employed for auditory immersion, while haptic devices with vibrational signals such as gloves, vests, or full-body suits enhance the sense of touch.

Since virtual reality is designed and implemented based on the understanding and cognition of the human nervous system and brain, and can influence human emotional and affective states.

From a practical perspective, Immersive Virtual Reality (IVR) cannot be separated from Artificial Intelligence (AI). From a technical standpoint, IVR is the result of an inseparable connection between non-invasive neural technology, such as head-mounted displays (HMDs), and a suite of AI systems related to voice recognition, language processing, visual pattern analysis, facial expressions, emotions, and physical interactions for avatar control and environmental interaction.

Users can experience virtual environments through 2D displays such as computer monitors, televisions, smartphones, and tablets, viewing events from their perspective. In this mode, they remain connected to their surrounding physical reality. Alternatively, using head-mounted displays (HMDs) with integrated screens and

headphones, including glasses or helmets with embedded displays and audio systems, they can completely detach from their physical environment and become fully immersed in the virtual environment. Another characteristic of virtual reality is user-avatar embodiment. Embodiment means creating a sensation in the user as if the avatar is their virtual body, achieved through synchronizing avatar movements with the user's real physical movements. Through this embodiment, the user experiences presence within the avatar's body and perceives and experiences the surrounding world through the avatar's eyes.

3. Results and Discussion

In the criminal law domain, an analysis has been conducted examining the potential challenges and risks that the expansion of virtual reality technology may pose to individuals' privacy, security, and psychological well-being. This analysis has identified three specific risks associated with the increasing prevalence of virtual reality technologies and their growing applications in people's daily lives, particularly commercial virtual reality operated by private companies for profit and economic return. The three main risk areas are as follows:

1. Due to its interactive and immersive nature virtual reality can collect and record large volumes of users' personal and sensitive information during use. This information includes behavioral patterns, interests, preferences, biometric and physiological data such as heart rate, body energy consumption, etc., which are comprehensively collected to create a complete and accurate user profile, potentially resulting in severe violations of users' mental privacy.

2. Generally, an avatar refers to a digital and virtual representation of a user in the virtual reality environment. VR is designed and developed in such a way that users can have real-world-like interactions and experiences through their avatars in the virtual environment, enabling the simulation of physical experiences for the user's avatar in the virtual space.

3. Virtual reality, due to creating a highly immersive and interactive environment, significantly enables the manipulation of users' behavior, beliefs, emotions, and decision-making. This potential indicates the risk of exploitation and control of individuals by virtual reality environment operators and designers." It should be noted that* the current criminal policy approach requires re-evaluation and reassessment in line with the current advancement of neural technologies and artificial intelligence to effectively monitor and address the challenges and consequences arising from the development of these technologies. The evolving landscape of neural technologies and AI necessitates a more precise and informed criminal policy approach for controlling criminal behaviors. Neural technologies with the potential for unauthorized direct access to individuals' brain activity, whether invasive or non-invasive, regardless of duration, should be explicitly criminalized by criminal law to preserve individuals' mental integrity. Accordingly, altering brain activity without user-victim consent (brain hacking) should be explicitly defined as a criminal offense as technology has reached a level of development that makes such direct intervention possible. Immersive virtual reality is a non-invasive, indirect, and less effective technology. Non-invasive means the technology doesn't physically enter or alter the user's body. Virtual reality provides an indirect experience of reality as users interact with a simulated environment rather than the real world. The term 'less effective' indicates that virtual reality may not fully replicate real-world experiences. These characteristics make evaluating content or behavior in immersive virtual reality more challenging compared to real-world assessments. The most significant challenge criminal law faces in evaluating content or behavior in immersive virtual reality concerns the effectiveness of user manipulation.

4. Conclusion

This article has evaluated the potential of virtual environments in the formation of predictable crimes and focused on three crime-prone areas including mental privacy violation, emotional harm, and manipulation of users' ideas, thoughts, and decisions. Finally, it suggests that criminal law must swiftly define the 'red lines' of citizens' widespread use of virtual reality with a human-centered approach .

To achieve this goal, a legal framework has been designed for criminalizing specific risks associated with immersive virtual reality. Regarding user privacy, we have proposed that users' mental information beyond neural data should be protected to the same extent as other human body parts, including:





حقوق فناوری های نوین

<http://doi.org/10.22133/mtlj.2025.444138.1301>

حقوق کیفری در چالش عبور از واقعیت مجازی

مهدی کریمی^{۱۵}

استادیار، گروه حقوق، دانشکده حقوق و علوم اجتماعی، دانشگاه پیام نور، تهران، ایران.

اطلاعات مقاله	چکیده
مقاله پژوهشی تاریخ دریافت: ۱۴۰۲/۱۱/۲۷ تاریخ پذیرش: ۱۴۰۳/۰۴/۱۳ واژگان کلیدی: واقعیت مجازی، حقوق کیفری، احساسات مجازی، هوش مصنوعی، آواتار *نویسنده مسئول رایانامه: m.karimi342@pnu.ac.ir نحوه استناددهی: کریمی، مهدی (۱۴۰۴). حقوق کیفری در چالش عبور از واقعیت مجازی. حقوق فناوری های نوین، ۶(۱۱)، ۲۷۷-۲۹۸. ناشر: دانشگاه علم و فرهنگ https://www.usc.ac.ir شاپای الکترونیکی: ۲۷۸۳-۳۸۳۶	این مقاله در مقام بررسی خطرات استفاده از فناوری واقعیت مجازی به منظور دستیابی به اهداف حقوق کیفری است. در گام نخست با بررسی مطالعات علمی برای تعیین ماهیت واقعیت مجازی آن را یک فناوری عصبی غیرتهاجمی شناسایی کرده است که واجد هوش مصنوعی با ریسک بالاست. در عین حال، آن را یک فناوری عصبی تغییردهنده معرفی می کند که امکان تغییر آنچه مردم آن را به منزله واقعیت درک می کنند دارد. از این امکان تحت عنوان «واقع گرایی» یاد می شود که بیانگر غوطه ور شدن احساسی کاربر در یک تجربه مجازی است. نتایج این ظرفیت سه خطر کلیدی را آشکار می کند که عبارت اند از: ۱) قابلیت جمع آوری داده های گسترده و ذخیره شده در طول استفاده از آن؛ ۲) توانایی واقعیت مجازی برای بازتولید ذهنی تجربه «فیزیکی» آواتار در کاربر؛ ۳) ظرفیت درخور توجه آن برای دست کاری افراد. در گام دوم این مقاله فعالیت های مجرمانه بالقوه را در محیط های مجازی با تمرکز بر نقض حریم خصوصی ذهنی و دست کاری کاربران بررسی کرده و در نهایت پیشنهاد می شود که حقوق کیفری باید برای تعریف «خط قرمز» استفاده وسیع از واقعیت مجازی توسط شهروندان مداخله کند و یک چهارچوب قانونی برای جرم انگاری آسیب ها و خطرات مرتبط با آن ترسیم کند؛ بنابراین تدوین یک سیاست کیفری جامع و مانع که متضمن قوانین کیفری متناسب با فناوری در حال تحول مذکور است ضروری به نظر می رسد.

مقدمه

در عصر حاضر، فناوری واقعیت مجازی به منزله یکی از پیشرفته‌ترین دستاوردهای علم و فناوری، در حال تغییر شیوه تعامل انسان با محیط پیرامون است. این فناوری با ایجاد تجربیات شبیه‌سازی‌شده و غوطه‌ورکننده، مرزهای بین دنیای فیزیکی و مجازی را کمرنگ کرده است. پیشرفت‌های سریع در حوزه فناوری‌های نوین، چالش‌های جدیدی را برای نظام حقوقی به همراه آورده است. یکی از این فناوری‌های نوظهور که توجه زیادی را به خود جلب کرده، واقعیت مجازی است. اگرچه این فناوری پتانسیل‌های فراوانی برای پیشرفت در زمینه‌های مختلف دارد، اما استفاده از آن می‌تواند خطرات و چالش‌های جدی را به‌ویژه در حوزه حقوق کیفری به همراه داشته باشد.

مسئله اصلی این پژوهش، بررسی و تحلیل خطرات بالقوه استفاده از فناوری واقعیت مجازی در ارتباط با اهداف حقوق کیفری است. این فناوری با قابلیت‌های منحصر به فرد خود، از جمله جمع‌آوری گسترده داده‌ها، بازتولید ذهنی تجربیات فیزیکی و ظرفیت دست‌کاری افراد، چالش‌های جدی را برای نظام حقوقی ایجاد کرده است؛ بنابراین، با توجه به ماهیت پیچیده و نوآورانه این فناوری، ضروری است که نظام حقوقی برای مقابله با چالش‌های احتمالی آن آماده باشد.

اهمیت این پژوهش در شناسایی و پیش‌بینی خطرات احتمالی ناشی از استفاده گسترده از واقعیت مجازی است. با توجه به ماهیت نوظهور این فناوری و تأثیر عمیق آن بر تجربیات انسانی، ضروری است که نظام حقوقی برای مواجهه با چالش‌های آتی، آمادگی لازم را کسب کند. این امر به‌ویژه در حوزه حقوق کیفری اهمیت می‌یابد؛ زیرا می‌تواند از بروز جرائم جدید پیشگیری کرده و حقوق شهروندان را در فضای مجازی حفظ کند.

سؤال اصلی این پژوهش این است که چگونه می‌توان خطرات استفاده از فناوری واقعیت مجازی را در چارچوب حقوق کیفری شناسایی و پیش‌بینی و مدیریت کرد؟

اما سؤالات فرعی دیگری نیز مطرح می‌شود:

خطرات اصلی استفاده از فناوری واقعیت مجازی در ارتباط با اهداف حقوق کیفری کدام‌اند؟

چه نوع فعالیت‌های مجرمانه بالقوه‌ای ممکن است در محیط‌های مجازی رخ دهد؟

فرضیه اصلی این پژوهش بر این اساس استوار است که استفاده گسترده از فناوری واقعیت مجازی، ضمن ایجاد فرصت‌های نوین، به ظهور اشکال جدیدی از جرائم و تهدیدات علیه حقوق فردی و اجتماعی منجر شود؛ بنابراین نظام حقوق کیفری نیازمند بازنگری و تدوین چهارچوب‌های قانونی جدید برای مقابله با این چالش‌هاست.

۱. دگرگونی جرم و جنایت در عصر دیجیتال

در ربع آخر قرن بیستم، تغییرات مهمی در بافت اجتماعی، سیاسی و اقتصادی جدید آنچه «جامعه ریسک»^۱ نام گرفت (Beck, 2006, p. 102). در غالب کشورها صورت پذیرفت. این تغییرات با خود خطرات جدیدی مرتبط با پیشرفت صنعتی، فناوری و جهانی‌شدن را به همراه داشت. خطرات جدید، برخلاف حوزه‌ای که حقوق کیفری سنتی مثل حقوق فردی و مالکیت خصوصی از آن حمایت می‌کرد، دارای توانایی ایجاد آسیب در سطح جهانی نظام‌مند و مبتنی بر یک سیستم بود. نتایج این خطرات پیش‌بینی‌پذیر و مشخص نبودند و عواقب آن‌ها در میانه یا بلندمدت ظاهر می‌شد. همچنین معمولاً ناشی از ترکیب تعداد زیادی اعمال و کنش‌های افرادی بود که به‌صورت هماهنگ و با برنامه قبلی عمل نمی‌کردند (Mythen, 2014, p. 43).

در این راستا، حقوق کیفری در دوران مدرن دامنۀ حمایت خود را فراتر از حقوق فردی به منافع و اجتماعی مانند محیط زیست، سلامت عمومی، امنیت ملی، نظم اقتصادی و غیره نیز گسترش داد. همچنین دخالت خود را بر پیشگیری از آسیب قبل از وقوع آن متمرکز

1. Risk society

کرد (Silva Sanchez, 2001, p. 65). در حالی که حقوق کیفری هنوز کاملاً با پیچیدگی‌ها و چالش‌های ناشی از تحولات سریع اجتماعی، فناوریانه و فرهنگی جامعه وفق پیدا نکرده بود، جامعه ریسک به سرعت تحت تأثیر عواملی مانند انقلاب دیجیتال، پیشرفت شگفت‌آور در علوم اعصاب و هوش مصنوعی تغییر می‌کرد (Ghasemi, 2009, p. 34).

این انقلاب اجتماعی می‌توانست کارکرد حقوق کیفری را به چالش بکشد و تأثیرات و پیامدهای بنیادین در آن بگذارد؛ مانند عدم نظارت حقوق کیفری بر نقض حریم خصوصی ذهنی، آسیب عاطفی و دست‌کاری ایده، افکار و تصمیم‌گیری‌های کاربران؛ بنابراین، ضرورت اعمال تغییرات اساسی در حقوق کیفری احساس شد تا بتواند همچنان نقش خود را در جامعه ایفا کند. برای بررسی سیر تحول جرم در فضای دیجیتال، وب ۲/۰ را مانند الگویی فرضی در نظر می‌گیریم که علاوه بر دسترسی به هرگونه داده‌ای که توسط کاربران در اینترنت به اشتراک گذاشته می‌شود - مانند متن، عکس، فیلم، صوت و غیره (وب ۱/۰) - به یک پلتفرم پویا، مشارکتی و اجتماعی تکامل یافت که در آن کاربران می‌توانند با یکدیگر تعامل و محتوا ایجاد کنند. این محیط دیجیتال شامل وبلاگ‌ها، ویکی‌ها، شبکه‌های اجتماعی، سرویس‌های فایل، سرویس‌های پرداخت آنلاین و انواع مختلف خدمات آنلاین است.

در عصر وب ۲/۰، در ابتدا آنچه به منزله جرایم سایبری شناخته می‌شد، وفق تعریف توسط کنوانسیون بوداپست (Council of Europe, 2001) شامل رفتارهای مجرمانه‌ای است که با استفاده از سیستم‌های رایانه‌ای و فناوری اطلاعات و ارتباطات ارتکاب می‌یابند. تغییرات جدید در فضای دیجیتال، نیاز به انطباق حقوق کیفری با این تغییرات را برجسته‌تر کرد. این انطباق شامل به‌روزرکردن و اصلاح قوانین و مقررات کیفری برای پوشش دادن جرایم در فضای مجازی و رسیدگی به داده‌ها، سیستم‌های رایانه‌ای و شبکه‌ای است که نیازمند حمایت قانونی بودند و همچنین شامل اشکال جدید حملات سایبری یا هک کردن به صورت الکترونیکی در زمینه دیجیتال است. رفتارهای مجرمانه فوق حقوق قانونی موجود (مانند حریم خصوصی یا اموال) را تهدید می‌کرد. علاوه بر این، جرایم سایبری به دلیل ماهیت بدون مرز اینترنت، دامنه گسترده‌ای دارند که توسعه و تنظیم یک برنامه و چارچوب فراملی و فرامرزی برای مقابله با این رفتارها و پیگیری و مجازات جرایم مذکور در سطح بین‌المللی را ضروری می‌نمود. در مرحله دیگر و در گذار به وب ۳/۰، عامل دیگری نیز اضافه شد؛ به این معنا که علاوه بر اینترنت، عامل تعاملی، یعنی قابلیت شبکه‌های اجتماعی برای اینکه کاربران بتوانند با یکدیگر در تعامل و گفت‌وگو باشند نیز مداخله کرد که به اشکال جدیدی از جرائم در رسانه‌های اجتماعی منجر شد. رفتارهای مجرمانه اخیرالذکر یا از طریق استفاده از شبکه‌های اجتماعی مانند فیس‌بوک، توئیتر، اینستاگرام ارتکاب می‌یابند یا با استفاده از آن‌ها تسهیل می‌شوند (Hasanzadeh & Hosseini, 2010, p. 39). برای مثال، شبکه‌های اجتماعی نه تنها حریم خصوصی کاربران را با چالش‌هایی مواجه کرد، بلکه پتانسیل مخرب حملات به اطلاعات شخصی، عکس‌ها، ویدیوها و دیگر داده‌های خصوصی افراد در فضای مجازی را تقویت کردند. این امر به دلیل ظرفیت این شبکه‌ها برای انتشار گسترده و فوری محتوای که می‌تواند در مدت کوتاهی به مخاطبان زیادی برسد و همچنین امکان تعامل عمومی میان کاربران را چند برابر کرده است.

گسترش شبکه‌های اجتماعی به گسترش جرایم مرتبط با آزادی بیان از طریق رسانه‌های دیداری - شنیداری منجر شده است مانند آزار و اذیت سایبری، سخنان نفرت‌انگیز، توهین عمومی افراد؛ چراکه افراد ممکن است به دلیل ترس از چنین جرائمی در فضای شبکه‌های اجتماعی از ابراز آزادانه عقاید و بیان خود منصرف شوند؛ البته باید تصریح کرد الزاماً آزار و اذیت سایبری مرتبط با آزادی بیان نیست. علاوه بر این مشکل خاص دیگری برای حقوق کیفری وجود دارد و آن مسئولیت جمعی کاربرانی است که بدون هماهنگی و برنامه‌ریزی قبلی اقدام به باز نشر مطالب غیرقانونی می‌کنند یا درباره آن نظر می‌دهند و در نتیجه آسیب ناشی از جرم را تشدید می‌کنند. در این مرحله محیط دیجیتال به وب ۳/۰ تکامل یافت. در وب ۳/۰ قابلیت‌های پیشرفته‌تری همچون هوش مصنوعی و واقعیت افزوده گنجانده شده است که می‌توان آن را نتیجه ادغام هوش مصنوعی و آنچه به عنوان «وب معناگرا»^۱ شناخته می‌شود در محیط دیجیتال دانست که هر دو از طریق هم‌سویی انقلاب فناوری‌های عصبی انجام

۱. Semantic Web. وب معناگرا (معنایی) به معنای افزودن لایه‌ای از اطلاعات به وب است که به صفحات وب معنا و مفهوم می‌دهد تا توسط ماشین‌ها و نرم‌افزارها قابل فهم باشد.

شده است. به عبارت دیگر، هم‌سویی فناوری‌های مرتبط با مغز و اعصاب مانند هوش مصنوعی، یادگیری ماشینی و شبکه‌های عصبی به پیشرفت سریع این حوزه منجر شده است (Savage, 2019, p. 15).

در این محیط هوش مصنوعی متقاعدکننده، که برای تغییر رفتار انسان طراحی شده است، نقش محوری را همراه با واقعیت گسترده برعهده دارد که خود شامل واقعیت مجازی افزوده یا ترکیبی است (Mann et al., 2018, p. 67).
درمورد فنون هوش مصنوعی، تکامل از یادگیری ماشینی^۱ به یادگیری عمیق^۲ پیش رفته است که برپایه الگوریتم‌هایی استوار است و عملکرد شبکه‌های عصبی پیچیده را شبیه‌سازی می‌کنند.

به‌منظور تجزیه و تحلیل پیامدهای حقوقی یادگیری عمیق و این‌که چه تأثیراتی در حقوق کیفری خواهد داشت تکامل گفته‌شده براساس مبانی زیر عمل می‌کند: (۱) ظرفیت محاسباتی فوق‌العاده که مدیریت و پردازش و تجزیه و تحلیل حجم وسیعی از داده‌ها را ممکن می‌سازد؛ (۲) توانایی پیش‌بینی فوق‌العاده از طریق شناسایی الگوهای متعدد در داده‌ها و تدوین پیش‌بینی‌های مبتنی بر آن‌ها و ذخیره اطلاعات تولیدشده؛ (۳) ظرفیت عملیاتی بی‌نظیر که اجرای وسیع و توانایی پردازش حجم زیادی از داده‌های کاربران به‌صورت هم‌زمان و اقدامات شخصی‌سازی‌شده را ممکن می‌سازد؛ مانند ارائه تبلیغات به مصرف‌کنندگان براساس دانش کسب‌شده درمورد ترجیحات، ارزش‌ها، شرایط و نیازهای آن‌ها (Hermann, 2022, p. 68). برای انجام این وظایف، هوش مصنوعی به الگوریتم‌های پیشرفته‌ای متکی است که از طریق انبوهی از داده‌ها تغذیه می‌شوند. هوش مصنوعی برای حل مسائل پیچیده‌تر یا تصمیم‌گیری درمورد موضوعاتی که دارای متغیرهای مختلف هستند نیاز به داده‌های بیشتر و به‌روزتر دارد. برای مثال اگر قرار باشد هوش مصنوعی یک راهبرد سرمایه‌گذاری پیشنهاد دهد با پیچیده‌تر شدن بازارهای مالی نیاز دارد داده‌های به‌روزتر و جزئی‌تری از عوامل مختلف مؤثر در بازار در اختیار داشته باشد تا بتواند پیش‌بینی و تصمیم‌گیری دقیق‌تری انجام دهد. روشن می‌شود که مواد خام اقتصاد مبتنی بر فناوری‌ها و خدمات اینترنتی وب ۳/۰ «داده‌ها» هستند حجم بسیار زیادی از داده‌های نیمه‌پردازش‌شده که این داده‌ها باید به‌عنوان ورودی به سیستم‌های هوش مصنوعی داده شوند تا بتوانند از آن‌ها یاد بگیرند و الگوها را تشخیص دهند (Hakimpoor, 2023, p. 52). بدین دلیل اصطلاح معروف سرمایه‌داری نظارتی^۳ یعنی سرمایه‌داری که در آن داده‌ها و اطلاعات به‌منزله یک سرمایه و منبع ارزشمند محسوب می‌شوند ظهور یافته است (Zuboff, 2019, p. 85). این مدل جدید سرمایه‌داری است که در آن شرکت‌ها از طریق نظارت و ردیابی رفتار مصرف‌کنندگان اطلاعات و داده‌های زیادی درباره آن‌ها جمع‌آوری می‌کنند و از این اطلاعات به‌عنوان یک منبع سوددهی استفاده می‌کنند.

انقلاب هوش مصنوعی با انقلاب «زیست‌شناسی عصبی»^۴ در حال نزدیک شدن و ترکیب شدن با یکدیگر هستند. یعنی دستاوردها و پیشرفت‌های این دو حوزه در حال هم‌افزایی و تقویت کردن یکدیگر است. انقلاب زیست‌شناسی عصبی به پیشرفت‌های اخیر در درک سیستم عصبی و مغز انسان با استفاده از فناوری‌های نوین مانند تصویربرداری مغز رسیده است.

در این زمینه، برخی محققان از عبارت «خواندن و نوشتن» مغز ما برای توصیف رابطه متقابل بین هوش مصنوعی و علوم اعصاب استفاده می‌کنند (Goering et al., 2021, p. 53). اصطلاح «خواندن» به فرایند درک فعالیت و ساختار مغز اشاره دارد که هدف اساسی علم اعصاب است. همچنین «نوشتن» به توانایی دست‌کاری و تأثیرگذاری در فعالیت مغز اشاره دارد که یکی از جنبه‌های کلیدی هوش مصنوعی است. این ارتباط دوسویه زمانی کامل می‌شود که دسترسی فنی به خصوصی‌ترین اطلاعات انسان‌ها و تغییر افکار و احساسات و تصمیم‌گیری‌های یک فرد با استفاده از فناوری‌های عصبی امکان‌پذیر شود.

۱. Machine Learning: در یادگیری ماشینی، الگوریتم‌ها از داده‌های آموزشی برای یادگیری الگوها و انجام پیش‌بینی‌ها استفاده می‌کنند. در این روش، ویژگی‌های مهم داده‌ها به‌صورت دستی به‌دست متخصصان استخراج می‌شود.

۲. Deep Learning: در یادگیری عمیق، الگوریتم‌ها از شبکه‌های عصبی با لایه‌های مختلف استفاده می‌کنند تا بتوانند ویژگی‌های مهم داده‌ها را به‌صورت خودکار استخراج کنند. در این روش، الگوریتم‌ها می‌توانند الگوهای پیچیده‌تری را در داده‌ها تشخیص دهند.

3. Surveillance Capitalism

4. Neurobiology

براین اساس، می‌توان گفت که برای اهداف حقوق کیفری مانند بازدارندگی، اصلاح مجرمان، جبران خسارت و حفظ نظم عمومی جامعه، ادغام و ترکیب هوش مصنوعی و زیست‌شناسی عصبی عنصر مهمی است؛ زیرا محیط‌های دیجیتال قبلی عمدتاً به صورت غیرمستقیم بر روی رفتار و تصمیم‌گیری انسان‌ها اثر می‌گذاشتند، اما فناوری جدید مبتنی بر همسویی هوش مصنوعی و زیست‌شناسی عصبی، از طریق دست‌کاری مستقیم مغز و ذهن قادر به تأثیرگذاری در رفتار انسان خواهد بود (Tishehyar & Pazookizadeh, 2010, p. 116).

همین عامل است که باعث پدید آمدن دسته جدیدی از خطرات عمیق، گسترده و بنیادی شده است که کل سیستم و جامعه انسانی را تحت تأثیر قرار می‌دهند. این خطرات از دو امر ناشی می‌شوند: نخست از امکان تغییر ماهیت انسان از طریق فناوری‌های غیرتهاجمی عصبی («مداخلات عصبی») و به کارگیری وسایلی که برای اتصال به بدن و دستگاه عصبی انسان، به صورت دائم یا موقت، جاسازی می‌شوند و دوم ناشی از امکان دست‌کاری حالات ذهنی انسان‌ها که شامل افکار، احساسات، خاطرات و حتی تمایلات رفتاری و تصمیم‌گیری آن‌هاست.

۲. واقعیت مجازی فراگیر به منزله یک فناوری عصبی الفاکنده احساسات

واقعیت مجازی یک رابط کاربری پیشرفته انسان- رایانه است که کاربران با استفاده از دستگاه‌ها و اتصالات مختلف به یک رایانه یا پلتفرم قادرند خود را در تجربه‌های مجازی سه بعدی غوطه‌ور کنند. از صفحه‌نمایش‌ها و عدسی‌ها برای دید سه بعدی «استریوسکوپیک»^۲ استفاده می‌شود. هدفون‌ها برای غوطه‌وری شنیداری به کار گرفته می‌شوند. درحالی‌که دستگاه‌های لمسی با سیگنال‌های لرزشی مانند دستکش‌ها، وست‌ها یا لباس‌های تمام بدن، حس لامسه را افزایش می‌دهند. این اجزا با هم کار می‌کنند تا برای کاربر توهم حضور درون، حضور در لحظه و تعامل حیط مجازی سه بعدی، در زمان واقعی و از طریق یک آواتار ایجاد کنند (Heidari & Jafari, 2010, p. 106).

محیط واقعیت مجازی محیطی کاملاً مجازی، دیجیتال و مصنوعی است که از طریق رایانه ایجاد شده در نتیجه سیستم‌های واقعیت مجازی بیشتر روی غوطه‌وری شنیداری- بصری متمرکز بوده‌اند که به منزله یک معیار اساسی برای غوطه‌وری در این مقاله مدنظر قرار گرفته است (Huynh The et al., 2022, p. 94). چون واقعیت مجازی براساس درک و شناخت سیستم عصبی و مغز انسان طراحی و پیاده‌سازی می‌شود و می‌تواند بر حالات عاطفی و هیجانی انسان تأثیر بگذارد اولین سؤالی که مطرح می‌شود این است که آیا واقعیت مجازی می‌تواند یک نوع فناوری عصبی، که بر پایه دانش و عملکرد سیستم عصبی انسان طراحی و ساخته می‌شوند، در نظر گرفته شود یا خیر؟ پاسخ به این سؤال با بحث بین‌المللی در مورد حقوق عصبی ارتباط مستقیمی دارد. اگر واقعیت مجازی جزو فناوری‌های عصبی طبقه‌بندی نشود از حمایت‌های حقوقی ویژه‌ای که برای فناوری‌های عصبی در نظر گرفته می‌شود برخوردار نخواهد بود و تحت پوشش چهارچوب‌ها و مقررات بین‌المللی حقوق عصبی قرار نمی‌گیرد. از منظر فنی و تخصصی فناوری عصبی را این گونه تعریف کرده‌اند: فناوری عصبی به فناوری‌ای گفته می‌شود که با فعالیت مغز یا ساختار آناتومیک مغز را اندازه‌گیری کند (برای مثال از طریق تصویربرداری MRI^۳ یا ثبت امواج مغزی EEG)^۴ تا بتواند در فعالیت مغز تداخل ایجاد کند و آن را تحت تأثیر قرار دهد (مانند رابط مغز- رایانه یا تحریک الکتریکی مغز) (Ligthart et al., 2023, p. 94).

با توجه به این رویکرد باید نتیجه گرفت که واقعیت مجازی یک فناوری عصبی نیست؛ زیرا از دستگاه‌های طراحی شده اختصاصی مثل دستگاه ثبت امواج مغزی یا تحریک مغزی عمیق برای خواندن یا تغییر فعالیت مغزی استفاده نمی‌کند. با این حال اگر به جای تمرکز بر ساختار واقعیت مجازی (به این معنا که آیا از دستگاه‌های خاص خواندن یا تغییر فعالیت مغز استفاده می‌کند یا خیر) بر روی عملکرد آن متمرکز شویم (یعنی این که واقعیت مجازی چه کارهایی انجام می‌دهد) دیگر پاسخ به این سؤال آن قدرها ساده و یک‌سویه نخواهد بود و پاسخ آن نیاز به بررسی بیشتر دارد؛ زیرا اگر بر عملکرد تمرکز کنیم واقعیت مجازی قابلیت خواندن فعالیت ذهنی از طریق داده‌ها و تأثیرگذاری مستقیم بر فعالیت‌های ذهنی مثل القای احساسات و خاطرات را دارد. به عبارت روشن‌تر، واقعیت مجازی قادر است با استفاده از ترکیب و تحلیل داده‌های

1. Neurointerventions
2. Stereoscopic
3. Magnetic Resonance Imaging
4. Electroencephalograph

جمع‌آوری شده از کاربر (مثل الگوهای حرکتی و ضربان قلب) فعالیت‌ها و حالات ذهنی او را تاحدی بخواند و درک کند. علاوه بر این واقعیت مجازی می‌تواند مستقیماً نیز در فعالیت‌های ذهنی کاربر تأثیر بگذارد؛ برای مثال با القا و برانگیختن احساسات و عواطف خاصی در کاربر یا از طریق فعال کردن حافظه فضایی او مسیرها را به یاد بیاورد نقشه‌ها را در ذهن مجسم کند و فاصله و جهت اشیا نسبت به یکدیگر را تخمین بزند. از این منظر، همان‌طور که وینسنت پیشنهاد داده است، واقعیت مجازی را می‌توان یک فناوری عصبی در نظر گرفت؛ زیرا توانایی مستقیمی برای تأثیرگذاری در فعالیت مغز دارد (Vincent et al., 2020, p. 11).

البته با این حال واقعیت مجازی یک فناوری غیرتهاجمی عصبی است که بدون نیاز به مداخله فیزیکی یا جراحی در بافت مغز روی فعالیت مغز تأثیر می‌گذارد یا آن را می‌خواند؛ مانند الکتروانسفالوگرام^۱ و به نسبت فناوری‌های عصبی اختصاصی که مستقیماً و تهاجمی با مداخله در بافت مغز فعالیت مغز را تحت تأثیر قرار می‌دهند یا می‌خوانند؛ مانند تحریک عمقی مغز کارآیی کمتری دارد (شهریاری، ۱۳۹۰، ص ۵). از لحاظ کاربردی واقعیت مجازی فراگیر را از هوش مصنوعی نمی‌توان جدا کرد. به لحاظ فنی، واقعیت مجازی فراگیر نتیجه اتصال ناگسستگی فناوری عصبی غیرمداخله‌ای (مانند نمایشگرهایی که به سر افراد بسته می‌شود)^۲ و مجموعه‌ای از سامانه‌های هوش مصنوعی مرتبط با شناسایی صدا، پردازش زبان، تجزیه و تحلیل الگوهای بصری، ابرازهای چهره‌ای، احساسات و تعاملات فیزیکی برای کنترل آواتار و تعامل با محیط است.

فناوری‌های کلیدی که به تجربه غوطه‌وری و ادغام کاربر با محیط مجازی و آواتار در واقعیت مجازی کمک می‌کنند شامل فناوری‌های رابط انسانی (مانند دستگاه‌های تلفن همراه، ساعت‌های هوشمند، عینک‌های هوشمند، دستگاه‌های پوشیدنی، نمایشگرهای سربسته، شناسایی گفتار و بسته‌های الکترونی) و فناوری‌های محاسبات فضایی (مانند موتورهای سه‌بعدی، نقشه‌برداری جغرافیایی) می‌شوند (Huynh-The et al., 2022, p. 98). از طریق ترکیب این فناوری‌ها، مغز کاربر احساس می‌کند که درون یک واقعیت جایگزین قرار گرفته و آن را مستقیم تجربه می‌کند؛ درحالی‌که میزان غوطه‌وری و حضور توسط دستگاه‌های استفاده‌شده تسهیل می‌شود. در واقعیت مجازی فراگیر، انواع فناوری‌های عصبی غیرتهاجمی با سایر فناوری‌ها و هوش مصنوعی ترکیب می‌شوند تا در ابتدا محیطی غوطه‌ور برای کاربر ایجاد کنند. در واقع، محیطی ایجاد می‌شود که به کاربر اجازه می‌دهد با احساس بالایی از واقع‌گرایی کاملاً در آن غوطه‌ور شود. محیط مجازی آن‌قدر قانع‌کننده و واقعی است که کاربر کاملاً جذب و درگیر آن می‌شود (Slater, 2009, p. 78).

کاربران می‌توانند محیط‌های مجازی را از طریق صفحه‌نمایش‌های دوبعدی مانند مونیتر رایانه، تلویزیون، گوشی و تبلت، که تصاویر را به صورت دوبعدی و صاف نشان می‌دهند، تجربه کنند و اتفاقات را از زاویه دید خودشان ببینند؛ البته آن‌ها در این حالت از دنیای واقعی اطرافشان دور نمی‌شوند یا اینکه با استفاده از نمایشگرهای سربسته و هدفون، شامل عینک‌ها یا کلاه‌هایی که یک صفحه نمایش و هدفون درون آن‌ها تعبیه شده، می‌توانند کاملاً از محیط اطراف خود جدا و غرق در محیط مجازی شوند.

ویژگی دیگر واقعیت مجازی، همانندسازی کاربر با آواتار اوست. همانندسازی بدن معناست که در کاربر حسی ایجاد می‌شود؛ به گونه‌ای که گویا آواتار بدن مجازی اوست و این کار از طریق هماهنگ کردن حرکات آواتار با حرکات بدن واقعی کاربر انجام می‌شود. کاربر با همین همانندسازی، خود را در بدن آواتار احساس کرده و دنیای اطراف را از طریق چشمان آواتار می‌بیند و تجربه می‌کند. متقابلاً آواتار نیز در رفتار و آنچه کاربر از خود و هویت خود در حین تجربه واقعیت مجازی درک می‌کند تأثیر می‌گذارد (Rosenberg et al., 2013, p. 82). همانندسازی کاربر وقتی بیشتر خواهد بود که دستگاه‌های صوتی - تصویری با دستگاه‌های لمسی ترکیب شوند و ارتباط کامل‌تری بین کاربر و آواتار ایجاد کنند.

واقعیت مجازی از تکنیک‌های مؤثری استفاده می‌کند تا بتواند انواع احساسات را در کاربر القا کند و از این طریق بتواند احساس تجربه زندگی واقعی را در او ایجاد کند. این تکنیک‌ها محیطی شبیه به واقعیت ایجاد می‌کنند. در عین حال امکان دست‌کاری و کنترل دقیق متغیرهای

1. Electroencephalograph
2. Head-mounted Displays

محیط مجازی مانند شکل ظاهری، رنگ‌ها، بافت‌ها، اصوات، بوها و هر آنچه را قابلیت تنظیم و تغییر دارد داشته و می‌توانند واکنش‌ها و رفتار کاربران را در آن محیط مطالعه و بررسی کنند. در یک تجربه فراگیر سه‌بعدی که کاربر احساس می‌کند مستقیماً در آن محیط حضور دارد و آن را می‌بیند درک کاربر از طریق فرایندهای زیر انجام می‌شود: ۱. فریب حواس کاربر به‌طوری که گمان کند آنچه در محیط مجازی می‌بیند واقعی است؛ ۲. انتقال و جابه‌جاشدن حس مکان کاربر به درون محیط مجازی؛ ۳. این که محیط به‌اندازه کافی برای کاربر واقع‌گرا به نظر برسد؛ ۴. عاملیت کاربر، بدین معنا که کاربر احساس می‌کند می‌تواند بر محیط پیرامون خودش اثر بگذارد و آن را کنترل کند. برای مثال وقتی دستش را حرکت می‌دهد آواتار هم به همان شکل دستش را حرکت می‌دهد یا وقتی قدم بر می‌دارد در محیط مجازی حرکت می‌کند. این امر ابتدا از این‌رو امکان‌پذیر می‌شود که واقعیت مجازی به‌صورت پیش‌بینانه عمل می‌کند، درست مانند مغز ما که در تعامل با دنیای واقعی چنین است. برای فهمیدن کامل مطلب باید توضیح داد که علوم اعصاب، مغز انسان را با یک شبیه‌ساز مقایسه می‌کند. مغز ما در طول فرایند تکاملی، توانایی پیش‌بینی محرک‌های شنیداری، بصری، لامسه و غیره را پیش از اینکه به‌شکل آگاهانه توسط خود فرد حس شود کسب کرده و پیش‌بینی می‌کند که حواس فرد چه محرک‌هایی را دریافت خواهد کرد. به این توانایی مغز در پیش‌بینی ادراکات حسی قبل از وقوع واقعی آن‌ها «مرزگذاری پیش‌بینانه»^۱ می‌گویند؛ بدین‌صورت واقعیت مجازی فراگیر به‌صورت پیش‌بینانه عمل می‌کند و محتوای شبه واقعی تولید می‌کند که دقیقاً با آنچه مغز ما در پاسخ به دنیای واقعی تولید می‌کند هم‌خوانی دارد (Riva et al., 2019, p. 61).

تحقیقات بیانگر آن است که واقعیت مجازی صرفاً به‌دنبال ارائه محیطی با شباهت زیاد به واقعیت نیست؛ بلکه هدف اصلی آن غوطه‌وری احساسی کاربر در محیط مجازی است تا از یک مشاهده‌گر ساده به شرکت‌کننده‌ای تبدیل شود که درگیری عاطفی با محیط دارد و آنچه در محیط اتفاق می‌افتد واقعی تلقی کند (Slater et al., 2020, p. 54). به این موضوع با عنوان واقع‌گرایی روان‌شناختی^۲ اشاره می‌کنند؛ بنابراین غوطه‌وری، حضور و هویت‌یابی با آواتار زمانی تقویت می‌شوند که این تجربه با توانایی برانگیختن احساسات در کاربر، به‌ویژه اضطراب، آرامش، ترس و شادی یکپارچه شود (Bernardo et al., 2021, p. 74).

به همین دلایل، همان‌طور که ریوا و همکاران مطرح می‌کنند، واقعیت مجازی نه‌تنها یک فناوری متقاعدکننده بلکه یک فناوری تحول‌آفرین نیز هست که قادر است درک افراد از واقعیت را تغییر دهد (Riva et al., 2022, P. 96). باید توجه کرد استفاده گسترده باعث ایجاد نگرانی‌های اخلاقی قابل توجهی مانند نقض حریم خصوصی ذهن، اعتیاد و وابستگی، ترویج خشونت، انزوای اجتماعی و مشکلات بهداشت روان شده است. نگرانی اخلاقی ناظر به استفاده دوگانه از فناوری‌های واقعیت مجازی است چرا که از این فناوری‌ها علاوه‌بر استفاده در حوزه‌های پزشکی، آموزشی و تفریحی، می‌توان به‌طور غیرقانونی برای دست‌کاری افکار، درک واقعیت و ترجیحات که به رفتارهای اخلاقی نادرست منجر شود استفاده کرد. همان‌طور که بلیتز و مارکل اشاره کرده‌اند این نگرانی‌های شایان توجه درمورد اطلاعات نادرست و دست‌کاری حالات ذهنی کاربران امری است که حقوق کیفری باید به آن بپردازد (Bublitz & Merkel 2014, p. 7). در مغز انسان بخشی از شبکه عصبی به نام نورون‌ها هستند که بسیار انعطاف‌پذیرند و وظیفه پردازش اطلاعات حسی و ادراکی را برعهده دارند. وقتی فرد وارد محیط واقعیت مجازی می‌شود اطلاعات بصری، شنیداری و حس عمیق کاذب ایجادشده باعث فریب این نورون‌ها می‌شود. در نتیجه آن‌ها فکر می‌کنند فرد واقعاً در آن مکان حضور دارد و همان‌طور که در دنیای واقعی واکنش نشان می‌دهند در محیط مجازی نیز فعال شده و اطلاعات را پردازش می‌کنند و بدین‌ترتیب باعث می‌شود فرد احساس کند واقعاً در مکانی حضور دارد که از طریق محیط مجازی شبیه‌سازی شده است.

استفاده طولانی از فناوری واقعیت مجازی فراگیر با توجه به توانایی آن در تحریک حواس و القای تجربیات زنده می‌تواند تغییرات پایداری را در مغز، شخصیت و رفتار کاربران ایجاد کند. این فناوری با تأثیر در قابلیت انطباق‌پذیری و تغییرپذیری نورون‌ها نوروپلاستیسته^۳ و توانایی مغز در رشد و ترمیم سلول‌های عصبی، سبب شکل‌گیری الگوها و عادات جدیدی در مغز شده و به دگرگونی در رفتارهای انسانی منجر می‌شود.

1. Predictive coding
2. Psychological realism
3. Neuroplasticity

بدین جهت وقتی می‌خواهیم سیاست‌ها و قوانین جزایی و ضمانات اجراهای کیفری مرتبط با کنترل و نظارت بر واقعیت مجازی فراگیر وضع کنیم باید موضوع «احساسات و عواطف انسانی» را محور اصلی و کانون توجه قرار دهیم. چون واقعیت مجازی فراگیر با تأثیر در احساسات کاربر می‌تواند نحوه درک حقایق را برای او دچار اختلال کند. باید تمرکز سیاست‌گذاری کیفری بر حفظ حریم خصوصی و کرامت انسانی کاربران بر مدیریت عواطف و کنترل ابزارهای القای احساسات غیر واقعی باشد؛ چراکه خطر بیشتری را برای حقوق کاربران نسبت به محیط‌های دوبعدی ایجاد می‌کند. این ماهیت دوگانه وضع مقررات و قوانین کیفری و نظارت بر این فناوری را پیچیده و دشوار می‌کند؛ چراکه نیاز است میان آسیب‌های کوتاه‌مدت، که مستقیم و فوری هستند؛ مثل سرگیجه، تهوع، صدمات جسمانی و آسیب‌های بلندمدت آن که غیر مستقیم و تدریجی هستند مثل اعتیاد، افسردگی، تغییر شخصیت تفکیک قائل شد. این نگرانی بلندمدت به برخی جنبه‌های مطرح‌شده در بخش سه مربوط است که برای بررسی بیشتر به شرح زیر به آن می‌پردازیم.

۳. خطرات خاص واقعیت مجازی و پیشنهاد رویکرد حقوقی در مواجهه با آن

در حوزه حقوق کیفری، چالش‌ها و خطرات بالقوه‌ای که گسترش فناوری واقعیت مجازی می‌تواند برای حریم خصوصی، امنیت و سلامت روانی افراد داشته باشد، تحلیل و بررسی شده است. این تحلیل سه خطر خاص در ارتباط با رواج فزاینده استفاده از فناوری‌های واقعیت مجازی و افزایش کاربردهای آن در زندگی روزمره مردم، به‌ویژه واقعیت مجازی تجاری که با هدف کسب درآمد و بازده اقتصادی توسط شرکت‌های خصوصی که محصولات و خدماتی را تولید و عرضه می‌کنند، شناسایی کرده است. سه حوزه اصلی و خاص ریسک به شرح زیر است:

۱. واقعیت مجازی به دلیل ماهیت تعاملی و غوطه‌ورکننده‌ای که دارد، می‌تواند حجم زیادی از اطلاعات شخصی و حساس کاربران را حین استفاده جمع‌آوری و ضبط کند. این اطلاعات شامل مواردی مثل الگوهای رفتاری، علائق، ترجیحات، اطلاعات بیومتریک و فیزیولوژیکی مانند ضربان قلب، میزان مصرف انرژی بدن و غیره می‌شود که به‌طور جامعی گردآوری شده و یک پروفایل کامل و دقیق از کاربر ترسیم می‌کند. درنتیجه، به نقض شدید حریم خصوصی ذهنی کاربران منجر می‌شود؛

۲. اصولاً آواتار به نمایش دیجیتالی و مجازی یک کاربر در محیط واقعیت مجازی اطلاق می‌شود. واقعیت مجازی به‌گونه‌ای طراحی و توسعه یافته است که کاربر می‌تواند از طریق آواتار خود در محیط مجازی، تعاملات و تجربیاتی شبیه به دنیای واقعی داشته باشد. این امر، توانایی شبیه‌سازی یک تجربه فیزیکی برای آواتار کاربر در محیط مجازی است؛

۳. واقعیت مجازی به دلیل ایجاد محیطی بسیار غوطه‌ورکننده و تعاملی، امکان دست‌کاری رفتار، عقاید، احساسات و تصمیم‌گیری‌های کاربران را به‌صورت چشمگیری فراهم می‌کند. این پتانسیل بیانگر خطر سوءاستفاده و کنترل افراد توسط مجریان و طراحان محیط‌های واقعیت مجازی است.

۳-۱. خطر اول: حفاظت از حریم خصوصی ذهنی کاربران در محیط واقعیت مجازی

یکی از مشکلات اساسی ناشی از هم‌سویی هوش مصنوعی و فناوری‌های عصبی، نگرانی درخور توجهی برای حفظ حریم خصوصی داده‌های ذهنی کاربران است؛ چراکه احتمال نقض حقوق مشروع آن‌ها را موجب می‌شود (Ienca et al., 2022, p. 92). هوش مصنوعی به‌دنبال ساخت سیستم‌هایی هوشمند است که قابلیت‌های ذهن انسان مانند یادگیری، استنتاج و تفکر منطقی را شبیه‌سازی کند. ازطرفی فناوری‌های عصبی بر روی شناخت سیستم عصبی و مغز انسان برای ساخت و توسعه واسطه‌های مغز - ماشین^۱ متمرکز شده‌اند و در این راستا هم‌سویی و ادغام این دو به معنای استفاده ترکیبی از توانایی‌های هوش مصنوعی و واسطه‌های مغز - ماشین برای دستیابی به پیشرفت‌های بهتر در هر دو حوزه است. بدین ترتیب فناوری جدیدی متولد می‌شود که توانایی‌های ذهن و مغز انسان را با قدرت پردازش هوش مصنوعی یکپارچه می‌کند. این امر می‌تواند موجب نگرانی‌های عمیق برای حفظ حریم خصوصی ذهنی کاربران تلقی شود.

1. Bbrain-computer interface

واقعیت مجازی فراگیر به دلیل ایجاد حس حضور و تعامل واقعی و عمیق برای کاربر خود نیز تهدیدی برای حریم خصوصی ذهنی و روانی اوست. علاوه بر این ویژگی های روان شناختی تجارب غوطه ورکننده مانند جذابیت و طبیعی به نظر رسیدن موجب می شود کاربران به افشای اطلاعات حساس و شخصی خود بی توجه شوند. این موارد باعث ایجاد دو عامل خطر اضافی برای نقض حریم خصوصی ذهنی کاربران در مقایسه با سایر فناوری ها می شود.

اول زمانی که این فناوری های عصبی در زمینه درمانی و بالینی استفاده می شوند ملاحظات و پروتکل های اخلاقی و پزشکی خاصی برای حفظ سلامت و ایمنی بیماران اعمال می شود، اما وقتی واقعیت مجازی به صورت تجاری و عمومی عرضه می شود، این تضمین ها و ملاحظات اخلاقی کمتر رعایت می شود و کاهش می یابد؛ بنابراین احتمال آسیب های اخلاقی و روانی ناشی از مصرف گسترده و بی رویه افزایش می یابد. دوم آن که در واقعیت مجازی فراگیر انواع گوناگونی از داده ها درباره کاربر از طریق دستگاه ها و وسایل متصل به سیستم قابل جمع آوری است. این دستگاه ها عبارت اند از: موقعیت یاب های جغرافیایی، میکروفن ها، دوربین ها و حسگرهایی که اطلاعات محیط واقعی پیرامون کاربر را ضبط می کنند. همچنین دستگاه های لمسی^۱ داده های زیستی و حرکتی کاربر مانند صدا، بیومتریک چشم، فعالیت مردمک را ثبت می کنند. علاوه بر این ها، مکالمات و تصاویر فعالیت های کاربر در دنیای مجازی نیز قابلیت ضبط شدن دارد.

این وضعیت و جمع آوری داده های گسترده از کاربر در محیط واقعیت مجازی فراگیر به دلایل زیر به منزله یک عامل خطر و نگرانی حریم خصوصی محسوب می شود: «حجم بسیار زیاد و جامع داده ها از جنبه های مختلف زندگی کاربر جمع آوری می شود که به راحتی امکان سوء استفاده را فراهم می کند.» «فقدان قوانین کافی برای محافظت از این داده ها در برابر دسترسی و استفاده های غیرمجاز و النهایه «امکان پایش، کنترل و تحت تأثیر قراردادن کاربر از طریق دست کاری این داده ها» نگرانی های جدی در مورد حریم خصوصی و امنیت کاربران ایجاد می کند. این داده ها امکان استنباط اطلاعات حساسی را در مورد هویت، نژاد، تنوع جنسی، ویژگی های فرهنگی، نمایه های روان شناختی، بیماری های بالقوه کاربران فراهم می کنند (Qamar et al., 2023, p. 67).

عمدتاً از طریق استفاده ترکیبی از فناوری های ردیابی چشم و انبساط مردمک تصویری پویا از حالات ذهنی کاربران و وضعیت روانی آن ها ارائه می دهد. ردیابی چشم نشان می دهد کاربران به کجا نگاه می کنند بر چه چیزی تمرکز دارند و برای چه مدت. همچنین انبساط مردمک نشان دهنده سطح علاقه آن ها به محرک های خاص است. در همین راستا هلر مفهوم «روان شناسی بیومتریک»^۲ را به منزله اصطلاحی جدید برای این نوع اطلاعات پویای مرتبط با بدن ارائه کرده است (Heller, 2020, p. 105). این اطلاعات نه تنها به هویت فرد، بلکه عمدتاً به علایق وی مرتبط بوده و از طریق منابع مختلف مانند اسکن چهره، واکنش های الکتریکی پوست، الکتروانسفالوگرافی^۳، الکترومیوگرافی^۴ و الکتروکاردیوگرافی^۵ به دست می آیند.

به این ترتیب هویت کاربر در جنبه های مختلف زیست شناختی خود شفاف می شود و به راحتی توسط دیگران قابل درک یا مشاهده می شود و کاربران نمی توانند این جنبه های خود را پنهان کنند. به همین علت، سازمان های بین المللی مختلف در مورد اهمیت این خطر، به ویژه در بخش هایی مانند نورومارکتینگ^۶، هشدار می دهند و تبعات منفی برای روابط اجتماعی شهروندان و آزادی های عمومی مردم را متذکر می شوند (UNESCO, 2023, p. 40)؛ بنابراین ضروری است صنعت فناوری واقعیت مجازی از طریق اقدامات مختلف زیر حفاظت از کاربر را افزایش دهد: الف) تقویت رضایت آگاهانه کاربر در مورد حریم خصوصی ذهنی و تجربه غوطه ورکننده: بدان معنا که کاربران باید کاملاً از خطرات احتمالی حریم خصوصی و تأثیرات روان شناختی ناشی از استفاده از این فناوری ها مطلع باشند و تنها در صورت تمایل آگاهانه به استفاده از آن ها

1. Haptic Device
2. Biometric psychography
3. Electroencephalograph
4. Electromyography
5. Electrocardiography
6. Neuromarketing

رضایت دهند؛ ب) تعیین سطوح مختلف مشخصات مدیریت محتوا: بسته به نوع محتوا و کاربران هدف باید سطوح مختلفی از کنترل و محدودیت برای نمایش اطلاعات در نظر گرفته شود و در ابتدا محتوی ارزیابی شود تا موضوع مخاطب هدف خاصی باشد؛ ج) پیاده‌سازی سیستم رتبه‌بندی برای سرگرمی واقعیت مجازی: مشابه سیستم‌های رده‌بندی سنی فیلم‌ها برای انواع سرگرمی‌های واقعیت مجازی نیز سیستم رتبه‌بندی براساس درجه محتوای حساس یا پرمخاطره ایجاد شود؛ د) ایجاد قواعد رفتاری در سراسر صنعت: به جای تکیه صرف بر تصویب قوانین و مقررات کیفری توسط مقنن خود صنعت باید اصولی حرفه‌ای و اخلاقی برای توسعه و استفاده از فناوری‌های فراگیر وضع کند. آنچه بیان شد نشان‌دهنده سطح اولیه حفاظت از کاربر بوده و بهترین رویکرد برای حمایت مؤثر از حریم خصوصی ذهنی کاربر است. در سطح دوم حریم خصوصی ذهنی کاربران اعم از آن‌ها که شناسایی شده (یعنی کاربرانی که هویت واقعی آن‌ها مستقیم یا غیرمستقیم از طریق داده‌هایی مانند نام، آدرس ایمیل، شماره تلفن و غیره مشخص شده) یا قابل شناسایی هستند (یعنی کاربرانی که اگرچه هویت مستقیم آن‌ها شناخته شده نیست، اما با ترکیب و تحلیل داده‌هایی که ارائه می‌دهند می‌توان به هویت واقعی آن‌ها پی برد) نیز باید از طریق حقوق کیفری تضمین شود؛ لذا حمایت از حریم خصوصی ذهنی کاربر توسط حقوق کیفری باید بر سه جنبه کلیدی متمرکز باشد:

۱) حفاظت باید بر اطراف داده‌های ساختاری و عملکردی مغز متمرکز شود و چنین داده‌هایی را به منزله اطلاعات شخصی حساس در نظر بگیرد؛ ۲) اطمینان از رضایت آگاهانه کاربر اعمال شود؛ ۳) امکان پردازش انبوه داده‌های ذهنی کاربران شناسایی شده یا قابل شناسایی ممنوع اعلام شود و این اقدام از حیث اعمال ضمانت اجرای کیفری برای جلوگیری از تجاری‌سازی آن‌ها با ممنوعیت قاچاق اعضای بدن انسان برابری کند.

در این راستا بولیتز و مرکل پیشنهاد کرده‌اند که هک مغزی^۱ باید به‌صراحت جرم‌انگاری شود. بدیهی است مسئولیت کیفری در درجه اول باید برعهده پلتفرم‌هایی باشد که مسئول جمع‌آوری و ذخیره داده‌ها در ساختار داخلی و فناوری ابر خودند (Bublitz et al., 2014, p. 75). آن‌ها باید ملزم به مدیریت ریسک‌هایی باشند که در تولید آن مشارکت دارند. علاوه بر آن‌ها هر بازیگر دیگری اعم از فرد (شخص حقیقی) یا سازمان (شخص حقوقی) که عمداً حریم خصوصی کاربران را از طریق اقداماتی مانند هک کردن دستگاه کاربر یا سرقت اطلاعات ذهنی کاربر نقض کند نیز باید مسئولیت کیفری داشته باشد.

۲-۳. خطر دوم: آسیب عاطفی ناشی از تجربیات عمیق

دومین خطر خاص واقعیت مجازی، توانایی آن برای بازتولید تجربه فیزیکی آواتار در مغز کاربر است. مغز تجربه مجازی را به‌طور واقعی درک و پردازش می‌کند؛ به‌گونه‌ای که کاربر آن را واقعی احساس می‌کند؛ حتی اگر بداند واقعی نیست (Slater, 2009, p. 54). این ویژگی باعث می‌شود به هنگام ارتکاب یک جرم علیه کاربر، وی تجربه بزه‌دیدگی خود را احساس کند، خاطرات آن را حفظ کند و حتی ممکن است تجربه آسیب‌زای خود را به زندگی واقعی منتقل کند. برای مثال، وقتی قربانیان سوءاستفاده جنسی تجربیات خود را توصیف می‌کنند، به یک آسیب عاطفی اشاره می‌کنند که «کاملاً واقعی به نظر می‌رسد» (Belamire, 2016, p. 98). این نوع رفتارهای مجرمانه در دنیای مجازی قابل‌پیش‌بینی است و احتمالاً شیوع زیادی خواهند داشت؛ زیرا این دنیاها محیط‌های غوطه‌ورکننده چندکاربره‌ای هستند که افراد می‌توانند از طریق آواتارهای خود و در زمان واقعی با یکدیگر و با اشیای مجازی تعاملاتی شبه‌واقعی داشته باشند. رفتارهای مجرمانه مذکور می‌تواند هرگونه آسیب جسمی مانند مشت‌زدن، لگدزدن و غیره باشد؛ با این حال، باید دوباره تأکید کرد که آسیب شخصی تنها در تجارب غوطه‌ورکننده رخ می‌دهد (Castro, 2022, p. 23). بنابراین، ارزیابی حقوقی رفتارهای طی تجارب واقعیت مجازی به سطح غوطه‌وری کاربر - قربانی و آگاهی کاربر دیگر

از آن بستگی خواهد داشت. به همین ترتیب، در مورد مسئولیت کیفری نیز تعیین اینکه چه کسی محتوای یا رفتار آسیب‌رسان را خلق یا کنترل می‌کند (کاربر، مالک پلتفرم) بسته به ماهیت عمل غیرقانونی ضروری خواهد بود.

۱-۲-۳. آسیب فیزیکی و روانی از تجربه مجازی

هنگام بررسی موضوع آسیب فیزیکی یا روانی به کاربران عموماً و کاربران خاص (منظور کاربرانی هستند که به دلیل ویژگی‌های فردی مانند سن یا وضعیت روانی در برابر آسیب‌های ناشی از واقعیت مجازی آسیب‌پذیرترند) ناشی از تجارب مجازی فراگیر سه موقعیت مختلف می‌تواند پیش آید: الف) آسیب فردی ناشی از استفاده و سوءاستفاده از این فناوری توسط مصرف‌کنندگان براساس کاربرد و هدفی که سازندگان فناوری واقعیت مجازی برای آن طراحی کرده‌اند؛ ب) آسیب فیزیکی به کاربر توسط اقدامات عمدی یک «بازیگر بد»؛^۱ ج) آسیب فیزیکی یا روانی به کاربر از طریق اقدامات انجام‌شده روی آواتار آن‌ها (مورد اخیر مشخصاً با واقعیت مجازی فراگیر مرتبط است).

قبل از پرداختن به هر یک از سه موقعیت بالا، باید تأکید کرد که اصل اساسی از منظر سیاست کیفری این است که بررسی حقوقی صدمات جسمی، ناشی از فضای مجازی، باید به همان شیوه‌ای که در دنیای واقعی انجام می‌شود صورت گیرد.

آنچه در زندگی واقعی غیرقانونی است، در زمینه مجازی فراگیر نیز باید غیرقانونی باشد. باید به آسیب‌ها و خطرات واقعی، که ممکن است برای کاربر رخ دهد (نه لزوماً آنچه در آواتار منعکس می‌شود)، توجه شده و به عنوان جرایم علیه تمامیت جسمانی اشخاص رسیدگی شوند. الف) آسیب فیزیکی و روانی به کاربر ناشی از استفاده و سوءاستفاده از واقعیت مجازی: مشابه بازی‌ها و فناوری‌های دوبعدی، مطالعات نشان داده‌اند که سوءاستفاده از واقعیت مجازی به عنوان محصولی که با هدف استفاده مصرف‌کنندگان در دسترس قرار گرفته است، ممکن است به بروز آسیب‌های بالقوه فیزیکی یا روانی در برخی افراد منجر شود. از جمله این آسیب‌ها می‌توان به اعتیاد، جدایی از واقعیت و از خودبیگانگی یا «دیسمورفیا»^۲ و آسیب‌های شخصی ناشی از حوادث اشاره کرد (Peckmann et al., 2022, p. 72). تأثیر استفاده بیش از حد از فناوری‌های مجازی بر افراد متفاوت است و تحت تأثیر عواملی همچون علاقه فرد به فناوری‌ها و استفاده از آن‌ها، بلوغ و رشد روانی و شخصیتی فرد، وضعیت اقتصادی، تحصیلات، فرهنگ کاربر قرار دارند؛

ب) آسیب فیزیکی به کاربر که مستقیماً توسط اقدامات عمدی یک طرف ثالث «بازیگر بد» ایجاد می‌شود: این مورد می‌تواند از طریق هک دستگاه‌های کاربر رخ دهد و در محیط واقعیت مجازی چندکاربره امکان‌پذیر است (Vondracek et al., 2023, p. 2)؛ مانند حمله‌ای که با دست‌کاری ادراک فضایی کاربر به تصادف یا آسیب‌های فیزیکی به او منجر شود یا هدایت کاربر او را به سمت پله‌هایی به صورت ناخودآگاه هدایت کند که ممکن است در آنجا سقوط کند. این دسته از آسیب‌های فیزیکی همچنین شامل موارد هک احساسات^۳ از طریق تسریع ضربان قلب کاربر با یک تجربه ترسناک می‌شود. این پیامدهای خطرناک فیزیکی می‌تواند مشمول ضمانت اجراها و مجازات‌های کیفری جرایم علیه تمامیت جسمانی اشخاص باشد؛

ج) آسیب فیزیکی واردشده بر آواتار با پیامدهایی برای کاربر از تجربه مجازی فراگیر: این گروه از موارد در واقعیت مجازی، که با ماهیت غوطه‌ور بودن آن مرتبط است، شامل رفتاری است که در آن محیط انجام می‌شود و به سمت آواتار که نماینده کاربر است هدایت می‌شود. برای مثال، در وضعیتی که در آن یک آواتار به صورت آواتار دیگری مشت می‌زند یا با چاقو آن را می‌زند، این سؤال مطرح می‌شود که آیا این رفتارها، درحالی که باعث آسیب واقعی فیزیکی به کاربر نمی‌شوند، اما بالقوه ممکن است باعث ناراحتی عاطفی قابل توجهی شوند، می‌توانند معادل فیزیکی خود در دنیای واقعی در نظر گرفته شوند؟ پاسخ آشکارا به نظر می‌رسد خیر باشد؛ حتی در بافت تجربیات غوطه‌ورکننده با دستگاه‌های لمسی تمام بدن نیز پاسخ منفی است. در مواردی مانند احساس درد ناشی از ضربه چاقو در یک لباس لمسی که تمام بدن را پوشانده، هیچ آسیب

۱. Bad Actor: افراد یا گروه‌های هکر هستند که با نفوذ به سیستم‌ها، امنیت کاربران فضای مجازی را به خطر می‌اندازند و ممکن است باعث وارد شدن آسیب‌های به آن‌ها شوند.

2. Dysmorphia

3. Emotion Hacking

فیزیکی به بدن کاربر وارد نمی‌شود. با این حال، ممکن است این سؤال مطرح شود که آیا چنین رفتارهایی که می‌توانند به آسیب روانی منجر شوند، از نظر قانونی امکان دارد که به عنوان آسیب روانی مجازات شوند؟ به نظر می‌رسد درحالی‌که از نظر تئوری امکان‌پذیر است، در عمل در حال حاضر ممکن نیست (Tahmasbi & Shahmiradi, 2015, p. 118)؛ زیرا برای اثبات قانونی آسیب روانی در روند یک دادرسی جنایی، باید شواهد درخور توجهی وجود داشته باشد؛ از جمله آنکه شواهد بیانگر آن باشند که آسیب روانی قبل از تعامل مجازی وجود نداشته است و همچنین لازم است رابطه‌ای علی بین آسیب روانی و تعامل مجازی تجربه شده وجود داشته باشد. به عبارت دیگر، آسیب روانی باید مستقیماً ناشی از تعامل با محتوای مجازی مضر یا اقدامات عمدی شخص ثالث از طریق آواتار آن‌ها باشد. و البته وجود نشانه‌های زیستی^۱ قابل شناسایی، که بیانگر آن باشند که آسیب در سطح زیستی و فیزیولوژیک بدن و مغز کاربر ایجاد شده است، لهذا تدارک و اثبات شواهد و مدارکی که بتوان از طریق آزمایش‌ها و روش‌های علمی، وجود آسیب روانی را اثبات کند در عمل باعث مواجهه حقوق کیفری با چالش‌های جدی می‌شود.

۳-۳. خطر سوم: دست‌کاری رفتار انسان

واقعیت مجازی فراگیر به منزله یک فناوری عصبی تحریک و القاکننده احساسات، خطر آشکار دست‌کاری و کنترل رفتار و افکار شهروندان را به همراه دارد. دست‌کاری به معنای القای محتوای طراحی شده یا ایده‌های دروغ به صورت غیرمستقیم به کاربر است؛ به گونه‌ای که گویا خود او به آن‌ها رسیده است. این خطر بزرگ‌تر از الگوریتم‌های متقاعدکننده در محیط دویعدی رسانه‌های اجتماعی مانند اینستاگرام یا فیس‌بوک و خطر جدی برای سلامت روان نوجوانان و مصرف‌کنندگان است (Harari, 2018, p. 105).

در بخش دوم لایحه هوش مصنوعی پیشنهادی پارلمان اروپا در مورد تدوین قوانین هماهنگ در زمینه هوش مصنوعی تأکید شده که برخی از سیستم‌های هوش مصنوعی می‌توانند خطرات غیرقابل قبولی از دست‌کاری افراد ایجاد کنند. به همین دلیل، ماده ۵ لایحه فوق‌الذکر استفاده از سیستم‌های هوش مصنوعی، که ناخودآگاه و زیر سطح آگاهی انسان او را تحت تأثیر قرار می‌دهند تا به طور واقعی و عینی رفتار شخص را تحریف کنند، ممنوع می‌کند. با این حال، این ممنوعیت به سیستم‌های هوش مصنوعی محدود است که می‌توانند باعث آسیب فیزیکی یا روانی مانند القای خودکشی یا خودآزاری به شخص شوند.

بنابراین، القای خودکشی یک کاربر در محیط مجازی از طریق آواتار خود باید مشمول همان قوانین و مجازات‌های کیفری باشد که در دنیای واقعی اعمال می‌شود. مسئولیت کیفری باید به افراد یا نهادهای حقوقی مسئول چنین محتوایی نسبت داده شود. اینکه افراد بتوانند بدون محدودیت و دخالت دیگران، افکار، عقاید و ایده‌های خود را آزادانه شکل دهند و در ذهن خود پیوراند، بخشی از مباحث گسترده حقوق عصبی است که اکنون مورد بحث و توجه محققان قرار دارد و از جمله حقوقی است که قوانین جزایی باید به حمایت از آن بپردازند و ریشه‌های چنین حقوقی را می‌توان در آزادی‌های مشروع و بنیادین اندیشه و افکار اشخاص دریافت (Bublitz, 2022, p. 98).

باید توجه داشت که رویکرد فعلی سیاست کیفری نیاز به ارزیابی و سنجش مجدد همگام با پیشرفت فعلی فناوری‌های عصبی و هوش مصنوعی دارد تا به طور مؤثر چالش‌ها و پیامدهای ناشی از توسعه این فناوری‌ها را تحت نظارت و رسیدگی قرار دهد. چشم‌انداز در حال تحول فناوری‌های عصبی و هوش مصنوعی، لزوم رویکردی دقیق‌تر و آگاهانه‌تر سیاست جنایی برای کنترل رفتارهای جنایی را می‌طلبد. در مورد فناوری‌های عصبی، که پتانسیل دسترسی مستقیم غیرمجاز در فعالیت مغز افراد را دارند، خواه تهاجمی (یعنی مداخله‌ای که نیاز به نفوذ فیزیکی به بدن و مغز دارد) یا غیرتهاجمی (یعنی مداخله‌ای که نیاز به نفوذ فیزیکی در بدن ندارد)، بدون در نظر گرفتن مدت آن، باید به صراحت توسط حقوق کیفری برای حفظ تمامیت ذهنی افراد جرم‌انگاری شود. در همین راستا، تغییر فعالیت مغز بدون رضایت کاربر قربانی (هک مغز) باید به صراحت به منزله جرم جنایی تعریف شود؛ زیرا فناوری به سطحی از توسعه رسیده است که چنین مداخله مستقیمی را ممکن می‌سازد (Gonzalez et al., 2022, p. 45).

واقعیت مجازی فراگیر یک فناوری غیرتهاجمی، غیرمستقیم و کمتر مؤثر است. غیرتهاجمی به این معناست که فناوری به طور فیزیکی وارد بدن کاربر نمی‌شود یا بدن را تغییر نمی‌دهد. واقعیت مجازی تجربه غیرمستقیم واقعیت را فراهم می‌کند؛ زیرا کاربران با یک محیط شبیه‌سازی شده به جای دنیای واقعی تعامل دارند. اصطلاح «کمتر مؤثر» نشان می‌دهد که واقعیت مجازی ممکن است کاملاً تجربیات دنیای واقعی را تکرار نکند. توجه به این ویژگی‌هاست که ارزیابی محتوا یا رفتار در واقعیت مجازی فراگیر در مقایسه با ارزیابی‌های دنیای واقعی چالش‌برانگیزتر است. مهم‌ترین چالشی که حقوق کیفری در ارزیابی محتوا یا رفتار در واقعیت مجازی فراگیر با آن روبه‌روست از حیث اثربخشی دست‌کاری کاربران است.

از نظر اثربخشی دست‌کاری، واقعیت مجازی فراگیر یک خطر متوسط از نظر شدت و میزان اثرگذاری بین فناوری‌های عصبی‌ای است که می‌تواند در دنیای واقعی، مثل تبلیغات و بازاریابی و در محیط دیجیتال دوبعدی توسعه یابد (Slack & McGregor, 2003, p. 96). خطر اصلی واقعیت مجازی فراگیر از ترکیب عوامل مختلفی مانند غوطه‌ورشدن عمیق در محیط مجازی، احساس حضور در لحظه و تعامل بسیار بالا به همراه استفاده از هوش مصنوعی برای تأثیرگذاری در کاربران ناشی می‌شود. در سطح متوسط خطر، به نظر می‌رسد که حمایت کیفری از سلامت روانی کاربران در برابر آسیب‌های احتمالی نباید به اندازه‌ای که برای فناوری‌های عصبی خاص پیشنهاد شده گسترده باشد. به همین دلیل، حقوق کیفری باید بخش‌های خاصی مثل بازی‌های رایانه‌ای و شبکه‌های اجتماعی، که افراد زمان زیادی را در آن‌ها سپری می‌کنند، در نظر بگیرد. با توجه به گزارش‌های حاصله در مورد هوش مصنوعی اقناع‌کننده، بخش‌هایی که اطلاعات نادرست و دست‌کاری شهروندان در آن‌ها ظرفیت زیان‌بار خود را نشان داده‌اند، عبارت‌اند از: حقوق مصرف‌کنندگان و سلامت روان نوجوانان (UNESCO, 2023, p. 39). در مورد واقعیت مجازی فراگیر نیز انتظار تأثیر مشابهی را در این حوزه‌ها می‌توان داشت. در این خصوص، برای مثال می‌توانیم بر دست‌کاری عاطفی با اهداف تجاری از طریق واقعیت مجازی فراگیر متمرکز شویم.

کاربران براساس رفتار و واکنش‌هایشان که در طول تجربیات واقعیت مجازی به‌صورت دائمی، پرتکرار و در زمان واقعی رصد می‌شوند، پیشنهاد محصولاتی دریافت خواهند کرد. در محیط متاورس، کاربران ممکن است به‌طور فزاینده‌ای در معرض تبلیغات زیرآستانه، بسیار تأثیرگذار و شخصی‌سازی شده قرار گیرند؛ لذا حفاظت از مصرف‌کننده در برابر این خطر نیز باید از طریق حقوق کیفری مورد توجه قرار گیرد. اجماع واضحی میان روان‌شناسان، متخصصان بازاریابی و علوم اعصاب در مورد اهمیت دانش روان‌شناسی و علوم اعصاب برای درک فرایند تصمیم‌گیری مصرف‌کننده وجود دارد که در آن احساسات نقش بنیادینی ایفا می‌کنند. تصمیمات مصرف‌کننده صرفاً براساس ویژگی‌های خود محصول نیست؛ بلکه بر پایه ارتباط و ایجاد نوعی پیوند احساسی مثبت در مشتری است که می‌تواند با برند و تجربه رضایت خرید یک محصول خاص برقرار شود.

این مبنای نوروبازاریابی است که تعریف آن عبارت است از: «استفاده از دانش علوم اعصاب در روان مصرف‌کننده به‌منظور تأثیرگذاری بر وی، به‌ویژه در تبلیغات و توجه مشتریان به‌گونه‌ای که احساس تعلق به یک برند داشته باشد و در طول زمان به خرید مجدد آن اقدام نماید» (Russo et al., 2022, p. 133). به همین دلیل، واقعیت مجازی به‌دلیل ماهیت فراگیر و تعاملی می‌تواند برای هر فرد به‌صورت شخصی‌سازی محتوایی متناسب با علایق، رفتار و ویژگی‌های وی ارائه کند. هلر و بار - زیو اشاره می‌کنند که تبلیغات مبتنی بر واقعیت مجازی می‌تواند اوج و نماد تبلیغات باشد؛ زیرا هدفش ایجاد تبلیغاتی است که کاربر نمی‌خواهد آن‌ها را رد کند یا حتی ممکن است متوجه نشود که آن‌ها تبلیغات هستند و به‌طور یکپارچه با تجربیات ادغام شده‌اند (Heller et al., 2021, p. 45). اگر به این موضوع، محتوای شخصی‌سازی شده را، که کاملاً با سلیقه‌ها، علایق و نیازهای آن‌ها هم‌سوست اضافه کنیم، تبلیغاتی می‌شود که بی‌تردید مقاومت‌ناپذیر است. علاوه‌براین، نوروبازاریابی براساس ایجاد پروفایل‌های مصرف‌کننده، یعنی تجزیه و تحلیل الگوهای رفتاری و ترجیحات وی به‌منظور شناسایی ویژگی‌های او و قرار دادن آن‌ها در یک پروفایل استوار است.

بررسی این هدف‌گذاری دیجیتال شخصی‌سازی شده از منظر قوانین کیفری باید مورد توجه قرار گیرد؛ لذا حقوق کیفری باید مصرف‌کنندگان را در قبال جرم تبلیغات گمراه‌کننده حمایت کند. این چهارچوب کیفری برای پرداختن به ادعاهای نادرست ارائه‌شده توسط تولیدکنندگان محصولات باید اعمال شود. دلیل این حمایت، جبران بهتر خسارت‌های واردشده به مصرف‌کنندگان و همچنین پیشگیری از وقوع جرایم علیه آن‌هاست. با این حال، حقوق کیفری علاوه بر اینکه این‌گونه از جرایم فوق را باید مجازات کند، باید تبلیغات زیرآستانه‌ای را نیز به منزله یک شیوه تجاری ممنوع، مشمول ضمانت اجراهای کیفری قرار دهد (Mosavimojab & Rafizadeh, 2015, p. 157). بنابراین، با توجه به این فناوری‌های تأثیرگذار، مصرف‌کنندگان باید حق داشته باشند مطلع شوند که تجارب واقعیت مجازی فراگیر به‌منظور اهداف تجاری ارائه می‌شود و در برابر تکنیک‌های زیرآستانه‌ای، که فراتر از فریب هستند، حمایت شوند.

نتیجه‌گیری

این مقاله به بررسی نقشی پرداخته است که حقوق کیفری باید در مدیریت استفاده غیردرمانی از واقعیت مجازی فراگیر توسط کاربران ایفا کند. در ابتدا با در نظر گرفتن واقعیت مجازی فراگیر به‌منزله یک سناریوی خطر متوسط به بررسی بین فعالیت‌های مجرمانه‌ای که صرفاً در دنیای واقعی و فیزیکی رخ می‌دهند و آن‌هایی که در محیط‌های دیجیتال دوبعدی به وجود می‌آیند پرداخته شده است.

با بررسی مطالعات تخصصی ماهیت واقعیت مجازی تجزیه و تحلیل شده است. از لحاظ فنی واقعیت مجازی یک فناوری عصبی است که هوش مصنوعی پرخطری در آن نهادینه شده است. از لحاظ عملکردی واقعیت مجازی یک فناوری عصبی تحول‌آفرین است که قادر به تغییر ادراک افراد از واقعیت است. کارایی آن در غوطه‌ورکردن کاربران در تجارب مجازی شبیه عملکرد مغز انسان است. ماهیت فراگیر واقعیت مجازی به سه حوزه خاص از خطراتی منجر می‌شود که به لحاظ قانونی به آنها توجه نشده است: (۱) ماهیت گسترده داده‌های جمع‌آوری و ذخیره‌سازی شده حین استفاده از آن‌ها؛ (۲) توانایی آن در شبیه‌سازی ذهنی تجارب فیزیکی آواتارها در کاربران؛ (۳) پتانسیل قابل توجه آن برای دست‌کاری افراد.

این مقاله ظرفیت محیط‌های مجازی را در تکوین جرایم پیش‌بینی‌پذیر ارزیابی کرده است و بر سه حوزه جرم‌خیز که شامل نقض حریم خصوصی ذهنی و آسیب عاطفی و دست‌کاری ایده، افکار و تصمیم‌گیری‌های کاربران است تمرکز کرده است. در نهایت پیشنهاد می‌کند که قانون کیفری باید به سرعت «خطوط قرمز» استفاده گسترده شهروندان از واقعیت مجازی را با رویکردی انسان‌محور تعریف کند. در راستای این هدف، چهارچوب حقوقی برای جرم‌انگاری خطرات خاص مرتبط با واقعیت مجازی فراگیر طراحی شده است. در مورد حریم خصوصی کاربر پیشنهاد کرده‌ایم که اطلاعات ذهنی کاربر (فراتر از داده‌های عصبی) باید به همان اندازه سایر اعضای بدن انسان محافظت شود که عبارت‌اند از: (۱) ممنوعیت دسترسی، انتشار یا پردازش غیرمجاز اطلاعات فیزیکی یا روان‌شناختی استخراج‌شده کاربران حین تجارب مجازی فراگیر؛ (۲) ممنوعیت معاملات سودآور این اطلاعات شخصی حساس.

در مورد آسیب عاطفی ناشی از تجربه مجازی، در نظر گرفتن این نکته حیاتی است که رویکرد حقوق کیفری مستقیماً به سطح غوطه‌وری تجربه کاربران بستگی دارد که به چندگانگی آسیب‌ها منجر می‌شود. بنابراین، معیار عمده راهنمایی که می‌توان استخراج کرد این است که باید هویت واقعی در زندگی کاربر - قربانی و کاربر - مرتکب و آسیب واقعی متحمل شده را بدون در نظر گرفتن نمایش آواتارها در تجربه مجازی ملاک قرار داد. در نهایت در مورد خطر دست‌کاری انسان این نتیجه نیز گرفته شده است که در واقعیت مجازی فراگیر، محافظت کیفری باید بر بخش‌های خاصی متمرکز شود که احتمال وقوع پیامدهای شدیدتر در آن‌ها وجود دارد. برای مثال در مورد دست‌کاری مصرف‌کننده، ممنوعیت صریح تبلیغات زیرآستانه‌ای که به‌راحتی می‌تواند از طریق واقعیت مجازی فراگیر انجام شود پیشنهاد شده است.

ظرفیت ارتکاب جرایم مرتبط با واقعیت مجازی فراگیر چشم‌انداز پیچیده‌ای را برای حقوق کیفری ایجاد می‌کند. سطوح متفاوت غوطه‌وری، قصد جنایی متهم، آواتارها، شناسایی اشخاص واقعی پشت آواتار، فقدان آگاهی اجتماعی در مورد خطرهای مرتبط با واقعیت مجازی، چالش‌های صلاحیت قضایی و اجرای قانون و مسئولیت نهادهای درگیر در زیرساخت‌های واقعیت مجازی، مالکیت محتوا یا کسب منافع از تجارت واقعیت مجازی در حدوث این پیچیدگی مؤثر است.

منابع

- حسن‌زاده، محمد و حسینی، سیدمهدی (۱۳۸۹). دسترس‌پذیری وب، مفاهیم و کاربردها. رهیافت، ۲۰(۴۶)، ۳۳-۴۴.
- حکیم‌پور، یاسمین (۱۴۰۲). از الگوریتم‌ها تا یادگیری عمیق، آنچه باید درمورد هوش مصنوعی بدانیم. حسابرس، ۱۲۳، ۵۰-۵۳.
- قاسمی، محمدعلی (۱۳۸۸). جامعه ریسک و اهمیت آن برای مطالعات استراتژیک. مطالعات راهبردی، ۱۲(۴۵)، ۲۷-۴۶.
- طهماسبی، جواد و شاهمرادی، خیراله (۱۳۹۷). چالش‌ها و خلأهای موجود در فرایند رسیدگی به جرایم سایبری. دادگستری، ۸۲(۱۰۴)، ۹۵-۱۲۱. doi: 10.22106/rlj.2018.34680
- موسوی مجاب، سید درید و رفیع‌زاده، علی (۱۳۹۴). دامنه مسئولیت کیفری اشخاص حقوقی در قانون مجازات اسلامی. پژوهش حقوق کیفری، ۴(۱۳)، ۱۴۷-۱۶۹.
- تیشه‌یار، ماندانا و پاژکی‌زاده، زهرا (۱۳۸۹). وب‌نویسی و عرصه عمومی در ایران. رسانه، ۸۲(۲)، ۱۱۱-۱۲۶.
- حیدری، علی‌مراد و جعفری، علی (۱۳۸۹). حمایت کیفری از رسانه‌های دیداری و شنیداری. رسانه، ۸۲(۲)، ۸۷-۱۱۰.
- شهریاری، حمید (۱۳۹۰). دین، فرهنگ و فناوری اطلاعات: مزایا و چالش‌های هویت مجازی در فضای سایبر. راه‌آورد نور، ۳۵(۱۰)، ۲-۷.
- داریل اسلک، جنیفر و مک گرگوروایز، جی (۱۳۸۲). تکنولوژی: مطالعات فرهنگی و فناوری. ترجمه علی کسمایی رسانه، ۵۳، ۹۳-۱۱۳.
- Beck, U. (2006). *La sociedad del riesgo: Hacia una nueva modernidad* [The risk society: Towards a new modernity] (J. Navarro Perez, D. Jimenez, & M. R. Borrás, Trans.). Paidós.
- Belamire, J. (2016). My first virtual reality groping. *Athena Talks*, 20, 1190. Retrieved from <https://medium.com/athena-talks/my-first-virtual-reality-sexual-assault-2330410b62ee>.
- Bublitz, J. C. (2022). Novel neurorights: From nonsense to substance. *Neuroethics*, 15(1), 7. doi: 10.1007/s12152-022-09481-3.
- Bublitz, J. C., & Merkel, R. (2014). Crimes against minds: On mental manipulations, harms and a human right to mental self-determination. *Criminal Law and Philosophy*, 8, 51-77. doi: 10.1007/s11572-012-9172-y.
- Castro, D. (2022). Content moderation in multi-user immersive experiences: AR/VR and the future of online speech. Information Technology and Innovation Foundation. Retrieved from <https://itif.org/publications/2022/02/28/content-moderation-multi-user-immersive-experiences-arvr-and-future-online/>
- Council of Europe. (2001). Budapest convention on cybercrime. European Treaty Series No. 185. Retrieved from <https://rm.coe.int/1680081561>
- Diniz Bernardo, P., Bains, A., Westwood, S., & Mograbi, D. C. (2021). Mood induction using virtual reality: A systematic review of recent findings. *Journal of Technology in Behavioral Science*, 6, 3-24. doi: 10.1007/s41347-020-00152-9.
- Goering, S., Klein, E., Specker Sullivan, L., Wexler, A., Agüera y Arcas, B., & Yuste, R. (2021). Recommendations for responsible development and application of neurotechnologies. *Neuroethics*, 14(3), 365-386. doi: 10.1007/s12152-021-09468-6

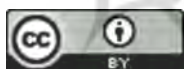
- Gonzalez-Tapia, M. I. (2023). Virtual emotions and criminal law. *Frontiers in Psychology*, 14, 1260425. doi: 10.1007/s41347-020-00152-9.
- Harari, Y. N. (2018). 21 Lessons for the 21st Century (1st Edn.). New York: Spiegel & Grau.
- Heller, B. (2020). Reimagining reality: Human rights and immersive technology. Harvard Carr Center Discussion Paper Series. Retrieved from <https://carrcenter.hks.harvard.edu/publications/reimagining-reality-human-rights-and-immersive-technology>
- Heller, B., & Bar-Zeev, A. (2021). The problems with immersive advertising: In AR/VR, nobody knows you are an ad. *Journal of Online Trust and Safety*, 1(1). doi: 10.54501/jots.v1i1.21
- Hermann, E. (2022). Artificial intelligence and mass personalization of communication content—An ethical and literacy perspective. *New media & society*, 24(5), 1258–1277. doi: 10.1177/14614448211022702
- Huynh-The, T., Pham, Q. V., Pham, X. Q., Nguyen, T. T., Han, Z., & Kim, D. S. (2022). Artificial intelligence for the metaverse: A survey. *Engineering Applications of Artificial Intelligence*, 117, 105581. Available from <http://arxiv.org/abs/2202.10336>.
- Ienca, M., Fins, J. J., Jox, R. J., Jotterand, F., Voienky, S., Andorno, R., ... & Kellmeyer, P. (2022). Towards a governance framework for brain data. *Neuroethics*, 15(2), 201. doi: 10.1007/s12152-022-09498-8
- Ligthart, S., Ienca, M., Meynen, G., Molnar-Gabor, F., Andorno, R., Bublit, C., & Kellmeyer, P. (2023). Minding rights: Mapping ethical and legal foundations of 'neurorights'. *Cambridge quarterly of healthcare ethics*, 32(4), 461–481. doi: 10.48550/arXiv.2302.06281
- Mann, S., Havens, C., Iorio, J., Yu, Y., Yuan, & Furness, T. (2018). All reality: Values, taxonomy, and continuum, for virtual, augmented, eXtended/MiXed (X), mediated (X, Y), and multimediated reality/intelligence. In *Presented at the AWE 2018*.
- Mythen, G. (2017). *Understanding the risk society: Crime, security and justice*. Bloomsbury Publishing.
- Peckmann, C., Kannen, K., Pensel, M. C., Lux, S., Philipsen, A., & Braun, N. (2022). Virtual reality induces symptoms of depersonalization and derealization: A longitudinal randomised control trial. *Computers in Human Behavior*, 131, 107233. <https://doi.org/10.1016/j.chb.2022.107233>
- Qamar, S., Anwar, Z., & Afzal, M. (2023). A systematic threat analysis and defense strategies for the metaverse and extended reality systems. *Computers & Security*, 128, 103127. <https://doi.org/10.1016/j.cose.2023.103127>
- Riva, G., Wiederhold, B. K., & Mantovani, F. (2019). Neuroscience of virtual reality: From virtual exposure to embodied medicine. *Cyberpsychology, Behavior, and Social Networking*, 22(1), 82–96. <https://doi.org/10.1089/cyber.2017.29099.gri>

- Rosenberg, R. S., Baughman, S. L., & Bailenson, J. N. (2013). Virtual superheroes: Using superpowers in virtual reality to encourage prosocial behavior. *PloS One*, 8(1), e55003.
<https://doi.org/10.1371/journal.pone.0055003>
- Russo, V., Bilucaglia, M., & Zito, M. (2022). From virtual reality to augmented reality: A neuromarketing perspective. *Frontiers in Psychology*, 13, 965499. <https://doi.org/10.3389/fpsyg.2022.965499>
- Savage, N. (2019). How AI and neuroscience drive each other forwards. *Nature*, 571(7766), S15–S15. doi: 10.1038/d41586-019-02212-4
- Silva Sanchez, J.-M. (2001). *The expansion of criminal law: Aspects of criminal policy in post-industrial societies* (2nd ed.). Civitas.
- Slater, M. (2009). Place illusion and plausibility can lead to realistic behaviour in immersive virtual environments. *Philosophical Transactions of the Royal Society B: Biological Sciences*, 364(1535), 3549–3557. doi: 10.1098/rstb.2009.0138
- Slater, M., Gonzalez-Liencre, C., Haggard, P., Vinkers, C., Gregory-Clarke, R., Jelley, S., & Silver, J. (2020). The ethics of realism in virtual and augmented reality. *Frontiers in Virtual Reality*, 1, 512449.
<https://doi.org/10.3389/frvir.2020.00001>. doi: 10.3389/frvir.2020.00001
- UNESCO, University of Milan-Bicocca (Italy), State University of New York (SUNY) Downstate Health Sciences University. (2023). *The risks and challenges of neurotechnologies for human rights*.
- Vincent, N. A., Nadelhoffer, T., & McCay, A. (Eds.). (2020). *Neurointerventions and the law: Regulating human mental capacity*. Oxford University Press.
- Vondracek, M., Baggili, I., Casey, P., & Mekni, M. (2023). Rise of the metaverse's immersive virtual reality malware and the man-in-the-room attack & defenses. *Computers & Security*, 127, 102923.
<https://doi.org/10.1016/j.cose.2022.102923>
- Zuboff, S. (2023). The age of surveillance capitalism. In *Social theory re-wired* (pp. 203–213). Routledge.
- [In Persisn]**
- Daryl Slack, J., McGregor (2003), Technology: Cultural Studies and Technology, Wise, Translator: Ali Kasmaii, *Journal Media*, 53, 93-113
- Ghasemi, M. A. (2009). Risk society and its importance for strategic studies. *Journal Strategic Studies*, 12(45), , 27–46.
- Hakimpour, Y. (2023). From Algorithms to Deep Learning: What We Should Know About Artificial Intelligence. *Journal Auditor*, 123, 50–53.

- Hassanzadeh, M., & Hosseini, S. M. (2010). Web accessibility: Concepts and applications. *Journal Rahyaft*, 20(46), 33–44.
- Heidari, A. M., & Jafari, A. (2010). Criminal Protection of Visual and Auditory Media. *Journal Media*, 82(2), 87-110.
- Mousavi Mojab, S. D., & Rafiezadeh, A. (2015). The scope of criminal liability of legal entities in the Islamic Penal Code. *Criminal Law Research Quarterly*, 4(13), 147–169.
- Shahriari, H. (2011). Religion, Culture, and Information Technology: Advantages and Challenges of Virtual Identity in Cyberspace. *Rahavard-e Noor*, 35(10), 2-7.
- Tahmasbi, J., & Shahmoradi, K. (2018). Challenges and Existing Gaps in the Cyber Crime Investigation Process. *Legal Journal of Justice*, 82(104), 95-121. <https://doi.org/10.22106/rlj.2018.34680>
- Tisheyar, M., & Pazoki Zadeh, Z. (2010). Web writing and the public sphere in Iran. *Journal Media*, 82(2), 111–126.

COPYRIGHTS

©2025 by the authors. Published by University of Science and Culture. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution 4.0 International (CC BY 4.0) <https://creativecommons.org/licenses/by/4.0/>



پژوهشگاه علوم انسانی و مطالعات فرهنگی
پرتال جامع علوم انسانی