مبانی جرم‌انگاری جرایم سایبری مجازی

افسانه زمانی جباری[1]* و امین پژوهش جهرمی[2]

[1]جانشین معاون دادستان دادسرای عمومی و انقلاب شیراز؛ و دانشجوی دکترای حقوق کیفری و جرم‌شناسی دانشگاه تربیت مدرس؛
afsaneh.s.zamani@gmail.com

[2]استادیار دانشگاه صنعتی مالک‌اشتر؛ تهران، ایران
amin.pazhouhesh@gmail.com

چکیده

هدف مقاله حاضر، پاسخ به این پرسش است که جرایم سایبری مجازی چگونه در قلمرو حقوق جزا قرار گرفته و بر اساس چه مبانی و شرایطی جرم‌انگاری می‌شوند. با وجود رقم پرشمار حضور کاربران اینترنت در دنیاهای مجازی، پژوهش‌های محدودی به‌ویژه در مورد کیفیت ارتکاب، گستره و شمول، هویت مجرمان و بزه‌دیدگان و نیز پیامدهای ناشی از وقوع جرایم سایبری مجازی انجام شده است. پژوهش حاضر با بهره‌گیری از هستی‌شناسی فلسفی و هم‌چنین فلسفه حقوق، به تبیین شرایط لازم و کافی برای قرارگرفتن جرایم سایبری مجازی در زیرمجموعه حقوق جزا پرداخته و نتیجه می‌گیرد شرط لازم برای آن که کنش سایبری مجازی به‌عنوان یک جرم، زیرمجموعه قوانین کیفری قرار گیرد، حصول یک نتیجه و پیامد فرامجازی است و شرط کافی آن است که نتیجه چنین ماهیتی، مداخله در آزادی شهروندان را با استفاده از قانون مجازات بر اساس یکی از اصول محدود کننده آزادی فینبرگ توجیه کند.

واژگان کلیدی: جرایم سایبری مجازی، مبانی جرم‌انگاری

۱- مقدمه

ظهور فناوری رایانه، ارتکاب انواع جرایم جدیدی را موجب شده است، جرایم سایبری[1]، جرایمی است که مجرم با استفاده از رایانه و شبکه‌های رایانه‌ای اقدام به جرم می‌کند. نمونه‌هایی از جرایم سایبری عبارتند از: انتشار بدافزارهای رایانه‌ای، کلاه‌برداری الکترونیک[2] و انتشار هرزه‌نگاری کودکان با استفاده از اینترنت. جدیدترین نسل جرایم سایبری، جرایم سایبری مجازی[3] است که شامل جنبه خاصی از رایانه‌ها و یا شبکه‌های رایانه‌ای است؛ مجازی‌بودن، مواردی همچون هرزه‌نگاری کودکانِ مجازی (که دربرگیرنده عکس و یا فیلم هرز از کودکان واقعی نیست، بلکه شامل تصاویر شبیه‌سازی شده رایانه‌ای از کودکان مجازی است)، سرقت اشیای مجازی و یا قتل در فضای مجازی. اما درواقع رفتارهایی همانند ربودن اشیای مجازی و کشتن آواتار (چهرک)[4] در دنیای مجازی به‌عنوان جنایت و زیرمجموعه حقوق جزا قرار می‌گیرند؟ بخشی از مقاومت قانون‌گذاران کیفری برای پاسخ به این پرسش و ورود به حوزهٔ مجازی، ناشی از رویکرد عینیت‌گرایی در اندیشه‌های حقوق کیفری در شناخت و تشخیص جرایم است. رفتار مجرمانه (کنش فیزیکی)، ارتباط بین مکان‌های فیزیکی (محل‌های وقوع جرم) و تأثیر جرایم ارتکابی بر بزه‌دیده (افراد واقعی) عوامل مورد نظر قانون‌گذار در جرایم سنتی است [۱]. برای مثال جرم قتل، سلب حیات یک فرد حقیقی نه یک آواتار است. هم‌چنین تعرض به فرد مجازی همانند تعرض به فرد حقیقی در جرایم سنتی نیست؛ زیرا در حوزه جرایم سنتی، فرد حقیقی به‌لحاظ فیزیکی مورد تعرض و صدمه قرار می‌گیرد؛ اما تجاوز مجازی، تعرض واقعی نیست و یک فرد حقیقی از لحاظ جسمی مورد تجاوز قرار نمی‌گیرد، بلکه تصویر یا نمایشی از تعرض در فضای مجازی است. هم‌چنین جرم ورود غیرمجاز در حقوق کیفری سنتی، نیازمند ورود فیزیکی فرد حقیقی به مکان فیزیکی است و با ورود آواتار مجازی به فضای مجازی متفاوت خواهد بود. بدین دلیل، مفهوم «ورود» در فضای مجازی با معیارهای شناسایی این جرم در قلمرو حقوق کیفری سنتی، چندان قابل فهم و تحلیل نیست. معنای رفتار مجازی در دنیای مجازی برای بیش‌تر قوانین

[1] Cybercrime
[2] E-fraud
[3] Virtual cybercrime
[4] Λvater یا چهرک

*نویسندهٔ مسؤول

جزایی، نامربوط و نامأنوس است (البته نه آن بخش از جرایم سنتی که از طریق ابزارهای سایبری تحقق می‌یابند). اما واقعیت آن است که همین رفتارها در دنیای مجازی که تا کمتر از یک دهه پیش، به‌عنوان «بازی» به‌شمار می‌رفت، هم‌اکنون با توسعه قابلیت‌های فناوری و حضور میلیون‌ها نفر کاربر در آن (با آزادی عمل کاربران برای برقراری ارتباط و تحقق رؤیاهای دور از دسترس در دنیای واقعی)، تبدیل به زیست مجازی در جهانی به موازات جهان واقعی شده است؛ جهانی که میلیون‌ها نفر در آن زندگی، کار و ثروت‌اندوزی می‌کنند؛ و حتی مرتکب جرم می‌شوند. آماده‌شدن نظام‌های حقوقی برای رویارویی با مسایل این دنیای مجازی، هم‌چنین تجهیز به سلاح دانش و پیش‌بینی ضمانت اجراهای لازم برای حفظ حقوق اشخاص، ضرورتی است که حتی اگر همین امروز نیز بدان پرداخته شود، کمی دیر است.

با وجود فعالیت صدها میلیون کاربر در دنیاهای مجازی همانند دنیای مجازی «زندگی دوم[1]»[2]، پژوهش‌های محدودی به‌ویژه در مورد کیفیت ارتکاب، گستره و شمول، هویت مجرمان و بزه‌دیدگان و نیز پیامدهای ناشی از وقوع جرایم سایبری مجازی انجام شده است که از آن‌جمله می‌توان به موارد زیر اشاره کرد:

کِر در مقاله خود با عنوان «حقوق جزا در دنیای مجازی» [۱] به دو پرسش توصیفی و هنجاری می‌پردازد: چه وقت رفتار یک فرد در دنیای مجازی موجب مسئولیت کیفری می‌شود؟ و آیا وضع قوانین جزایی جدید برای مقابله با آسیب‌های وارده به افراد در دنیای مجازی ضروری است؟ نویسنده بیان می‌کند که قوانین جزایی موجود به‌علت اتکا بر درک دنیای فیزیکی (و نه مجازی)، توجه چندانی به جرایم سایبری مجازی ندارند و مواردی مثل قتل مجازی، تهدیدهای مجازی و یا سرقت مجازی را به رسمیت نمی‌شناسند. کِر، تلاش برای معرفی اهمیت این دنیای جدید به قانون‌گذاران و وضع یا توسعه قوانین کیفری را ضروری می‌داند. استریکوردا در مقاله‌اش با عنوان «صلاحیت دادگاه در جرایم ارتکابی دنیای مجازی» [۲] به ضرورت بررسی جرایم سایبری مجازی (همچون سرقت اشیای مجازی، قتل آواتار یا تولید و توزیع هرزه‌نگاری کودکان مجازی) با استفاده از قانون جزا پرداخته و این موضوع را دارای دست‌کم چهار بعد فلسفی، حقوقی-اقتصادی، عملی، و قانونی[3] می‌داند. در مقاله یادشده، هر یک از این ابعاد مورد مطالعه قرار گرفته و بر اساس تحلیل انجام‌شده، معیارهایی برای جرم‌انگاری جرایم سایبری مجازی ارائه می‌دهد. استریکوردا در مقاله دیگری با عنوان «سرقت اشیای مجازی در بازی‌های چندنفرهٔ رایانه‌ای برخط: تحلیل هستی شناختی و اخلاقی» [۳] با اشاره به پرونده سرقت اشیای مجازی در دنیای مجازی چندنفره بازی‌های رایانه‌ای برخط در هلند و صدور حکم برای آن، به این پرسش می‌پردازد که آیا اشیای مجازی باید به‌عنوان "شیء" در نظر گرفته شوند تا سرقت آن‌ها به‌عنوان جرم تلقی شده و قابلیت رسیدگی در حقوق کیفری داشته باشد. پژوهش‌گر این پرسش را دارای دو جنبه هستی‌شناسانه و اخلاقی می‌داند. درواقع این بخش از پرسش که آیا اشیای مجازی به‌عنوان «شیء» محسوب شوند تا بتوانند «سرقت شوند» یک سؤال هستی‌شناختی است و بخش دیگر پرسش که آیا باید تحت شمول قانون جزا قرار بگیرند، یک سؤال اخلاقی است. شائن‌گولد در مقاله‌اش با عنوان «صلاحیت شخصی دادگاه در جرایم ارتکابی در دنیای مجازی» [۴]، ضمن پرداختن به موضوع تجاوز به عنف در دنیای مجازی، چنین بیان می‌کند که مسایلی نظیر تجاوز، حمله، آزار عاطفی، افترا، اختلافات ناشی از قرارداد و حتی حقوق مالکیت در دنیای مجازی فاقد عناصر لازم برای اقامه دعوا در دادگاه‌های آمریکا است؛ اما استدلال می‌کند که با این وجود، آسیب‌های واقعی وارده به بزه‌دیده، قابلیت طرح دعوا دارند. رامبلز در مقاله خود با عنوان «دزدی عصر دیجیتال؛ آیا می‌توان اموال مجازی را به سرقت برد» [۵]، به بررسی مسایل درخصوص سرقت اموال مجازی پرداخته و برای درک اهمیت توسعه حقوق کیفری و مسئولیت کیفری از «دنیای واقعی» به «دنیای مجازی» استدلال‌هایی ارایه می‌دهد. مقاله یادشده ضمن تمرکز بر سرقت اموال مجازی و بررسی نحوه برخورد نظام‌های قضایی با این موضوع، قوانین کیفری «دنیای واقعی» نیوزیلند و به‌کارگیری این قوانین به حوزه اموال مجازی را بررسی می‌کند. گوریندو و گروز در مقالهٔشان با عنوان «جنایت و نفرت در دنیاهای مجازی» [۶] به این واقعیت می‌پردازند که دنیاهای مجازی سه‌بعدی، جمعیتی بیش از خیلی از کشورهای دنیا را شامل می‌شوند که بروز تمامی فعالیت‌های ممکن در یک کشور از جمله بروز انواع جرایم در آن محتمل است؛ جرایمی همانند سرقت، تجاوز، قتل و آزار جنسی کودکان. درضمن نویسندگان یادشده مدلی برای فهم انگیزه‌های مجرمان و چگونگی تفکر این افراد از جرم در دنیای مجازی ارایه می‌دهند. گین‌چارد

[1] Second life

[2] Gartner, Inc. Gartner says 80 percent of active Internet users will have a "Second Life" in the virtual world by the end of 2011, 2011, http://www.gartner.com/it/page.jsp?-id=503861

[3] constitutional dimension

در مقالهٔ خود با عنوان «جرم در دنیای مجازی؛ محدودیت‌های قانون جزا» [۷] با این استدلال که دنیاهای مجازی مصون از بروز و تحقق جرم نیستند و کاربران در این دنیاها می‌توانند رفتارهایی همانند صدمه به اموال مجازی و یا کنترل آواتار کاربران دیگر را انجام دهند، تلاش می‌کند تا بخشی از این رفتارها را در حوزه جرایم رایانه‌ای (تحت عنوان دسترسی‌های غیرمجاز یا تخریب اطلاعات رایانه‌ای) قرار دهد. وارن و پالمر [۸] در مقالهٔشان با عنوان «ریسک‌های جرم در محیط‌های مجازی سه‌بعدی» ضمن بررسی چند نمونه از انواع جرایم در دنیای سایبری مجازی، راه‌کارهایی برای پیشگیری از جرایم سایبری مجازی ارائه می‌دهد: وضع قوانین داخلی توسط شرکت‌های ایجادکننده دنیاهای مجازی؛ اطلاع‌رسانی به کاربران درباره شرایط استفاده از خدمات و یا موافقت‌نامه صدور مجوز کاربر نهایی؛ و هشداردهی (مبنی بر این که برخی اقدامات انجام‌شده در این دنیای مجازی ممکن است افزون بر مجازات‌های سایبری، پیامدهای حقوقی واقعی نیز به دنبال داشته باشد). برینر[۹] در مقاله‌ای با عنوان «جرم فانتزی؛ نقش حقوق جزا در دنیای مجازی»، ضمن تحلیل انواع فعالیت‌ها در دنیای مجازی از جمله فعالیت مجرمانه، با بررسی تاریخچه تکامل دنیای مجازی و افزایش روافزون حضور افراد در دنیای مجازی، این دنیا را تحقق زندگی دوم دانسته و نتیجه می‌گیرد بشر بخش زیادی از وقتش را در آینده در این دنیا سپری خواهد کرد. نویسنده در ادامه به تحلیل شرایط جرم‌انگاری رفتارهای مجازی که منجر به «ضرر» در دنیای واقعی شده و رفتارهای مجازی را که تنها در دنیای مجازی «ضرر» به دنبال دارد، تحلیل می‌کند؛ بدین صورت که دستهٔ نخست را واجد شرایط جرم‌انگاری به‌عنوان جرایم اینترنتی دانسته که می‌توانند تحت شمول قوانین کیفری قرار بگیرند و درخصوص دسته دوم به ضرورت جرم‌انگاری این رفتارها اشاره می‌کند. گودمن و برینر در [۱۰] «شکل‌گیری اجماع در درک رفتار مجرمانه در فضای سایبری» ضمن بیان علل نگرانی و دغدغه‌های جهانی درباره رفتارهای مجرمانه در دنیای سایبری، به اقدامات مورد نیاز در سطح ملی و بین‌المللی برای درک مشترک و شکل‌گیری اجماع در این باره می‌پردازد. کیتال در [۱۱] با مروری بر جرایم سایبری مجازی، معتقد است جهان در هزاره جدید، شاهد جرایم جدید (حتی بیش از آن‌چه تاکنون در عرصه مجازی رخ داده) خواهد بود که علت اصلی آن وقوع تغییرات عمده در زمینه ارتکاب جرم با حرکت از جرایم واقعی به سوی جرایم مجازی است. نویسنده مقاله ضمن نامتناسب دانستن قوانین موجود با عصر دیجیتال، بر ضرورت درک پارادایم فکری جدید قانون‌گذاری تأکید می‌کند.

نگارندگان مقالهٔ حاضر نیز با بهره‌گیری از هستی‌شناسی فلسفی و هم‌چنین فلسفه حقوق مبتنی بر ادبیات نظری موجود، به تبیین شرایط لازم و کافی برای قرارگیری جرایم سایبری مجازی در شمول حقوق کیفری پرداخته و امیدوارند پژوهش حاضر بتواند ضمن ارایه اطلاعات جدیدی از کیفیت، گستره، و پیامدهای جرایم این حوزه، پایه‌ای برای پژوهش‌های بیش‌تر باشد.

۲- روش پژوهش

این پژوهش از نظر هدف، کاربردی، از نظر نوع، کیفی و با توجه نحوه گردآوری داده‌ها، کتابخانه‌ای (مطالعات ثانویه از نوع فراتحلیل) و مبتنی بر مطالعه منابع اطلاعاتی برخط خارجی همچون ساینس‌دایرکت[۱]، اسپرینگر[۲]، جان‌وایلی[۳]، آی‌تریپل‌ایی[۴]، و تیلور و فرانسیس[۵] بدون درنظرگرفتن قید زمانی تهیه شده است (گفتنی است به منابع برخط داخلی همچون بانک جامع مقالات کنفرانس و همایش‌های سیویلیکا[۶]، مرکز اطلاعات علمی برخط جهاد دانشگاهی[۷]، پایگاه مجلات تخصصی نور[۸]، سامانه نشر مجلات علمی *دانشگاه تهران*[۹]، پایگاه مطبوعات ایران[۱۰]، پژوهشگاه علوم و فناوری اطلاعات *ایران*[۱۱] نیز مراجعه شد اما داده‌ای به دست نیامد). پژوهش حاضر در دو مرحله انجام و در سه بخش ارائه شده است:

- مطالعات نظری: جرایم سایبری مجازی چیستند و چگونه در نظام‌های قانونی موجود بررسی می‌شوند؟. در این بخش، ابتدا تعریفی از «جرایم سایبری مجازی» ارائه شده و محدوده آن تعیین می‌شود.
- تحلیل هستی‌شناختی: شرایط لازم و کافی برای آنکه جرایم سایبری مجازی به‌عنوان جرم زیرمجموعه قوانین موجود قرار گیرند، کدامند؟. در این بخش تلاش می‌شود (بر اساس منابع) موجود نشان داده شود که جرایم سایبری مجازی توانایی ایجاد ضررهای فرامجازی را دارند.

[1] www.sciencedirect.com
[2] Link.springer.com
[3] Onlinelibrary.wiley.com
[4] Ieeexplore.ieee.org
[5] www.tandfonline.com
[6] www.civilica.com
[7] www.SID.ir
[8] www.noormags.com
[9] journal.ut.ac.ir
[10] www.magiran.com
[11] www.irandoc.ac.ir

- در بخش سوم، شرایط لازم و کافی برای این که جرایم سایبری مجازی به‌عنوان یک جرم زیرمجموعه قوانین موجود قرار گیرند، بررسی می‌شود.

۳- جرایم سایبری

جرم، به‌طورکلی به آن دسته از رفتارهای انسانی اطلاق می‌شود که توسط قانون ممنوع شده باشد. پیشوند «سایبری» اشاره به استفاده از رایانه یا شبکه‌های رایانه‌ای دارد؛ «رایانه-واسط[1]» [۹]. درنتیجه، جرایم سایبری شامل هر عمل محرمانهٔ انسانی با استفاده از رایانه است که توسط قانون ممنوع شده باشد. جرایم سایبری، جرایمی جدید و چالش‌ساز هستند؛ زیرا استفاده از رایانه و شبکه‌های رایانه‌ای امکان انجام «اشکال جدید و متفاوت از فعالیت انسانی را فراهم می‌سازند که گاه در محدوده قانون مجازات موجود قرار نمی‌گیرند» [۱۰]. از یک سو، استفاده از رایانه و شبکه‌های رایانه‌ای، گونه‌های جدید فعالیت‌های انسانی ضد اجتماعی را ممکن می‌سازند که پیش از ظهور رایانه و شبکه‌های رایانه‌ای امکان‌پذیر نبودند؛ به‌عنوان مثال گسترش بدافزارهای رایانه‌ای [۱۲]. از سوی دیگر، رایانه و شبکه‌های رایانه‌ای می‌توانند به‌عنوان ابزاری برای ارتکاب جرایم سنتی، همانند کلاه‌برداری[2] مورد استفاده قرار گیرند. به همین دلیل ضروری است قانون‌گذاران مُدام به بررسی و تعیین ممنوعیت یا جواز اشکال جدید و متفاوت فعالیت‌های انسانی (که با استفاده از رایانه و شبکه‌های رایانه‌ای ارتکاب می‌یابد)، بپردازند و در این راه ناگزیر به تصویب قوانین و مقررات و ضمانت اجراهای جدید هستند. این که کدام‌یک از اشکال جدید و متفاوت رفتارهای انسانی، با ممنوعیت قانونی و یا سایر ضمانت اجراها مواجه شود با توجه به نوع نظام‌های حقوقی مختلف، تغییر می‌کند، با این وجود، اشتراکاتی نیز وجود دارد [۱۰].

آشناترین ابتکار عمل بین‌المللی برای توسعه قلمرو کیفری به حوزه جرایم سایبری، کنوانسیون جرایم سایبری[3] است که توسط تعداد زیادی از کشورهای عضو اتحادیه اروپا و برخی کشورهای دیگر، از جمله ایالات متحده آمریکا و ژاپن به تصویب رسیده است. این کنوانسیون ۹ نوع رفتار جدید و متفاوت انسانی در استفاده از رایانه و یا شبکه‌های رایانه‌ای را تعریف می‌کند. پنج دسته نخست عبارتند از: دسترسی غیرقانونی[4]، ممانعت غیرقانونی[5]، تداخل داده‌ها[6]، دخالت سیستم[7] و سوءاستفاده از دستگاه[8]. این جرایم با اشکال جدید فعالیت‌های انسانی در ارتباط هستند که پیش از ظهور رایانه و شبکه‌های رایانه‌ای وجود نداشتند. آن‌ها را می‌توان تحت عنوان «جرایم رایانه‌ای[9]» نیز طبقه‌بندی کرد. چهار دسته جرم بعدی عبارتند از: جعل رایانه‌ای[10]؛ کلاه‌برداری رایانه‌ای[11]؛ جرایم مربوط به هرزه‌نگاری کودک؛ و جرایم مربوط به نقض مالکیت فکری و حقوق مرتبط. موارد یادشده، درحقیقت به نوعی همان جرایم سنتی هستند که از رایانه و شبکه‌های رایانه‌ای به‌عنوان ابزاری برای ارتکاب جرم استفاده می‌شود. هم‌چنین این دسته از جرایم را می‌توان تحت عنوان «جرایم تسهیل‌شده با رایانه[12]» نیز طبقه‌بندی کرد [۱۳].

۴- واژه «مجازی»

صفت «مجازی» در دو معنای پیشارایانه (پیش از دوران رایانه) و رایانه‌پایه به‌کار می‌رود. در معنای سنتی پیشارایانه، «مجازی» دارای دو معنا است: نخست به معنای «شبه[13]»؛ و دوم به معنای «خیالی»، «افسانه[14]» و یا «جعلی[15]». در مورد معنای مبتنی بر رایانه، اصطلاح «مجازی» می‌تواند به «هر چیزی اشاره داشته باشد که توسط یک رایانه ایجاد و یا انجام شده و شبیه یک «هویت» واقعی است. به‌عنوان مثال، حافظه مجازی. این حافظه یک شبیه‌سازی رایانه‌ای از حافظه فیزیکی است که می‌تواند به همان اندازه حافظه واقعی کارآمد باشد [۱۴]. اصطلاح «مجازی» می‌تواند متضمن مفهوم «دنیای مجازی» نیز باشد. دنیای مجازی یک محیط رایانه‌ای شبیه‌سازی‌شدهٔ تعاملی است که توسط کاربران متعدد در یک زمان در دسترس است. نخستین دنیای مجازی در اواخر دهه ۱۹۷۰ ارائه شد که بازی‌های مبتنی بر متن رایانه‌ای برخط بودند. از اواسط دهه ۱۹۸۰، افزایش سرعت دسترسی به اینترنت و بهبود قدرت پردازش رایانه، امکان گرافیک پیچیده‌تر سه‌بعدی را فراهم ساخت و

[1] Computer-mediated
[2] Fraud
[3] Convention on Cybercrime

[4] Illegal access
[5] Illegal interception
[6] Data interference
[7] System interference
[8] Misuse of devices
[9] Computer crime
[10] Computer-related forgery
[11] Computer-related fraud
[12] Computer-facilitated crime
[13] Quasi or Pseudo
[14] Make-believe
[15] Fake

درنتیجه دنیای مجازی سه‌بعدی (دنیای مجازی گرافیکی) با ارایه «یک نسخه واقعیت افزوده[1]» تحقق یافت [۱۵]. حضور کاربران در این دنیای مجازی از طریق آواتار[2] (یک انسان گرافیکی سه‌بعدی) امکان‌پذیر می‌شود. کاربران از طریق آواتارهای‌شان، با یکدیگر و با اشیای مجازی تعامل می‌کنند. درنهایت، اصطلاح «مجازی» را می‌توان برای «واقعیت مجازی[3]» استفاده کرد. واقعیت مجازی شامل محیط شبیه‌سازی‌شدهٔ رایانه‌ای تعاملی با تصاویر سه‌بعدی است. ویژگی واقعیت مجازی آن است که در آن کاربران محیط‌شان را از طریق «آواتار» تجربه نمی‌کنند، بلکه از طریق چشم و حواس دیگرشان درک می‌کنند. واقعیت مجازی برای به‌کارگیری حواس انسان، به‌منظور تولید همان حسی که در محیط واقعی تولید می‌شود، طراحی شده‌اند [۱۶]. این سامانه مشتمل بر صفحه نمایش نصب‌شونده بر سر و یک دستکش داده‌ای[4] یا لباس داده‌ای[5] متصل به رایانه است. هم‌زمان که کاربر با محیط شبیه‌سازی‌شدهٔ رایانه‌ای تعامل می‌کند، از صفحه نمایش، تصاویر سه‌بعدی دریافت کرده و از طریق دستکش داده‌ای یا لباس داده‌ای بازخورد حسی (همانند حس مقاومت زمان گرفتن شیء) می‌گیرد [۱۴]. فناوری واقعیت مجازی برای شبیه‌سازی محیط واقعی نیز استفاده می‌شود؛ به‌عنوان مثال در پزشکی، برای شبیه‌سازی ساختار آناتومیک و آموزش جراحان [۱۴]. «شبیه‌سازی رایانه‌ای» و «تعامل»، جوهر معنایی واژه «مجازی» است که مد نظر این مقاله است.

۵- جرایم سایبری مجازی

با استفاده از تعریف یادشده از اصطلاح مجازی، «جرایم سایبری مجازی» را می‌توان به‌عنوان «جرایم سایبری‌ای» تعریف کرد که از طریق استفاده از یکی از ویژگی‌های خاص رایانه و شبکه‌های رایانه‌ای، یعنی شبیه‌سازی رایانه‌ای صورت می‌پذیرد. درنتیجه جرایم سایبری مجازی شامل ممنوعیت «رفتار انسانی شبیه‌سازی‌شده رایانه‌ای[6]» یا «رفتار انسانی که توسط شبیه‌سازی رایانه‌ای امکان‌پذیرشده[7]» است. درک تمایز بین این دو رفتار، واجد اهمیت است:

نوع نخست، عملی است که به خودی خود مجازی است. درواقع «رفتار شبیه‌سازی‌شده رایانه‌ای» در محیط مجازی از طریق دستگاه ورودی به رایانه تحقق می‌یابد. نمونه‌ای از آن، بازی «پرندگان خشمگین» است. این عمل انسانی شبیه‌سازی‌شده رایانه‌ای شامل سه مرحله است: مرحلهٔ نخست، انجام یک عمل جسمانی توسط یک انسان. به‌عنوان مثال؛ فشاردادن یک دکمه؛ مرحله دوم، شبیه‌سازی رایانه‌ای (رایانه، عمل جسمانی را به‌عنوان دستور خاص تفسیر می‌کند-به‌عنوان مثال پرتاب پرنده)؛ و مرحله سوم، تغییرات در محیط مجازی (یا در فضای غیرمجازی) که مورد نظر آن فرمان است. برای مثال؛ خراب شدن بلوک‌های چیده شده روی هم.

نوع دوم (رفتار انسانی که توسط شبیه‌سازی رایانه‌ای امکان‌پذیر شده)، عملی است که به خودی خود مجازی نیست؛ اما برحسب یک جسم مجازی تعریف می‌شود. شبیه‌سازی رایانه‌ای، شرط امکان‌پذیری چنین عملی است و ماهیت آن رفتار، با توجه به ویژگی‌های شبیه‌سازی رایانه‌ای تعیین می‌شود [۱۵]. تولید، نگهداری یا توزیع تصاویر یا فیلم هرزه‌نگاری کودکان مجازی[8]، نمونه‌ای از رفتار انسانی است که توسط شبیه‌سازی رایانه امکان‌پذیر شده است. اعمال مرتبط با هرزه‌نگاری کودکان مجازی، به خودی خود مجازی نیست؛ اما بر پایه یک موضوع مجازی (کودکان مجازی) تعریف می‌شود. تصاویر هرزه‌نگاری کودکان مجازی، تصاویر کودکانی است که (اگر چه واقعی به نظر می‌رسد)، اما یک کودک واقعی در این رفتار هرزه‌نگاری درگیر نیست. آن‌ها یا تصاویر و عکس‌های مورف[9] شده کودکان واقعی هستند و یا تصاویری هستند که به‌طور کامل به‌وسیلهٔ رایانه تولید شده‌اند؛ درنتیجه ساخت تصاویر هرزه‌نگاری کودک مجازی توسط شبیه‌سازی رایانه ممکن می‌شود. آن‌گونه که با تولید، توزیع و دراختیارداشتن تصاویر هرزه‌نگاری کودک غیرمجازی(کودک واقعی) مخالفت می‌شود، ماهیت رفتار تولید، توزیع و دراختیارداشتن تصاویر هرزه‌نگاری کودک مجازی (یا تصاویر مورف‌شده کودک واقعی) به آن علت که شامل بهره‌کشی از کودک نیست[10]، مورد ممنوعیت جدی قانون‌گذار قرار نگرفته است.

[1] Augmented version of reality
[2] Avatar
[3] Virtual reality
[4] Dataglove
[5] Datasuit
[6] Computer-simulated human act
[7] Human act made possible by computer simulation

[8] Virtual child pornography

[9] Morph: تبدیل تدریجی یک تصویر به تصویر دیگر

[10] کنوانسیون منع جرایم سایبری در حوزه پورنوگرافی کودکان، شامل تولید، نگهداری و توزیع پورنوگرافی کودکان مجازی نیز می‌شود. با این حال، ایسلند و اسکاتلند، حق منع‌نکردن پورنوگرافی مجازی کودکان را برای خود محفوظ داشته‌اند (کنوانسیون جرایم سایبری، ۲۰۰۱).

۶- امکان آسیب‌های فرامجازی از رفتارهای مجازی

شاید در نگاه نخست بعید به نظر برسد که عمل انسانی شبیه‌سازی‌شدهٔ رایانه‌ای یا عمل انسانی که با شبیه‌سازی رایانه‌ای امکان‌پذیر شده، بتواند منجر به آسیب فرامجازی (آسیب واقعی) شود، اما در ادامه نشان داده می‌شود این موضوع، چندان هم غیرمحتمل نیست. در سال ۲۰۰۹ قضات هلندی، چند نوجوان را به جرم سرقت اشیای مجازی در دنیای مجازی محکوم کردند. دراقع این چند نوجوان چند مبلمان مجازی را سرقت کرده بودند. استدلال قضایی آن بود که اموال مجازی ربوده شده با پول دارای ارزش فرامجازی (پول واقعی) خریداری شده بود، بنابراین دزدی آن، به منزله آسیب فرامجازی تلقی شد. در سال ۲۰۰۸ هکرها به درگاه اینترنتی بنیاد غیرانتفاعی صرع[1] نفوذ و پیامی به ظاهر رسمی منتشر کردند. کاربران با کلیک کردن این پیام به صفحه‌ای با انیمیشن رایانه‌ای منتقل می‌شدند که شامل الگوی مربعی با فلش نوری شدید در رنگ‌های مختلف بود و باعث تشنج در مبتلایان به صرع حساس به نور و حساس به الگو می‌شد[2]. تشنج حاصله در مبتلایان، ناشی از «عمل انسانی شبیه‌سازی‌شدهٔ رایانه‌ای» بود. عمل انسانی شبیه‌سازی‌شدهٔ رایانه‌ای یا عمل انسانی که توسط شبیه‌سازی رایانه امکان‌پذیرشده، می‌تواند جرایم مجازی خشن‌تری را نیز شامل شود. در سال ۲۰۰۸، پلیس ژاپن پرونده زنی را بررسی کرد که آواتاری را در دنیای مجازی می‌پل‌استوری[3] کشته بود[4]. درنتیجهٔ این رفتار، سلامت بدنی آواتار آسیب دیده بود[5].

برخی پژوهش‌گران استدلال می‌کنند که آسیب وارده از عمل انسانی شبیه‌سازی‌شدهٔ رایانه‌ای به سلامت بدنی آواتار، به معنای ایراد آسیب به سلامت مالک آواتار نیست [۱۷]، اما این سؤال مطرح می‌شود که آیا این رفتار (دست‌کم) نمی‌تواند منجر به ایراد آسیب به سلامت روانی مالک آواتار شود؟ زیرا یک فرد با ورود در فضای مجازی، از طریق آواتارش در این محیط شناسایی می‌شود، کسب هویت می‌کند و به تعاملاتی همچون ارتباطات اجتماعی و کسب درآمد می‌پردازد. آسیب بدنی وارده به آواتار می‌تواند به آسیب روحی مالک آن منجر شود [۱۸]. برای مثال، احساس فردی که آواتارش مورد تجاوز قرار گرفته، مانند آن است که خود او مورد آزار و اذیت قرار گرفته است. به‌عنوان مثال در سال ۲۰۰۶، هنگامی که آیلین گریف[6] (زنی که با سرمایه‌گذاری در یک بنگاه املاک مجازی در دنیای مجازی، ثروت زیادی کسب کرده بود)، زمانی که از طریق آواتارش در برنامه گفتگوی تلویزیونی دنیای مجازی برای صحبت در مورد موفقیتش حاضر شد، توسط آواتار کاربر دیگر مورد تعرض جنسی قرار گرفت. خانم گریف، افزون بر احساس تعرض به خودش، از آن‌جایی که هویت واقعی‌اش نیز برای بسیاری از کاربران شناخته شده بود، احساس می‌کرد که به آبرو و حیثیت وی نیز آسیب وارد شده است.

آسیب روحی به افراد نه‌تنها با اعمال انسانی شبیه‌سازی رایانه‌شده‌ای انجام می‌شود، بلکه با اعمال انسانی که توسط شبیه‌سازی رایانه‌ای امکان‌پذیر شده، نیز امکان‌پذیر است. به‌عنوان مثال، بسیاری از دنیاهای مجازی امکان گفتگو میان کاربران را فراهم می‌کنند. بنابراین مجرمان از طریق آواتارشان می‌توانند از این امکان برای ارسال پیام‌های نامناسب حاوی اذیت و آزار به کاربران دیگر سوءاستفاده کنند. باید اضافه کرد که اگر متن این پیام‌ها دربرگیرنده تهدید نیز باشد، نه‌تنها باعث ایراد آسیب به سلامت روانی قربانی می‌شود، بلکه می‌تواند کاهش امنیت قربانی را نیز به‌دنبال داشته باشد. درواقع آواتار فردی می‌تواند آواتار دیگری را در دنیای مجازی مورد زورگیری قرار دهد که این رفتار، همان عمل انسانی شبیه‌سازی‌شده رایانه‌ای است.

هم‌چنین از آن‌جایی که افراد در دنیای مجازی نیازمند کسب درآمد هستند، به‌عنوان مثال برخی افراد به خرید و فروش ملک و لباس می‌پردازند، و برخی نیز خدمات حفاظت شخصی مجازی ارائه می‌دهند، برخی نیز از طریق آواتارشان به ارایه و فروش سکس اقدام می‌کنند. همانند دنیای غیرمجازی (واقعی)، آن‌ها از مشتریان‌شان برای ارائه

---

[1] Epilepsy Foundation

[2] Hackers Assault Epilepsy Patients via Computer, http://www.wired.com/politics/security/news/2008/03/epilepsy

[3] MapleStory

[4] Woman arrested after virtual murder, http://www.telegraph.co.uk/news/newstopics/howaboutthat/3257876/Woman-arrested-after-virtual-murder.html

[5] عبارت سلامت بدنی به عنوان یک استعاره در اینجا استفاده می‌شود. سلامت بدنی یک آواتار به معنای واقعی کلمه نمی‌تواند رخ دهد، زیرا آواتار بدن فیزیکی ندارد. اما یک آواتار، یک بدن مجازی است که می‌تواند تقریبا در محیط مجازی آسیب ببیند.

[6] Ailin GRAEF

خدمت، هزینه دریافت کرده و بخشی از درآمدشان را به صاحب شرکت حفاظتی و یا فاحشه‌خانه می‌دهند. فحشای مجازی به‌طوراساسی متفاوت از فحشای غیرمجازی است؛ زیرا درعمل رابطه جنسی رخ نمی‌دهد. بلکه انیمیشن رایانه‌ای از رابطه جنسی ایجاد می‌شود. به همین علت نیز عنوان فحشای مجازی دارد [۹]. برخی پژوهش‌گران معتقدند دغدغه‌های متعارف در مورد نقض اصول اخلاقی در این مورد صدق نمی‌کند [۹]. اصل مزاحمت نیز که به‌طور کلی پایه‌ای برای منع هرزه‌نگاری است در این‌جا قابل به‌کارگیری نیست؛ اما از آن جایی که امکان فیلم‌برداری در دنیای مجازی وجود دارد و فیلم‌های ساخته‌شده نیز اغلب در یوتیوب قرار داده می‌شوند، می‌توان به فیلمبرداری غیرمجاز از لحظات خصوصی یک آواتار و انتشار آن در یوتیوب اشاره کرد که می‌تواند موجب هتک حیثیت مالک آواتار ارائه‌دهنده یا دریافت‌کننده این رابطه جنسی شود.

دوهمسری نیز موضوع بحث‌برانگیز دیگری است. کاربران می‌توانند از طریق آواتارشان در دنیای مجازی با یکدیگر ازدواج کنند. گر چه به‌طورقطع این ازدواج (دست‌کم تاکنون) از نظر قانونی در هیچ کجای دنیا به رسمیت شناخته نشده و تعهدآور نیست، اما افرادی که در دنیای واقعی متأهل هستند، می‌توانند از طریق آواتارشان، با آواتار فردی ازدواج کنند که در حال حاضر همسرشان نیست. آن‌ها درعمل در نوعی دوهمسری در دو جهان متفاوت درگیر می‌شوند [۹]. همچنین می‌توانند در این فضای مجازی (دنیای دوم) با بیش از یک آواتار ازدواج کنند که به منزله دوهمسری درون‌مجازی است. از آنجا که قوانین دنیای واقعی، مقررات دنیای مجازی را به‌طور کامل به رسمیت نمی‌شناسد، دوهمسری در دنیای مجازی نمی‌تواند زیرمجموعه قانون منع چندهمسری قرار گیرد [۹]. با وجود آن‌که برخی پژوهش‌گران، دغدغه‌های اخلاقی دنیای واقعی را در مسایلی نظیر چندهمسری در دنیای مجازی وارد نمی‌دانند، اما به‌طور قطع، باید رفتارهایی مانند تولید و توزیع هرزه‌نگاری کودکان مجازی، قتل آواتار، ایجاد مزاحمت یا هتک حیثیت و... را دارای تبعات غیراخلاقی دانست؛ چنان‌که هم‌اکنون ممنوعیت این رفتارها در دنیای مجازی در برخی کشورها جنبه قانونی پیدا کرده است.

با توجه به مثال‌های بالا و تبیین امکان آسیب‌های فرامجازی از رفتارهای مجازی، در ادامه به بررسی شروط لازم و کافی برای تحت شمول قانون جزا قرارگرفتن جرایم سایبری مجازی (جرم‌انگاری) پرداخته می‌شود. همان‌طورکه در مقدمه یاد شد، مطالعه جرایم سایبری مجازی متعلق به حوزهٔ هستی‌شناسی قانونی است؛ لذا با استفاده از هستی‌شناسی فلسفی سرل[1] به بررسی شروط لازم پرداخته و سپس با استفاده از فلسفه حقوق و ضمن تأمل بر نتیجه تحلیل هستی‌شناختی، شروط کافی نیز مشخص و تبیین می‌شوند.

۷- رویکرد هستی‌شناختی (برای تبیین شروط لازم)

واقعیت‌های موجود در جهان، به دو دستهٔ طبیعی و اجتماعی تقسیم می‌شوند. واقعیت‌های طبیعی، مستقل از ما وجود دارند (همانند طبیعت)؛ درحالی‌که واقعیت‌های اجتماعی، به‌ویژه زیرمجموعه خاصی از آن‌ها به نام واقعیت‌های نهادی[2]، وابسته به حیث التفاتی[3] جمعی ما انسان‌ها هستند؛ یعنی تنها با توافق یا پذیرش انسانی وجود دارند. یک مثال خوب از واقعیت نهادی، پول است. پول وجود دارد؛ زیرا ما کارکرد وضعیتی قانونی بر تکه‌های کاغذ و فلز وضع کرده‌ایم. کارکرد وضعیتی با استفاده از «قواعد تقویمی[4]» ایجاد می‌شوند که دارای شکل زیر هستند [۱۹]:

«X (در زمینه C) به عنوان Y محسوب می‌شود».

نمونه‌ای از قاعده تقویمی بدین شکل است:

تومان (همان X) در ایران (C)، به عنوان پول قانونی (Y) به شمار می‌رود.

مقررات کیفری[5]، نوع خاصی از قواعد تقویمی هستند؛ زیرا به‌طوردقیق شرایطی را مشخص می‌کنند که تحت آن، واقعیت نهادی (جرم) ایجاد می‌شود. آن‌ها بدین شکل هستند:

یک عمل خاص انسانی (همان X) در حوزه قضایی[6] خاص (C) به‌عنوان جرم (Y) به شمار می‌رود.

به‌عنوان مثال:

ربودن مال متعلق به غیر (همان X) در نظام کیفری ایران (C) به‌عنوان جرم سرقت (Y) محسوب می‌شود.

---

[1] Searle، از کارهای سرل به این دلیل استفاده می‌شود؛ زیرا او موثرترین هستی‌شناسی اجتماعی اخیر را ارائه می‌دهد، که یک هستی‌شناسی است که بر مسائل مربوط به زیست‌شناسی و فیزیک متمرکز نیست، بلکه بر مسائل جامعه متمرکز بوده و توجه ویژه‌ای به قانون دارد.

[2] Institutional facts
[3] Intentionality
[4] Constitutive rules
[5] Penal provisions
[6] Jurisdiction

یا

برای هر X که شرایط P را محقق کند، در زمینه C، X دارای وضعیت Y است [۱۹].

به‌عنوان مثال:

رفتاری اعم از گفته یا نوشته یا هر فعلی (همان X) که با توجه به شخصیت مخاطب آن، باعث سلب و هتک حیثیت و حرمت شخص به‌طور معمول شود (شرایط P)، در نظام کیفری ایران (C)، این رفتار (همان X)، توهین (Y) محسوب می‌شود.

از نظر حقوقی، شرایطی که باید برآورده شود تا یک رفتار انسانی به‌عنوان جرم به‌شمار رود به‌عنوان «عنصر[۱]» شناخته می‌شود. عناصر، بسته به جرم متفاوت هستند؛ اما سه عنصر اصلی برای هر جرم مورد نیاز است: عنصر قانونی (قانون‌گذار رفتاری را جرم شناخته و کیفری برای آن مقرر کرده باشد)؛ عنصر مادی[۲] (فعل یا ترک فعل مشخص به منصه ظهور و بروز یا کمینه به مرحله فعلیت برسد) و عنصر معنوی[۳] (با علم و اختیار ارتکاب یافته باشد). هم‌چنین در تمامی جرایم (به صراحت یا ضمنی) لازم است عنصر مادی دارای پیامد و نتیجه خاص باشد. به‌عنوان مثال، مرگ یا آسیب به شخص یا ازدست‌دادن اموال. این عنصر مشترک، علیت[۴] نامیده می‌شود.

در مورد جرایم سایبری مجازی، عناصر اساسی جرم می‌تواند «درون مجازی[۵]» (درون محیط مجازی‌ای که عمل در آن رخ می‌دهد) یا «فرامجازی[۶]» (خارج از محیط مجازی) تحقق یابد [۲۰]:

- عنصر مادی می‌تواند به شکل درون‌مجازی یا فرامجازی تحقق یابد. رفتار انسانی شبیه‌سازی‌شدهٔ رایانه‌ای (بازی پرندگان خشمگین)، عنصر مادی را به‌طور درون مجازی محقق می‌سازد؛ زیرا که چنین اقدامی از طریق یک دستگاه ورودی، در محیط مجازی رخ می‌دهد. اما یک رفتار انسانی که توسط شبیه‌سازی رایانه‌ای امکان‌پذیر شده، عنصر مادی را به‌طور فرامجازی محقق می‌سازد؛ زیرا که چنین اقدامی، اگر چه برحسب یک شیء مجازی تعریف می‌شود، اما در خارج از محیط مجازی رخ می‌دهد (هرزه‌نگاری کودکان مجازی).
- عنصر معنوی تنها می‌تواند به‌طور فرامجازی تحقق یابد (حتی زمانی که عنصر مادی به‌طور درون‌مجازی محقق شود). دلیل، آن است که در حال حاضر[۷] عنصر معنوی مربوط به وضعیت روانی کنش‌گر بشری است که لزوماً فرامجازی است. البته این بدان معنی نیست که در مورد عنصر مادی درون‌مجازی، وضعیت روانی کنش‌گر به‌طورکامل مستقل از محیط مجازی‌ای که عمل در آن صورت گرفته، مورد قضاوت قرار گیرد. در محیط مجازی می‌توان نشان داد که آیا رفتار کنش‌گر، آگاهانه یا عامدانه بوده است یا خیر.
- عنصر علیت همانند عنصر مادی، هم می‌تواند هم درون‌مجازی و هم فرامجازی محقق شود. عنصر علیت وقتی به‌طور درون‌مجازی تحقق می‌یابد که عنصر مادی دارای پیامدی درون‌مجازی باشد و وقتی به‌طور فرامجازی محقق می‌شود که عنصر مادی نتیجه‌ای خارج از محیط مجازی داشته باشد. گفتنی است که جایی که در آن عنصر علیت تحقق می‌یابد (داخل یا خارج از محیط مجازی)، وابسته به جایی نیست که عنصر مادی محقق می‌شود. به بیان دیگر یک عنصر مادی درون مجازی می‌تواند پیامد فرامجازی داشته باشد و بالعکس.

جایی که عنصر علیت در آن تحقق می‌یابد (درون مجازی یا فرامجازی)، اهمیت زیادی دارد؛ زیرا زمینه‌ای را مشخص می‌کند (C) که در آن وضعیت جرم (Y) یک عمل انسانی شبیه‌سازی‌شدهٔ رایانه‌ای و یا عمل انسانی که توسط شبیه‌سازی رایانه‌ای امکان‌پذیر شده (X) برقرار است. عمل انسانی شبیه‌سازی‌شدهٔ رایانه‌ای و یا عمل انسانی که توسط شبیه‌سازی رایانه‌ای امکان‌پذیر شده (X) که عنصر علیت (P) را به‌طور درون‌مجازی محقق می‌کند، ممکن است، به‌عنوان جرم (Y) در دنیای مجازی (C) به‌شمار رود، اما نمی‌تواند به‌عنوان جرم (Y) در دنیای غیرمجازی (C) به‌شمار رود. یک عمل انسانی شبیه‌سازی‌شدهٔ رایانه‌ای و یا عمل انسانی که با شبیه‌سازی رایانه‌ای (X) امکان‌پذیر شده که عنصر علیت (P)

---

[1] Element

[2] Actus reus: عمل کردن یا عمل نکردن غیرقانونی

[3] Mens rea: یک حالت ذهنی سزاوار سرزنش، معمولا لازم است که کنشگر آگاهانه عمل کند، به عمد یا بی پروا.

[4] Causation

[5] Intravirtually

[6] Extravirtually

[۷] در آینده، عنصر معنوی به‌الزام به وضعیت روانی کنشگر انسانی مربوط نخواهد بود، از آنجا که ماشین‌های یادگیرنده مستقل، مبتنی بر شبکه عصبی، الگوریتم ژنتیک و معماری عامل (agent architectures)، قادر به داشتن عنصر معنوی خودشان خواهند بود. هنگامی که چنین دستگاهی بخشی از یک محیط (واقعیت) مجازی شود، عنصر معنوی می‌تواند به‌طور درون‌مجازی ارضا شود. از آنجایی که این مقاله بر اعمال انسانی شبیه‌سازی‌شدهٔ رایانه‌ای و اعمال انسانی که توسط شبیه‌سازی رایانه ممکن شده، متمرکز است، عنصر معنوی درون‌مجازی فراتر از حوزه بحث آن قرار می‌گیرد.

را به‌طور فرامجازی محقق می‌کند، به‌طورقطع به‌عنوان جرم (Y) در جهان غیرمجازی (C) به‌شمار می‌رود.

زمینه (C) (دنیای مجازی یا غیرمجازی) که در آن جرم (Y) (یک عمل انسانی شبیه‌سازی‌شدهٔ رایانه‌ای و یا عمل انسانی که توسط شبیه‌سازی رایانه‌ای امکان‌پذیر شده (X)) رخ می‌دهد، تعیین‌کنندهٔ آن است که کنش رخ داده در دامنه مقررات جزایی موجود گنجانده شود یا خیر؛ زیرا قوانین کیفری بر محیط‌های مجازی منطبق نیست. این موضوع را می‌توان با «دایره جادو[1]» توضیح داد. دایره جادو، خطی استعاری است که قلمرو غیرمجازی را از قلمرو مجازی جدا کرده و از شمول قوانین کیفری مستثنی می‌کند و لذا تنظیم رفتار در این محیط، به مدیران و یا کاربران آن محیط وابسته است. باید توجه داشت، ممکن است قوانین تنظیمی توسط مدیران و یا کاربران دنیای مجازی، همان‌هایی باشند که در دنیای غیرمجازی، ممنوع و دارای ضمانت اجرای قانونی باشند. هم‌چنین ممکن است، رفتاری در دنیای مجازی ممنوع شود؛ درحالی‌که همین رفتار در دنیای غیرمجازی ممنوع نباشد و بالعکس. درصورتی‌که یک عمل انسانی شبیه‌سازی‌شدهٔ رایانه‌ای یا یک عمل انسانی که توسط شبیه‌سازی رایانه‌ای امکان‌پذیر شده، فقط در محیط مجازی به‌عنوان یک جرم به‌شمار رود، تنها موجبات پرداخت خسارت به بزه‌دیده را فراهم می‌کند و تابع قانون جزا نیست؛ اما یک عمل انسانی شبیه‌سازی‌شدهٔ رایانه‌ای و یا عمل انسانی که توسط شبیه‌سازی رایانه‌ای امکان‌پذیر شده که در دنیای غیرمجازی (واقعی) به عنوان جرم به شمار می‌رود، خط استعاری دایره جادو را قطع کرده و بنابراین، در قلمرو قانون جزا قرار می‌گیرد. برای مثال، می‌توان به موضوع مصرف مواد مخدر و روان‌گردان در دنیای مجازی اشاره کرد. بیش‌تر کشورهای جهان، جنبه‌های مختلف تولید، تجارت و دراختیارداشتن مواد مخدر و برخی داروها را ممنوع کرده‌اند؛ زیرا این مواد می‌توانند باعث ایجاد مشکلاتی برای سلامتی افراد مصرف‌کننده شوند. در دنیای مجازی «زندگی دوم» نیز کاربران می‌توانند دارویی به نام «سکلی‌ماین[2]» را از طریق آواتار خود تولید، نگهداری و استفاده کرده و تجارت کنند. عمل انسانی شبیه‌سازی‌شدهٔ رایانه‌ای در تولید، تجارت و یا دراختیارداشتن «سکلی‌ماین» در بازی «زندگی دوم» عنصر علیتی را محقق می‌سازد که عنصر مادی آن، درون‌مجازی است؛ اما «سکلی‌ماین» تنها می‌تواند از طریق آواتار در دنیای مجازی استفاده شود و بنابراین نمی‌تواند مشکلات سلامتی برای مالک آواتار ایجاد کند. از آنجا که عمل انسانی شبیه‌سازی‌شدهٔ رایانه‌ای در تولید، فروش و یا دراختیارداشتن «سکلی‌ماین» (X) در دنیای مجازی، عنصر علیت (P) را به‌طور درون‌مجازی محقق می‌سازد، نمی‌تواند به‌عنوان جرم (Y) در دنیای غیرمجازی (C) به حساب آورده شود. اگر قواعد «زندگی دوم» تولید، فروش و یا دراختیارداشتن «سکلی‌ماین» را منع کند، این رفتار تنها در آن محیط مجازی می‌تواند به‌عنوان جرم تلقی شود.

گاهی یک عمل انسانی شبیه‌سازی‌شدهٔ رایانه‌ای و یا عمل انسانی که توسط شبیه‌سازی رایانه‌ای امکان‌پذیر شده (X) می‌تواند عنصر مادی و علیت یک جرم را به‌طور درون‌مجازی ایجاد کرده و از سوی دیگر، عنصر مادی و علیت جرم دیگری را به‌طور فرامجازی محقق سازد. بنابراین چنین رفتاری به‌عنوان جرم (Y) در محیط مجازی (C) به‌شمار رفته و به‌عنوان جرم (Z) در دنیای غیرمجازی (C) به‌شمار می‌رود. پیش‌تر گفته شد در سال ۲۰۰۸، پلیس ژاپن پرونده زنی را بررسی کرد که شوهر آواتاری‌اش (آواتاری که شوهر آواتار خودش بود) را در دنیای مجازی کشته بود. این زن حساب مالک آواتار شوهر مجازی‌اش را هک و آواتار فرد را حذف کرده بود. با توجه به این که حذف یک آواتار درواقع، قتل نفس در دنیای مجازی به‌شمار می‌رود، عمل زن ژاپنی هر دو عنصر مادی (کشتن) و عنصر علیت (مرگ آواتار) جرم را به‌طور درون‌مجازی محقق ساخته بود. افزون بر این، هم «اقدام به قتل» و هم «مرگ» آواتار درون محیط مجازی رخ داده بود؛ اما مرگ آواتار پیامدی نیز در دنیای غیرمجازی داشت؛ مالک آواتار مقتول، همزاد مجازی خود را از دست داده بود. در بسیاری از کشورها، تخریب غیرقانونی اطلاعات رایانه جرم‌انگاری شده است (ماده ۴ کنوانسیون جرایم سایبری). از آنجا که آواتار، متشکل از داده‌های رایانه‌ای است، می‌توان گفت که قتل آواتار نوعی تخریب داده‌های رایانه‌ای محسوب می‌شود. از آنجایی که زن به‌طور غیرقانونی به حساب کاربر آواتار دسترسی پیدا کرده و آن را تخریب کرده بود، تحقق درون‌مجازی عناصر جرم قتل، تحقق فرامجازی عناصر جرم تخریب اطلاعات رایانه را نیز موجب شده است؛ بنابراین چنین رفتاری که به‌عنوان جرم قتل در دنیای مجازی (C) به‌شمار رفته، به‌عنوان جرم تخریب اطلاعات در دنیای غیرمجازی (C) به‌شمار می‌رود.

برای نتیجه‌گیری می‌توان بیان داشت، عمل انسانی شبیه‌سازی‌شدهٔ رایانه‌ای و یا عمل انسانی که توسط شبیه‌سازی رایانه‌ای امکان‌پذیر شده که عناصر یک جرم را

[1] Magic circle
[2] Seclimine

محقق می‌سازد، تنها زمانی می‌تواند در شمول قلمرو حقوق کیفری موجود قرارگیرد که به‌عنوان یک جرم در دنیای غیرمجازی به‌شمار رود و درواقع عنصر علیت را به‌طور فرامجازی محقق کند. بنابراین، شرط لازم برای قراردادن جرایم سایبری مجازی در شمول قلمرو حقوق کیفری موجود، آن است که عناصر علیت را به‌طور فرامجازی محقق سازد؛ اما شرط کافی چیست؟ پاسخ به این پرسش، بستگی به موضعی دارد که در بحث فلسفی حقوقی (پوزیتیویست قانونی یا نظریه‌پردازان قانون طبیعی) اتخاذ می‌شود. بخش بعد به اجمال به این موضوع می‌پردازد.

۸- رویکرد فلسفی (برای تبیین شروط کافی)

در فلسفهٔ حقوق، دو نظریه اصلی رقیب در مورد محتوای قانون وجود دارد؛ اثبات‌گرایان حقوقی[1]؛ و نظریه‌پردازان قانون طبیعی[2]. اثبات‌گرایان حقوقی، همانند آستین[3]، بر این مدعا هستند که قوانین ممکن است دارای هر محتوایی باشند. بنابراین معتقدند قانون‌گذاران و نظام‌های قضایی برای آوردن هر عمل انسانی شبیه‌سازی‌شدهٔ رایانه‌ای و یا عمل انسانی که توسط شبیه‌سازی رایانه‌ای امکان‌پذیر شده و دارای نتیجه فرامجازی است و عناصر یک جرم را برآورده می‌سازد، به قلمرو حقوق کیفری، آزاد هستند. در این صورت شرط لازم، همان شرط کافی است و نیاز به شرط دیگری نیست. در مقابل، نظریه‌پردازان قانون طبیعی معتقدند محتوای قوانین به‌واسطهٔ رابطهٔ‌شان با اخلاق تعیین می‌شود. قانون طبیعی کلاسیک (که فیلسوفان باستانی مانند افلاطون و سیسرو[4] آن را توسعه داده و توسط توماس آکویناس[5] به‌تفصیل شرح داده شده)، بر این مدعا هستند که ارتباطی ضروری بین حقوق و اخلاق وجود دارد و قانون غیراخلاقی، قانون محسوب نمی‌شود. نظریه‌پردازان قانون طبیعی معتقدند که قانون‌گذاران و نظام‌های قضایی، تنها زمانی می‌توانند یک عمل انسانی شبیه‌سازی‌شدهٔ رایانه‌ای و یا عمل انسانی که توسط شبیه‌سازی رایانه‌ای ممکن شده و نتیجه فرامجازی را دارد، تحت قلمرو حقوق کیفری قرار دهند که نتیجه فرامجازی ناقض اصول اخلاقی داشته باشد. در این صورت، بر اساس دیدگاه نظریه‌پردازان قانون طبیعی، افزون بر شرط لازم (پیامد فرامجازی)، شرط کافی (غیراخلاقی بودن پیامد فرامجازی) نیز ضروری است؛ حال این سؤال مطرح می‌شود که کدام اصول اخلاقی می‌تواند به تعیین این که چگونه قانون مجازات باید با جرایم سایبری مجازی مقابله کند، کمک کنند. فینبرگ معتقد است هنگامی که قانون‌گذاران و یا نظام‌های قضایی، یک عمل انسانی خاص را زیرمجموعه مجازات کیفری قرار می‌دهند، شهروندان، دیگر مجاز به انجام این عمل نیستند. با توجه به نظر فینبرگ، یک‌چنین تداخلی با آزادی شهروندان با استفاده از قانون مجازات، به‌طورمعمول بر اساس یکی از اصول محدودکنندهٔ آزادی زیر مشروعیت می‌یابد: اصل ضرر (قاعده لاضرر)، اصل مزاحمت، اصل حمایت‌گرایی قانونی یا اخلاقگرایی حقوقی؛ لذا شرط کافی آن است که نتیجه فرامجازی شامل آسیب (به دیگری و یا به خود)، مزاحمت[6] یا شری از نوع دیگر باشد که بتواند مداخله در آزادی شهروندان را با استفاده از قانون مجازات بر اساس یکی از اصول محدود کننده آزادی فینبرگ توجیه کند.

۹- نتیجه‌گیری

رمان‌ها، فیلم‌های ویدیویی، تلویزیون (ماهواره‌ای و یا کابلی)، بازی‌های ویدیویی و سپس شبکه‌های اجتماعی تحت وب یا مبتنی بر تلفن همراه و در مجموع، هر نوآوری در سرگرمی عامه، تاکنون نشان داده‌اند که ظرفیت تبدیل‌شدن به تهدید علیه نظم اخلاقی و امنیت عمومی را دارند. توسعه «دنیاهای مجازی» نیز از همین روند تبعیت می‌کند. می‌توان انتظار داشت هم‌چنان‌که اجتماع‌های واقعی در حال کم‌رنگ‌شدن هستند، اجتماع‌های مجازی (شبکه‌های اجتماعی و در ادامه، دنیاهای مجازی) روزبه‌روز پررنگ‌تر شده و افراد، هویت خود را بیش‌تر از این اجتماع‌ها می‌گیرند؛ لذا می‌توان انتظار داشت پدیده دنیاهای مجازی نیز در آینده مسایل مبتلا به خود را در پی داشته باشد. مسایلی نظیر وضعیت مالکیت اشیایی که در این دنیاها با پول واقعی خریداری شده، وضعیت شراکت در کسب‌وکارهای مشترک، وضعیت میراث و نظایر آنها، هم‌چنین ارتکاب انواع رفتارهای مجرمانه در دنیای مجازی و دادخواهی بزه‌دیدگان، موجبات دغدغه و دل‌نگرانی را برای سیاست‌گذاران و قانون‌گذاران فراهم کرده است. با این حال، اشراف بر این نوآوری‌ها به‌طورمعمول با مقاومت‌هایی در جامعه حقوقی مواجه است:

[1] Legal Positivists
[2] Natural Law Theorists
[3] Austin
[4] Cicero
[5] Thomas Aquinas
[6] Offense

- نخست بدان علت که جرایم سایبری مجازی، حوزه‌ای تخصصی و بیش‌تر میان‌رشته‌ای است که به گستره‌ای از علوم و تجربیات مختلف نیازمند است و باید تحلیل حقوقی آن‌ها توأم با تحلیل‌های فنی باشد.
- دوم آن‌که بر خلاف جرایم واقعی، جرایم سایبری به‌علت بی‌مرز بودن‌شان، جرایمی جهانی به‌شمار می‌روند و لذا تا حدودی متفاوت از فرایند متعارف وضع قانون هستند.
- سوم آن‌که با نگاهی کوتاه به گذشته، در می‌یابیم به‌طوراساسی فاصلهٔ زمانی میان عرضه فناوری و بروز جرم مرتبط، و فاصله زمانی میان عرضه فناوری و وضع قوانین کیفری متناسب نیست. به‌عنوان مثال، هنگامی که شبکه‌های رایانه‌ای در دهه هفتاد میلادی معرفی شدند، نخستین دسترسی غیرمجاز به این شبکه‌ها مدت کوتاهی پس از معرفی رخ داد. به‌طور مشابه، جرایم نرم‌افزاری بلافاصله پس از معرفی رایانه‌های شخصی در دهه هشتاد میلادی ارتکاب یافت (هنگامی‌که از محصولات نرم‌افزاری، رونوشت تهیه شد)؛ درحالی‌که در هر دو مورد، شرایط وضع قانون برای این مسایل فراهم نبود و مدت زمانی طول کشید تا زمینه وضع قوانین متناسب فراهم شود (گریک، ۲۰۰۹). طولانی‌شدن این فرایندها، یعنی شناخت سوءاستفاده‌های احتمالی از فناوری‌های جدید و انجام اصلاحات لازم در قوانین کیفری ملی، فرصت‌های طلایی را برای مجرمان فراهم می‌آورد.
- چهارم آن‌که به‌طور کلی، قانون‌گذاران، نیازمند مجال و فرصت برای به‌روزرسانی قوانین کیفری ملی برای جرم‌انگاری اشکال جدید جرایم سایبری هستند. حتی جرایمی که جدید نبوده و توسط قانون مجازات تعریف شده‌اند، نیازمند بررسی و به‌روزرسانی هستند. به‌ویژه آن‌که در بیش‌تر موارد، امکان انتقال تجربه جرم‌انگاری جرایم سنتی به حوزه سایبری وجود ندارد.

در پایان نگارندگان این مقاله معتقدند از آنجایی که جرایم سایبری مجازی، در آینده‌ای نه‌چندان دور دامن‌گیر کشورمان می‌شود؛ لذا شناخت جرایم سایبری مجازی و پیش‌بینی تمام سازوکارهای کیفری (جرم‌انگاری) و غیرکیفری (جبران خسارت) باید در اولویت پژوهش‌های مراکز دانشگاهی و پژوهش‌های قضایی قرار گیرد؛ و به‌عنوان نتیجه‌گیری می‌توان بیان داشت، عمل انسانی شبیه‌سازی شده رایانه‌ای و یا عمل انسانی که توسط شبیه‌سازی رایانه‌ای امکان‌پذیر شده که عناصر یک جرم را محقق می‌سازد، تنها زمانی می‌تواند در شمول قلمرو حقوق کیفری موجود قرارگیرد که به‌عنوان یک جرم در دنیای غیرمجازی به‌شمار رود و درواقع عنصر علیت را به‌طور فرامجازی محقق کند. بنابراین، شرط لازم برای قراردادن جرایم سایبری مجازی در شمول قلمرو حقوق کیفری موجود، آن است که عناصر علیت را به‌طور فرامجازی محقق سازد؛ و شرط کافی آن است که نتیجه فرامجازی شامل آسیب (به دیگری و یا به خود)، مزاحمت یا شری از نوع دیگر باشد که بتواند مداخله در آزادی شهروندان را با استفاده از قانون مجازات بر اساس یکی از اصول محدودکنندهٔ آزادی فینبرگ توجیه کند.

۱۰- مراجع

[1] S. Orin Kerr, "Criminal Law in Virtual Worlds," In *University of Chicago Legal Forum*, 2015, vol. 8, no. 1, 11-15.

[2] L. Strikwerda,"Should virtual cybercrime be regulated by means of criminal law? A philosophical, legal-economic, pragmatic and constitutional dimension," *Information & Communications Technology Law,* 2014, 23, no. 1, pp.31-60.

[3] L. Strikwerda, "Theft of virtual items in online multiplayer computer games: an ontological and moral analysis," *Ethics and information technology,* 2012, 14, no. 2, pp.89-97.

[4] Z.Schaengold, "Personal Jurisdiction over Offenses Committed in Virtual Worlds," U. Cin. L. Rev, 2012, vol.81, pp. 361-370.

[5] W.Rumbles, Theft in the digital: Can you steal virtual property, Canterbury L., 2011, Rev., 17, 354.

[6] T. Gorrindo, and J. E. Groves, "Crime and hate in virtual worlds: a new playground for the id?," *Harvard review of psychiatry,* vol.18, no.2, pp.113-118, 2010.

[7] A. Guinchard, "Crime in virtual worlds: The limits of criminal law," *International Review of Law, Computers & Technology,* vol. 24, no. 2, pp.175-182, 2010.

[8] I.Warren, and D. Palmer, "Crime risks of three-dimensional virtual environments," *Trends and issues in crime and criminal justice*, vol.388, pp. 1-15, 2010.

[9] W. Susan Brenner, Susan , "Fantasy Crime: The Role of Criminal Law in Virtual Worlds," *Vanderbilt Journal of Entertainment and Technology Law,*vol.11, pp.1-58, 2008.

[10] D.M. Goodman, and W.S. Brenner, "The emerging consensus on criminal conduct in cyberspace," *Int'l JL & Info. Tech,* 2002, vol.10, pp.139-150.

[11] N.K. Katyal, "Criminal law in cyberspace," *University of Pennsylvania Law Review,* vol.149, no. 4, pp.1003-1114, 2001.

[12] T.H. Tavani, "Ethics and technology: Ethical issues in an age of information and communication technology", 2003.

[13] A.M. Weber, "The Council of Europe's Convention on Cybercrime," *Berkeley Technology Law Journal,* vol. 18, no. 1, pp.425-446, 2003.

[14] P. Brey, "Virtual reality and computer simulation," In *Ethics and Emerging Technologies*, Palgrave Macmillan UK, 2014.

[15] S.J. Hartz, *The Value of Virtual Worlds and Entities: A Philosophical Analysis of Virtual Worlds and Their Potential Impact on Well-Being*. 2010.

[16] C.Allen , *13 Artificial life, artificial agents, virtual realities: technologies of autonomous agency*, The Cambridge handbook of information and computer ethics. 2010.

[17] T.M. Powers, "Real wrongs in virtual communities," *Ethics and information technology,* vol. 5, no. 4, pp.191-198, 2003.

[18] J. Wolfendale, "My avatar, my self: Virtual harm and attachment," *Ethics and Information Technology,* vol. 9, no. 2, pp.111-119, 2007.

[19] J.R. Searle, *Making the Social World: The Structure of Human Civilization*. Oxford UP, New York, 2010.

[20] S.J. Hartz, "Virtual worlds and their challenge to philosophy: understanding the "intravirtual" and the "extravirtual"," *Metaphilosophy,* vol.43, no. 4, pp.499-512, 2012.

افسانه زمانی جباری تحصیلات مقطع کارشناسی و کارشناسی ارشد را در رشته حقوق دانشگاه تهران گذرانده و دانشجوی دکترای حقوق در رشته حقوق کیفری و جرم‌شناسی دانشگاه تربیت مدرس است. ایشان هم‌اکنون به‌عنوان جانشین معاون دادستان و دادیار اظهارنظر دادسرای عمومی و انقلاب شیراز مشغول به فعالیت است. علایق پژوهشی ایشان شامل حقوق کیفری، جرم‌شناسی، پیش‌گیری از جرم و آیین دادرسی کیفری است.

امین پژوهش جهرمی تحصیلات مقطع کارشناسی و کارشناسی ارشد خود را در رشته مکانیک در دانشگاه صنعتی شریف گذرانده و دکترای خود را در رشتهٔ مدیریت از دانشگاه تهران دریافت کرده است. ایشان هم‌اکنون به‌عنوان استادیار و عضو هیأت علمی رسمی دانشگاه صنعتی مالک‌اشتر مشغول به فعالیت است. علایق پژوهشی ایشان شامل مدیریت دانش، نوآوری باز، مدیریت کسب‌وکار و شرکت‌های کوچک و دانش‌بنیان است.