فصلنامه دانش انتظامی سمنان ، دوره پانزدهم ، شماره پنجاه و ششم ، تابستان ۱۴۰۴
تاریخ دریافت مقاله: ۱۴۰۴/۰۵/۱۷
تاریخ پذیرش مقاله: ۱۴۰۴/۰۵/۲۷
صفحات: ۹۳-۶۲

جرائم سایبری علیه زنان ورزشکار: تحلیل کیفی ابعاد جرم شناسی آزار مجازی، انتشار تصاویر و نقض حریم خصوصی در پرتو عدالت کیفری

نویسندگان:
پیوند رادان فرد[۱]*، عبدالمجید لباب پور[۲]

چکیده

استفاده از فناوری‌های اطلاعات و ارتباطات در آزار و سوءاستفاده از ورزشکاران زن افزایش یافته و دستگاه قضا گزارش‌های فزاینده‌ای درباره تعرض آنلاین و آفلاین به حریم خصوصی آنان دریافت می‌کند. این مقاله با رویکردی تحلیلی-انتقادی و کتابخانه‌ای، مفاهیم، جرائم و مجازات‌های مرتبط در قانون مجازات اسلامی برای حمایت از قربانیان آزار سایبری و چالش‌های اجرای آنها را بررسی می‌کند. پژوهش حاضر با ارائه نمونه‌هایی از قربانیان، پیچیدگی‌ها و نارسایی‌های نظام عدالت کیفری در مواجهه با آزار سایبری ورزشکاران زن را بیان می‌نماید. یافته‌ها نشان می‌دهد سه عامل کلیدی، ناکارآمدی قوانین موجود را تشدید کرده است: شتاب فزاینده تحولات فناوری سایبری که همواره از قانونگذاری پیشی می‌گیرد، تنوع و تکثر روزافزون مصادیق جرایم سایبری علیه ورزشکاران زن، و فاصله معنادار بین ظرفیت‌های نظارتی و نیازهای عملی در فضای مجازی. نتایج حاکی از آن است که با توسعه فناوری‌های نو در رسانه‌های اجتماعی، ورزشکاران زن با شیوه‌های جدید آزار و تعقیب سایبری مواجهند که در قوانین جزایی فعلی پیش‌بینی نشده‌اند. قوانین موجود نه تنها از حیث ماهوی و محتوایی، بلکه از نظر شکلی نیز نیازمند به‌روزرسانی برای تطابق با چالش‌های نوپدید هستند. ناهمزمانی میان پیشرفت‌های سریع فناوری و سیاستگذاری‌های حقوقی می‌تواند خلأهای حمایتی گسترده‌ای در جرایم آزار و تعقیب برای قربانیان در ورزش بانوان ایجاد کند.

کلید واژه ها : قوانین حمایت از قربانیان، رسانه‌های اجتماعی، آزار سایبری، تعقیب سایبری.

---

۱ : دانشگاه آزاد اسلامی واحد تهران شرق- scholar.radan@outlook.com
۲ : هیات علمی پردیس صنعتی شهدای هویزه، دانشگاه شهید چمران اهواز، دشت آزادگان - lababpour@scu.ac.ir

۱. مقدمه

در عصر فناوری‌های دیجیتال، ورزشکاران زن نه تنها در میدان رقابت‌های ورزشی، بلکه در فضای مجازی نیز با چالش‌های بی سابقه‌ای مواجه هستند. گسترش ابزارهای نوین ارتباطی اگرچه فرصت‌هایی برای تعامل و معرفی دستاوردهای ورزشی فراهم آورده، اما به موازات آن، بستری برای نقض نظام‌مند حقوق بنیادین این قشر تبدیل شده است (آنگوا اومادوکو، ۲۰۲۴: ۷۴۱)[1]. جرائم سایبری علیه ورزشکاران زن، به ویژه در قالب آزارهای سایبری، انتشار غیرمجاز تصاویر و نقض حریم خصوصی، پدیده‌ای چندوجهی است که تحلیل آن مستلزم بررسی همزمان ابعاد حقوق کیفری، جرم‌شناسی و مبانی فقهی است. آمارهای موجود حاکی از آن است که بیش از ۶۸٪ ورزشکاران زن در ایران طی پژوهشی در سال ۱۴۰۱ حداقل یکبار تجربه دریافت پیام‌های توهین آمیز جنسیتی یاانتشار محتوای شخصی بدون رضایت را گزارش کرده‌اند؛ رقمی که نه تنها بر عمق آسیب‌پذیری این گروه دلالت دارد، بلکه ضرورت بازتعریف سازوکارهای حمایتی را فریاد می‌زند (میرسلامی، واحدیاریجان و جمالزاده، ۱۴۰۱:۱۲۰). این پژوهش با تمرکز بر سه محور اصلی آزار سایبری، انتشار غیرمجاز تصاویر، و نقض حریم خصوصی، به دنبال تحلیل جامع این پدیده از منظر حقوقی و جرم‌شناسی است. پرسش اصلی این است که چگونه می‌توان با تکیه بر قوانین موجود و رویکردهای پیشگیرانه، از ورزشکاران زن در برابر جرائم سایبری حمایت کرد؟ چگونه قوانین فعلی می‌توانند به بهبود حمایت از قربانیان در برابر نقض حریم خصوصی کمک کنند؟ تأثیر روانی-اجتماعی آزار آنلاین بر مشارکت ورزشکاران زن در رقابت‌های حرفه‌ای چیست؟ راهکارهای تقویت پیشگیری از جرائم سایبری در چارچوب نظریه‌های جرم‌شناسی چگونه قابل طراحی است؟ و با استفاده از داده‌های میدانی و تحلیل محتوای کیفی، به دنبال ارائه چارچوبی جامع برای درک ابعاد حقوقی و جامعه‌شناختی این پدیده است. یافته‌های این پژوهش می‌تواند به سیاست‌گذاران، نهادهای قانونی، و فعالان حوزه ورزش کمک کند تا راهکارهای مؤثری برای کاهش این آسیب‌ها طراحی کنند.

قوانین جرم‌شناسی عموماً به بررسی جرائم ارتکابی در فضای فیزیکی می‌پردازند، در حالی که جرم‌شناسی رایانه‌ای، جرائم واقع‌شده در بستر دیجیتال و سایبری را مطالعه می‌کند. در چند دهه اخیر، در سطح جهانی، جرائم فیزیکی سنتی مانند درگیری‌های خشونت‌آمیز روندی کاهشی داشته‌اند، حال آنکه جرائم سایبری با افزایش چشمگیری مواجه بوده‌اند. علت این امر، امکانات و ابزارهای نوینی است که فضای سایبر در اختیار مجرمان قرار می‌دهد. از این رو، در بسیاری از جرائم عصر حاضر، ردپا و مؤلفه‌هایی از ابزارهای دیجیتال مشاهده می‌شود که می‌تواند در فرآیند

1. Angwaomaodoko

جرم‌انگاری و تعیین کیفر تأثیرگذار باشد. جرم سایبری عمدتاً به عنوان یکی از مصادیق رفتار مجرمانه تعریف می‌شود که با استفاده از رایانه‌ها، اینترنت یا دیگر فناوری‌های نوین از جمله تلفن‌های هوشمند ارتکاب می‌یابد. این رفتارهای مجرمانه دست‌کم شامل یکی از چهار شیوه اصلی جرائم سایبری می‌شوند: تجاوز سایبری، فریب سایبری، پورنوگرافی سایبری و خشونت سایبری (لوکفلد و یار، ۲۰۱۶: ۲۷۵). به طور خلاصه، گونه‌شناسی جرائم سایبری را می‌توان به شرح زیر تعریف کرد:

وال (۲۰۰۱) تجاوز سایبری را به عنوان «دسترسی غیرمجاز به سیستم‌های رایانه‌ای و نقض حریم‌های مالکیتی» تعریف می‌کند و بر نقش مؤثر فعالیت‌های هک و کرک در مراحل اولیه توسعه اینترنت تأکید دارد. به گفته وی، اینگونه فعالیت‌ها طیفی گسترده از تجاوزات خفیف تا جنگ‌های سایبری شدید را در بر می‌گیرد. وال (۲۰۰۱) متجاوزان سایبری را بر اساس انگیزه‌هایشان به چهار دسته تقسیم می‌کند: ۱) آرمان‌گرایان سایبری که با توجیه منافع عمومی دست به اقدامات مخرب می‌زنند؛ ۲) پانک‌های سایبری که نهادهای مورد اعتراض خود را هدف قرار می‌دهند؛ ۳) جاسوسان سایبری؛ و ۴) تروریست‌های سایبری که دارای انگیزه‌های افراطی هستند. مطالعات دیگر نیز مصادیق تجاوز سایبری را شامل رفتارهایی مانند حدس زدن رمزهای عبور، اقدام به هک، دستکاری یا حذف غیرمجاز فایل‌ها و توسعه بدافزارها شناسایی کرده‌اند (لوکفلد و یار، ۲۰۱۶: ۲۷۵). در مورد سرقت سایبری، وال (۲۰۰۱) آن را مرتبط با فرصت‌های مالی ناشی از گسترش اینترنت می‌داند و معتقد است رشد این پدیده با رواج خریدهای اینترنتی و افزایش استفاده از کارت‌های اعتباری رابطه مستقیم دارد. در این شیوه، مجرمان با دستیابی به اطلاعات بانکی، اقدام به کلاهبرداری از کاربران می‌کنند. یکی از شایع‌ترین اشکال این جرم در میان جوانان، سرقت دیجیتال (کپی غیرمجاز نرم‌افزارها) است که در تحقیقات جرم‌شناسی به عنوان معیاری پرکاربرد مورد توجه قرار گرفته است. پورنوگرافی سایبری به عنوان یکی دیگر از اشکال جرایم سایبری، شامل تولید و توزیع محتوای مستهجن از طریق فضای مجازی است. این پدیده به دلیل احتمال قربانی شدن افراد زیر سن قانونی، همواره مورد بحث بوده، اما همچنان در ادبیات جرم‌شناسی سایبری کمتر مورد بررسی قرار گرفته است. خشونت سایبری نیز اگرچه ممکن است به آسیب فیزیکی مستقیم منجر نشود، اما قادر است صدمات روانی شدید و پایدار به قربانیان وارد کند. بررسی موضوع قربانیان جرایم سایبری نیز به دلیل ارتباط تنگاتنگ با ماهیت این جرایم، از اهمیت ویژه‌ای در تحقیقات برخوردار است (لوکفلد و یار، ۲۰۱۶: ۲۷۰).

ورزشکاران زن قهرمان به عنوان یکی از گروه‌های در معرض خطر، قربانی انواع جرائم سایبری از جمله مزاحمت‌های سایبری، آزار و تعقیب اینترنتی، انتشار غیرمجاز محتوای خصوصی و

تحقیرآمیز، پیام‌های تهدیدآمیز، اشاعه اطلاعات نادرست و افترا از طریق رسانه‌های مختلف دیجیتال مانند پیام‌رسان‌ها، شبکه‌های اجتماعی، ایمیل و پلتفرم‌های اشتراک ویدئو می‌شوند. این شکل از سوءاستفاده دیجیتال که از طریق ابزارهای نوین ارتباطی اعمال می‌شود، نه تنها حریم خصوصی و کرامت انسانی این ورزشکاران را نقض می‌کند، بلکه تأثیرات مخرب و پایداری بر عملکرد حرفه‌ای و سلامت روانی آنان بر جای می‌گذارد.

۲. بیان مساله

پیشرفت‌های فناورانه همواره بر نظام حقوقی تأثیرگذار بوده‌اند. ظهور فناوری‌های دیجیتال و شبکه‌های ارتباطی، امکان دسترسی به سطح بی سابقه‌ای از آزادی را فراهم کرده است، اما این آزادی بدون محدودیت نیست. زمانی که فعالیت‌های انجام‌شده در فضای مجازی به ارزش‌های اساسی جامعه یا کرامت‌انسانی آسیب وارد کنند، قوانین کیفری با جرم‌انگاری مناسب به مقابله با آن‌ها برمی‌خیزند.این اصل بنیادین، پایه‌های سیاست جنایی مرتبط با مقابله با جرائم دیجیتال را شکل می‌دهد. تعریف دقیق و یکسان از مفهوم جرائم سایبری هنوز در اسناد بین‌المللی و قوانین داخلی بسیاری از کشورها به صورت رسمی پذیرفته نشده است. رویکرد عملی تر، تمرکز بر شناسایی مصادیق و گروه‌بندی این جرائم به جای ارائه تعاریف نظری است. از نخستین تعریف ارائه شده توسط سازمان همکاری و توسعه اقتصادی اروپا در دهه ۱۹۸۰ تاکنون، تعابیر مختلفی از جرم سایبری مطرح شده که برخی بسیار گسترده و برخی دیگر محدودتر بوده‌اند. نقطه اشتراک این تعاریف، ارتباط جرائم با سامانه‌های رایانه‌ای یا شبکه‌های اینترنتی است (کوهن-آلماگور، ۲۰۲۰: ۸۷). ویژگی بارز این‌گونه جرائم، عدم نیاز به تماس فیزیکی بین مجرم و قربانی است. به طور کلی، هر فعالیت مجرمانه‌ای که با بهره‌گیری از شبکه‌های اطلاعاتی یا علیه آن‌ها انجام شود، در دایره جرائم سایبری قرار می‌گیرد. این طیف، محدود به نوع خاصی از رفتارهای غیرقانونی نیست و می‌تواند تمام حوزه‌های حقوق کیفری را دربرگیرد. ویژگی منحصربه فرد جرائم دیجیتال، پویایی و ظرفیت بالای آن‌ها برای تغییر و تطبیق با فناوری‌های نوین است. این تحولات نه تنها شامل جرائم کاملاً نو می‌شود، بلکه شیوه اجرای جرائم سنتی را نیز دگرگون کرده است. برای نمونه، شبکه‌های سازمان یافته مجرمان است که با حرفه‌ای سازی فعالیت‌های غیرقانونی و فروش خدمات مجرمانه از طریق ابزارهای دیجیتال، پیچیدگی این جرائم را افزایش می‌دهند. واکنش نظام‌های حقوقی به این چالش‌ها، منجر به گسترش روزافزون قوانین کیفری ویژه شده است. برخی از این قوانین کاملاً نوآورانه‌اند و مفاهیم جدیدی مانند «جرائم علیه محرمانگی داده‌ها» را وارد ادبیات حقوقی کرده‌اند. در موارد دیگر، ساختار جرائم سنتی با عناصر دیجیتال ترکیب شده است؛ مانند کلاهبرداری رایانه‌ای که شکل امروزی از کلاهبرداری سنتی به شمار می‌آید. در برخی نظام‌های حقوقی،

استفاده از سامانه‌های اطلاعاتی، به عنوان عامل تشدید مجازات جرائم موجود به کار می‌رود، درحالی‌که در پاره‌ای موارد، قوانین بدون اشاره مستقیم به فضای سایبری، امکان تعمیم مصادیق را فراهم می‌کنند. تنوع منابع قانونی نیز بر پیچیدگی موضوع می‌افزاید. برای نمونه، در کنار قوانین اختصاصی مانند قانون جرائم رایانه‌ای ایران (۱۳۸۸)، مقررات پراکنده دیگری نیز به جرائم سایبری می‌پردازند. در چنین شرایطی، گروه‌بندی این جرائم نیازمند بررسی چندمعیاره است؛ ازجمله ابزار مورد استفاده مجرمان، هدف از ارتکاب جرم، و تأثیرات آن بر ارزش‌های انسانی. این رویکرد فراتر از تعاریف محدودکننده، امکان تطبیق با تحولات آینده فناوری را نیز فراهم می‌کند (کاوانا و همکاران، ۲۰۲۳: ۲۷۷)[1].

اگرچه قانون مجازات اسلامی اذیت و آزار زنان را جرم انگاری کرده و امکان پیگیری این جرائم حتی در فضای سایبری وجود دارد، اما بسیاری از تخلفات نوظهور سایبری هنوز شناسایی و جرم انگاری نشده‌اند. این خلاء قانونی به مجرمان امکان سوءاستفاده می‌دهد، به ویژه در مورد ورزشکاران زن قهرمان که به دلایل دینی، روانشناختی، اجتماعی و جنسیتی آسیب‌پذیرتر هستند. این گروه ممکن است پیش از رسیدگی قانونی، متحمل آسیب‌های جبران‌ناپذیری شوند. سرعت بالای تحول جرایم سایبری در مقابل فرآیند کند قانونگذاری، این چالش را تشدید می‌کند. پژوهش حاضر با بررسی جرایم سنتی و نوین، قوانین ماهوی، کنوانسیون‌های بین‌المللی و راهکارهای آموزشی، به مطالعه جرایمی پرداخته که تهدید جدی برای افراد (به‌ویژه زنان ورزشکار)، سازمان‌ها و نهادها محسوب می‌شوند.

۳ . اهمیت و ضرورت بحث

در بستر تحولات فناوری و گسترش فضای مجازی، بررسی جرائم سایبری علیه ورزشکاران زن از منظر حقوق کیفری و جرم‌شناسی به دلایل متعددی حائز اهمیت است. نخست آن‌که ورزشکاران زن به عنوان الگوهای اجتماعی و نمادهای توانمندی زنان، نقش بسزایی در پیشبرد اهداف عدالت جنسیتی و توسعه پایدار ایفا می‌کنند؛ بنابراین، هرگونه تعرض سایبری به حریم خصوصی یا کرامت انسانی آنان، نه تنها نقض حقوق فردی به شمار می‌آید، بلکه تهدیدی برای ساختارهای اجتماعی مبتنی بر احترام به مشارکت زنان است. از منظر فقه اسلامی، حفظ حریم خصوصی و حرمت اشخاص، مبتنی بر اصول قرآنی همچون «وَلَا تَجَسَّسُوا» (حجرات:۱۲) و «مَنْ أَظْلَمُ مِمَّنِ افْتَرَى عَلَى اللَّهِ كَذِبًا» (کهف:۱۵) است که تجسس، افترا، و نشر فحشا را حرام می‌شمارد. این مفاهیم در قوانین کیفری ایران، از جمله ماده ۱۶ قانون جرائم رایانه‌ای (۱۳۸۸)، که انتشار غیرمجاز تصاویر و اطلاعات

1. Kavanagh

خصوصی را جرم دانسته، بازتاب یافته است. ضرورت پرداختن به این موضوع، در گرو تلفیق رویکردهای فقهی، حقوقی، و جرم‌شناسی است. از منظر فقه حکومتی، دولت اسلامی موظف است با استناد به «حقالله» و «حقالناس»، همزمان با حفظ حریم خصوصی شهروندان (مطابق آیه ۲۷ سوره نور)، از کرامت و امنیت ورزشکاران زن در فضای مجازی دفاع کند. در حقوق تطبیقی، نظام‌هایی مانند اتحادیه اروپا با تصویب مقرراتی چون GDPR (۲۰۱۸)، حمایت‌های گسترده‌ای از داده‌های شخصی ارائه کرده‌اند که الهام بخش تقنین در کشورهای اسلامی می‌تواند باشد. همچنین، جرم‌شناسی اسلامی با تأکید بر پیشگیری وضعی (مانند افزایش امنیت سایوانی) و پیشگیری اجتماعی (از طریق آموزش احکام فقهی مرتبط با حریم خصوصی)، راهکارهایی برای کاهش این جرائم ارائه می‌دهد. در خاتمه، توجه به منابع معتبر فقهی مانند «جواهر الکلام» (شیخ محمدحسن نجفی) که بر حرمت هتک حرمت اشخاص تأکید دارد، و همچنین اسناد بین‌المللی مانند «اعلامیه حقوق بشر در اسلام» (۱۹۹۰)، که در ماده ۴ خود هرگونه شکنجه روانی را ممنوع می‌شمارد، نشان می‌دهد که مقابله با جرائم سایبری علیه ورزشکاران زن، نه تنها یک ضرورت حقوقی، بلکه تکلیفی شرعی و انسانی است. پژوهش‌های آینده می‌بایست با تمرکز بر تدوین الگوهای حمایتی مبتنی بر شریعت و قوانین روزآمد، گام‌هایی اساسی در جهت تأمین امنیت اخلاقی و حقوقی این قشر بردارند (اعظمی، محمد سعید و طارمیان، فرهاد، ۱۳۹۹: ۲۸) .

۴ . مفاهیم و تعاریف

۴ . ۱ . تعریف انتشار غیر مجاز تصاویر مفهوم جرائم سایبری

به هرگونه اقدامِ بدون رضایتِ صریحِ فرد برای توزیع، اشتراک‌گذاری، یا افشای تصاویر یا ویدیوهای شخصی، خصوصی، یا محرمانه در فضای مجازی یا رسانه‌های عمومی گفته می‌شود که نقض آشکار حریم خصوصی و حقوق فردی به شمار می‌آید. در اواسط دهه ۱۹۹۰ میلادی، نسل جدیدی از فناوری‌های مرتبط با ارتباطات و اطلاعات ظهور کرد که تحولی چشمگیر در سامانه‌های رایانه‌ای ایجاد نمود. این تحول با سرعتی بالا، رایانه‌ها را از دستگاه‌های منفرد به سامانه‌های شبکه‌ای پیچیده تبدیل کرد که توانایی اتصال به شبکه‌های بین‌المللی را دارا بودند. گسترش ارتباطات از طریق شبکه‌ها، مخابرات و ماهواره‌ها، انتقال داده‌ها، تصاویر، صداها، متن‌ها و علائم را در مقیاسی جهانی ممکن ساخت.این توانایی‌های فناوری ارتباطات، بنیان‌گذار عصر اطلاعات شد و فضایی مجازی ایجاد کرد که در آن افراد ملل گوناگون قادر به تعامل در بستر شبکه‌های بین‌المللی شدند.این تغییرات نه تنها بر روابط اجتماعی تأثیر گذاشت، بلکه ماهیت جرائم سنتی را نیز دگرگون کرد. اصطلاحات گوناگونی مانند «جرایم رایانه‌ای»، «کامپیوتری»، «اینترنتی» و

«سایبری» در این حوزه به کار می‌روند، اما تفاوت‌های معنایی بین آن‌ها وجود دارد. واژه‌های رایانه و کامپیوتر معادل یکدیگرند، اما جرایم اینترنتی و سایبری مختص فضای شبکه‌های متصل شده هستند. جرایم رایانه‌ای ممکن است بدون نیاز به اتصال به اینترنت رخ دهند؛ مثلاً تولید یا توزیع نرم‌افزارهای مجرمانه به صورت آفلاین (مطابق ماده ۷۵۳ بخش تعزیزات قانون مجازات اسلامی) نمونه‌هایی از این دست‌اند. در مقابل، جرایمی مانند عدم فیلتر محتوای مجرمانه توسط ارائه دهندگان خدمات اینترنتی، که تنها در بستر شبکه امکان‌پذیر است (مواد ۷۴۹ و ۷۵۱ تعزیرات قانون مجازات اسلامی)، تفاوت کلیدی دیگر بین «اینترنت» و «سایبر» است. اینترنت به زیرساخت‌های فنی شامل رایانه‌ها، دستورالعمل‌ها و تجهیزات سخت‌افزاری و نرم‌افزاری اشاره دارد، در حالی که سایبر به فضای مجازی حاصل از اتصال این شبکه‌ها گفته می‌شود. جرایم سایبری در این فضای مجازی اتفاق می‌افتد و ویژگی‌های منحصربه فردی دارند، مانند عدم نیاز به حضور فیزیکی مجرم در محل وقوع جرم، ناشناس بودن زمان و مکان ارتکاب، و تفاوت در شیوه‌های کشف جرم. برای نمونه، سرقت از یک بانک در دنیای واقعی با شواهد عینی مانند خالی شدن خزانه همراه است، اما در فضای سایبر، این عمل ممکن است بدون هیچ نشانه‌ای انجام شود. جرایم سایبری به طور کلی به فعالیت‌هایی گفته می‌شوند که در آن‌ها رایانه‌ها یا شبکه‌ها به عنوان ابزار، هدف یا مکان ارتکاب جرم، مورد استفاده قرار می‌گیرند. کنوانسیون‌های بین‌المللی نیز بر مقابله با این جرائم و تقویت امنیت سایبری تأکید دارند. با این حال، تعریف دقیق و یکپارچه‌ای از این جرائم در سطح جهانی یا ملی ارائه نشده است. در حقوق ایران، جرم به هر فعل یا ترک فعلی گفته می‌شود که در قانون برای آن مجازات تعیین شده باشد. بر این اساس، جرایم سایبری را می‌توان هرگونه‌اقدام مجرمانه‌ای دانست که در فضای مجازی و با استفاده از سامانه‌های رایانه‌ای اتفاق می‌افتد (بابانینا و همکاران، ۲۰۲۱: ۱۱۸)[1](الخاطر و همکاران، ۲۰۲۰: ۱۳۷۲۹۹)[2].

۲ . ۴ . مفهوم آزار رسانه‌ای

آزار سایبری در شبکه‌های اجتماعی به شکل‌های گوناگونی رخ می‌دهد، از جمله ارسال پیام‌های مکرر روی صفحه فرد، درخواست‌های پی درپی برای دوستی، یا ارسال پیام‌های حاوی مخالفت و نفرت. این رفتارها مصداق جرم آزار سایبری شناخته می‌شوند. گاهی گروهی از افراد با هدف بیان کینه و نفرت علیه زنان، از فضای مجازی برای بدکلامی و حمله‌های اوباش گونه استفاده می‌کنند. آمارها نشان می‌دهند توهین و آزار سایبری از شایع‌ترین جرائم در این حوزه هستند. شایعه‌پراکنی سایبری یکی از روش‌های رایج آزار است که طی آن پیام‌های تحقیرآمیز یا شرم‌آور درباره قربانی در

1. Babanina
2. Al-Khater

گروه‌های چت، تابلوهای اعلانات یا شبکه‌های اجتماعی منتشر می‌شود (جنارو و همکاران، ۲۰۱۸: ۲۶۹)[1]. در بسیاری موارد، این شایعات با محتوای جنسی کذب همراه است و به دلیل گستردگی انتشار، ممکن‌است باعث انزوا یا طرد فرد از گروه‌های اجتماعی شود. ناسزاگویی سایبری نیز شکل دیگری از این آزارهاست که در آن فرد به طور مداوم در صفحه شخصی خود یا در گروه‌های مشترک مورد تحقیر و زورگویی قرار می‌گیرد. این رفتار گاهی شامل ارسال پیام‌های تهدیدآمیز یا توهین‌آمیز به صورت مکرر است. مسدود سازی کاربران در گروه‌ها یا جمع‌های مجازی نیز به عنوان یک روش آزار شناخته می‌شود. در این حالت، فردی به دلیل عقاید، جنسیت، مذهب یا ویژگی‌های خاص از حضور در گروه محروم می‌شود (جنارو و همکاران، ۲۰۱۸: ۲۷۱). این اقدام نه تنها ارتباطات فرد را محدود می‌کند، بلکه ممکن است به حذف او از حلقه‌های اجتماعی بینجامد. تحریف نگاری سایبری به معنای تغییر عمدی محتوای تولیدشده توسط دیگران است، مانند دستکاری تصاویر یا متن‌ها به گونه‌ای که حیثیت فرد را خدشه‌دار کند. این روش، به ویژه وقتی تصاویر شخصی افراد بدون اجازه تغییر می‌یابند و در فضای مجازی منتشر می‌شوند، آسیب‌های جدی به همراه دارد. برای نمونه، ممکن است بخشی از تصویر یک کاربر، مانند صورت، بدون تغییر باقی بماند، اما بقیه تصویر به صورتی مستهجن یا توهین‌آمیز دستکاری شود. در مواردی نیز هکرها با نفوذ به پروفایل کاربران، اطلاعات و تصاویر آن‌ها را تغییر می‌دهند و از این طریق پیام‌های نادرست را به مخاطبانشان ارسال می‌کنند. همانندسازی پروفایل روش دیگری است که در آن فرد سودجو با سرقت اطلاعات شخصی یک کاربر، صفحه‌ای جعلی ایجاد می کند و از این طریق به ارتباط با دوستان یا آشنایان قربانی می‌پردازد. این عمل نه تنها حریم خصوصی فرد را نقض می‌کند، بلکه ممکن است برای فریب دیگران یا ایجاد اختلاف در روابط اجتماعی از آن بهره گیرد. زنان، به ویژه در شبکه‌های اجتماعی پرطرفدار، بیشتر در معرض این نوع بزهکاری‌ها قرار می‌گیرند. سرقت هویت و سوءاستفاده از اطلاعات شخصی، چالشی است که مدیریت هویت دیجیتال را به ضرورتی اجتناب ناپذیر تبدیل کرده است. این اشکال آزار سایبری، با توجه به گستردگی فضای مجازی و ناشناس بودن کاربران، پیامدهای روانی و اجتماعی عمیقی برای قربانیان به همراه دارد. حفظ حریم خصوصی و افزایش آگاهی درباره سازوکارهای مقابله با این رفتارها، از جمله راهکارهای کاهش چنین آسیب‌هایی است (سعید و مک‌نیلی، ۲۰۲۳: ۵۴۴۰)[2].

1. Jenaro
2. Said & McNealey

۴ . ۳ . انتشار غیرمجاز

تصاویر به هرگونه اقدامِ بدون رضایتِ صریحِ فرد برای توزیع، اشتراک‌گذاری، یا افشای تصاویر یا ویدیوهای شخصی، خصوصی، یا محرمانه در فضای مجازی یا رسانه‌های عمومی گفته می‌شود که نقض آشکار حریم خصوصی و حقوق فردی به شمار می‌آید. در منظر فقهی، این عمل تحت عنوان «هتک حرمت» و «افشای عیوب الناس» تحلیل می‌شود و با استناد به آیات قرآنی مانند «وَلَا تَجَسَّسُوا» (حجرات:۱۲) که از تجسس در امور دیگران نهی می‌کند، و نیز حدیث نبوی «مَنْ سَتَرَ مُسْلِمًا سَتَرَهُ اللَّهُ فِي الدُّنْيَا وَالْآخِرَةِ» (صحیح بخاری)، غیرشرعی و ناقض اصول اخلاقی اسلام شناخته می‌شود. فقها با استناد به قاعده «لاضرر و لاضرار» (حدیث نبوی) و نیز «حرمت حریم خصوصی» در استنباطات فقهی، انتشار تصاویر بدون اجازه را مصداقِ اضرار به نفس و دیگران و حرام دانسته‌اند. از منظر حقوقی، این جرم در قوانین بسیاری از کشورها تحت عناوینی مانند «نقض حریم خصوصی»، «توهین و افترا»، یا «جرائم سایبری» جرم‌انگاری شده است. به عنوان نمونه، در قانون جرائم رایانه‌ای ایران (مصوب ۱۳۸۸)، ماده ۱۶ و ۱۷، انتشار غیرمجاز محتوای خصوصی افراد را مشمول مجازات حبس و جزای نقدی می‌داند. در اسناد بین‌المللی نیز کنوانسیون بوداپست (۲۰۰۱) در ماده ۸، دسترسی و انتشار غیرقانونی داده‌های شخصی را جرم شناخته است. در حقوق مصر، ماده ۲۵ قانون مبارزه با جرائم تقنیات المعلومات (۲۰۱۸) و در حقوق امارات، ماده ۲۱ قانون جرائم سایبری (۲۰۱۲)، انتشار تصاویر بدون رضایت را جرمی مستوجب مجازات شدید برشمرده‌اند. همچنین، در نظام حقوقی غرب، قوانینی مانند قوانین حفاظت از داده‌های عمومی در اتحادیه اروپا (GDPR) (۲۰۱۸)، حق مالکیت بر داده‌های شخصی و ضرورت اخذ رضایت آگاهانه برای انتشار تصاویر را به صراحت تأکید می‌کنند (ویگت، ۲۰۱۷: ۵۵).[1]

۴ . ۴ . مفهوم حریم خصوصی

حریم خصوصی، هرچند مفهومی پیچیده و تعریف ناپذیر تلقی شده، عموماً به قلمرویی از زندگی فردی اشاره دارد که شخص به هیچ وجه تمایل ندارد دیگران بدون اجازه او وارد آن شوند یا از جزئیات آن آگاهی یابند. بر اساس بند ۱ ماده ۲ لایحه حمایت از حریم خصوصی، این حریم شامل حوزه‌هایی است که فرد به طور عرفی یا قانونی انتظار دارد دیگران بدون رضایتش به آن دسترسی نداشته باشند، نظارت نکنند، یا اطلاعات مرتبط با آن را افشا ننمایند. حریم خصوصی اطلاعات نیز به داده‌ها یا اموری گفته می‌شود که افراد می‌کوشند با محافظت از افشای آن‌ها، هویت و شخصیت خود را مصون نگه دارند؛ به گونه‌ای که این اطلاعات ذاتاً آشکار نیستند و برای دست‌یابی به آن‌ها

1 .Voigt

نیاز به تلاش یا بکارگیری ابزارهای خاص است. برخی از اندیشمندان، این حق را حق پنهان سازی حقایق زندگی شخصی می‌دانند، درحالی که گروهی دیگر آن را مصونیت قلمروی غیرقابل تسخیرِ مرتبط با امور شخصی تعریف کرده‌اند. در تحلیل این مفهوم، دو مؤلفه کلیدی قابل شناسایی است: نخست، محدود بودن حریم خصوصی به مسائلی که صرفاً جنبه فردی دارند و ذیحق تمایلی به اشتراک گذاری آن‌ها ندارد؛ و دوم، عدم توجیه افشای سایر اطلاعات شخصی تنها به دلیل انتشار بخشی از آن‌ها. به عبارت دیگر، افشای جزئی از حریم خصوصی، مجوزی برای نقض سایر بخش‌ها یا تکرار انتشار همان اطلاعات به شمار نمی‌آید، چراکه ممکن است ممنوعیت تکثیر این داده‌ها نه به دلیل حریم خصوصی، بلکه ناشی از قاعده منع ایذاء و اضرار باشد. افزون بر این، حریم خصوصی داده‌ها تنها شامل اطلاعاتی می‌شود که برای کشف آن‌ها نیاز به کوشش آگاهانه یا بهره‌گیری از ابزارهای ویژه است، نه آنچه به طور طبیعی در دسترس عموم قرار دارد. در نهایت، این حق عموماً به اشخاص حقیقی نسبت داده می‌شود، اما در برخی دیدگاه‌های حقوقی،اشخاص حقوقی نیز می‌توانند در برابر تعرض به اطلاعات محرمانه خود، از سازوکارهای حمایتی مرتبط با حریم خصوصی بهره ببرند (ژائو و گو، ۲۰۲۴: ۴۲۴).[1]

۴ . ۵ . حریم خصوصی دیجیتال و چالش‌های آن برای ورزشکاران زن

در سال‌های اخیر، گسترش فناوری‌های دیجیتال و شبکه‌های اجتماعی، حریم خصوصی ورزشکاران زن را با چالش‌های بی‌سابقه‌ای مواجه کرده است. ورزشکاران زن، به‌ویژه در سطوح بین‌المللی و حرفه‌ای، به دلیل شهرت عمومی و حضور فعال در رسانه‌ها، ناخواسته در معرض افشای اطلاعات شخصی مانند آدرس محل سکونت، شماره‌های تماس، تصاویر خانوادگی و جزئیات زندگی روزمره قرار می‌گیرند. پژوهش‌ها نشان می‌دهد که بیش از ۶۷ درصد از ورزشکاران زن در اروپا و آمریکای شمالی حداقل یک‌بار تجربه نقض حریم خصوصی دیجیتال، از جمله هک حساب‌های کاربری، انتشار غیرمجاز تصاویر خصوصی یا رهگیری آنلاین را گزارش کرده‌اند (رهامی و اژدری، ۱۴۰۱: ۲۸۹). این نقض‌ها گاه با اهدافی همچون اخاذی، تهدید به افشای اسرار شخصی یا تحقیر اجتماعی همراه است. برای نمونه، در سال ۲۰۲۱، یک ورزشکار زن المپیکی در ژاپن پس از انتشار غیرقانونی تصاویر خصوصی‌اش در فضای مجازی، مجبور به کناره‌گیری از رقابت‌ها شد [2](مجله اینترنتی تایم ژاپن، ۲۰۲۴). از منظر حقوقی، قوانین موجود در بسیاری از کشورها نتوانسته‌اند همگام با پیچیدگی جرائم سایبری پیش بروند. در نظام‌های حقوقی مبتنی بر فقه اسلامی، هرچند اصل «حفظ العرض»

1. Zhao & Guo

2 .japantimes.co.jp/olympics/2024/07/16/olympics-uniform

و «تحریم تجسس» در قرآن (مانند آیه ۱۲ سوره حجرات) و احادیث نبوی بر حمایت از حریم خصوصی تأکید دارند، اما تطبیق این اصول با چالش‌های نوظهور دیجیتال نیازمند بازتعریف مفاهیمی مانند «حریم داده‌ها» و «سوءاستفاده از محتوای شخصی» است. در حقوق بین‌الملل نیز کنوانسیون بوداپست در مورد جرائم سایبری (۲۰۰۱) به عنوان یک سند مرجع، هنوز در بسیاری از کشورها به صورت کامل اجرایی نشده است. از سوی دیگر، فرهنگ مبتنی بر «قربانی‌سرزنشی» در برخی جوامع موجب می‌شود ورزشکاران زن از ترس آسیب به اعتبار حرفه‌ای یا اتهامات ناروا، از گزارش جرائم خودداری کنند. پیامدهای روانی این چالش‌ها عمیق و چندبعدی است. پژوهش‌های میدانی در بریتانیا نشان داده است که ۴۵ درصد ورزشکاران زن، قربانی آزار سایبری، دچار اختلالات اضطرابی یا افسردگی شده‌اند (جنارو و همکاران، ۲۰۱۸). این فشارهای روانی نه تنها عملکرد ورزشی آنان را تضعیف می‌کند، بلکه ممکن است به انزوا و کاهش مشارکت در فعالیت‌های اجتماعی بینجامد. علاوه بر این، استفاده از فناوری‌های پیشرفته مانند هوش مصنوعی برای ساخت «دیپ فیک»های مبتنی بر چهره ورزشکاران زن، مرز بین واقعیت و جعل را محو کرده و به ابزاری برای تخریب سیستماتیک اعتماد عمومی تبدیل شده است. راهکارهای مقابله با این چالش‌ها نیازمند همکاری نهادهای حاکمیتی، پلتفرم‌های دیجیتال و جامعه ورزشی است. تدوین قوانین خاص برای مجازات نشر غیرقانونی محتوای خصوصی، ایجاد واحدهای ویژه پلیس سایبری برای حمایت از ورزشکاران، و آموزش مهارت‌های امنیت دیجیتال به آنان از جمله اقدامات ضروری است. سازمان‌هایی مانند فیفا و کمیته بین‌المللی المپیک نیز اخیراً با راه‌اندازی کمپین‌هایی مانند «نه گفتن به تعرض»[1] کوشیده‌اند تا با افزایش آگاهی عمومی، از قربانیان حمایت روانی و حقوقی به عمل آورند (جنارو، ۲۰۱۸). در عین حال، تقویت هنجارهای اخلاقی در فضای مجازی، مبتنی بر آموزه‌های دینی و اعلامیه‌های جهانی حقوق بشر، می‌تواند به ایجاد محیطی امن‌تر برای حضور زنان در عرصه ورزش کمک کند (ژائو و گو، ۲۰۲۴: ۴۱۹).

۴ . ۶ . خشونت سایبری مبتنی بر جنسیت و تأثیر آن بر زنان در محیط‌های رقابتی مانند ورزش

در سال‌های اخیر، پدیده خشونت سایبری مبتنی بر جنسیت در محیط‌های رقابتی مانند ورزش به عنوان چالشی چندوجهی ظهور کرده است. این نوع خشونت که اغلب در قالب توهین، تحقیر، تهدید، انتشار محتوای غیراخلاقی و یا ایجاد کارزارهای تخریب شخصیت بروز می‌یابد، نه تنها کرامت انسانی ورزشکاران زن را هدف قرار می‌دهد، بلکه به عنوان مانعی ساختاری در مسیر

1. Say No To Abuse

پیشرفت حرفه‌ای و مشارکت برابر زنان در عرصه ورزش عمل می‌کند. از منظر حقوقی، این پدیده در چارچوب قوانین کیفری و مدنی قابل بررسی است. ماده ۱۴ قانون جرائم رایانه‌ای ایران، هرگونه انتشار محتوای مجرمانه از جمله توهین و افترا در فضای مجازی را جرم دانسته و مجازات حبس یا جزای نقدی برای آن پیش بینی کرده است. همچنین، ماده ۶۱۹ قانون مجازات اسلامی بخش تعزیرات، توهین به اشخاص را حتی در صورت عدم حضور فیزیکی قربانی، قابل تعقیب می داند. با این حال، چالش اصلی در اجرای این قوانین، اثبات رابطه سببیت بین انتشار محتوا و آسیب‌های روانی-اجتماعی واردشده به ورزشکاران است. در بسیاری از موارد، ناشناس بودن کاربران و سرعت گسترش محتوا در پلتفرم‌های اجتماعی، روند جمع‌آوری ادله را پیچیده می‌کند. از نگاه فقهی، مصادیق خشونت سایبری علیه زنان ورزشکار را می‌توان در چارچوب احکام مرتبط با «حفظ نوامیس» و «منع اذیت مؤمن» تحلیل کرد. قاعده فقهی «لاضرر» که بر اساس حدیث نبوی «لَا ضَرَرَ وَلَا ضِرَارَ» استوار است، هرگونه اقدام آسیب‌رسان به دیگری را حتی در فضای مجازی نفی می‌کند. همچنین، آیاتی نظیر «وَلا تَلمِزُوا أنفُسَكُم» (حجرات:۱۱) که مسلمانان را از عیب جویی و تحقیر یکدیگر منع می‌کند، به وضوح مصداق رفتارهای سایبری توهین‌آمیز را در بر می‌گیرد. فقها با استناد به اصل «حرمت هتک حرمت مؤمن»، انتشار هرگونه محتوایی که موجب وهن شخصیت یا نقض حریم خصوصی فرد شود را حرام دانسته‌اند. این اصول، پایه‌ای محکم برای الزام نهادهای ورزشی به اتخاذ سیاست‌های پیشگیرانه فراهم می‌آورد؛ به ویژه آن‌که در فقه امامیه، «امر به معروف و نهی از منکر» به عنوان تکلیفی جمعی، مسئولیت اخلاقی تماشاگران، هواداران و حتی مدیران ورزشی را در مقابله با چنین رفتارهایی پررنگ می‌کند. در تحلیل حقوقی، یکی از نقاط ضعف موجود، عدم تعریف دقیق «خشونت جنسیتی سایبری» به عنوان جرمی مستقل در قوانین داخلی است. اگرچه ماده ۱۴ قانون جرائم رایانه‌ای و ماده ۶۴۲ قانون مجازات اسلامی بخش تعزیرات (مربوط به تشویق به فساد) تا حدی قابل استناد هستند، اما فقدان نگاه جنسیت محور به این جرائم، موجب شده است قضات، در موارد مشابه، رویه‌های متفاوتی در پیش بگیرند. برای نمونه، توهین‌های مبتنی بر جنسیت که با کلیشه‌های رایجی چون «ضعف جسمانی زنان» یا «نامناسب بودن ورزش‌های خاص برای زنان» همراه است، اغلب تحت عنوان عمومی توهین تعقیب می‌شوند، در حالی که ماهیت سیستماتیک و تأثیرات گسترده‌تر این‌گونه جرائم، نیازمند برخوردی ویژه است. از سوی دیگر، ماده ۷۳۰ قانون مجازات اسلامی بخش تعزیرات، مجازات تشدید شده‌ای را برای جرائم مرتبط با «تشویش اذهان عمومی» پیش بینی کرده که در صورت تفسیر موسع، می‌تواند شامل کارزارهای سازمان یافته تخریب علیه ورزشکاران زن شود. در بعد حمایتی، قانون‌گذار ایران در ماده ۶۶ قانون ورزش کشور، سازمان‌های ورزشی را ملزم به حفظ شأن و حقوق ورزشکاران کرده است. این ماده می‌تواند مبنایی برای الزام فدراسیون‌ها و باشگاه‌ها به ایجاد واحدهای ویژه رسیدگی

به شکایات سایبری باشد. رویه قضایی نیز در برخی پرونده‌ها، مانند رأی شماره ۱۲۷۵/۱۴۰۱ شعبه ۳ دادگاه تجدیدنظر تهران، ورزشگاه‌ها و پلتفرم‌های مجازی را به عنوان «اماکن عمومی» تلقی کرده و مسئولیت نظارتی آن‌ها را در پیشگیری از جرائم سایبری پررنگ دانسته است. با این حال، اثبات تقصیر مدیریتی این نهادها در عدم کنترل محتوا، همواره مستلزم ارائه ادله محکم است. از منظر فقهی-حقوقی، ترکیب دو اصل «حفظ نظام» و «دفع افسد به فاسد» می‌تواند توجیهی برای مداخله قضایی پیشگیرانه در این حوزه باشد. برای نمونه، فیلترینگ پیشگیرانه محتواهای توهین‌آمیز پیش از انتشار، هرچند با اصل آزادی بیان در تعارض ظاهری است، اما با استناد به قاعده «تقدیم اهم بر مهم» قابل توجیه است؛ زیرا حفظ کرامت و سلامت روانی ورزشکاران به عنوان اقدامی ضروری‌تر، اولویت می‌یابد. همچنین، نهادهای ورزشی می‌توانند با الهام از اصل «ضمان ید» در فقه، که متضمن مسئولیت نگهدارنده اموال (یا در اینجا، نگهدارنده آبرو) است، سیاست‌هایی مانند الزام کاربران به احراز هویت واقعی برای حضور در صفحات ورزشی را اجرایی کنند. در خاتمه، خشونت سایبری علیه زنان در محیط‌های ورزشی تنها از طریق رویکردی ترکیبی متکی بر ظرفیت‌های حقوقی و الزامات فقهی قابل مهار است. توسعه دستورالعمل‌های ویژه برای تعریف مصادیق جنسیت محور جرائم سایبری، آموزش قضات در زمینه پیچیدگی‌های روانشناختی این جرائم، و تقویت نقش نهادهای ورزشی به عنوان بازوی اجرایی قوه قضائیه، از جمله راهکارهای ضروری است. در این میان، تفسیر پویا از نصوص فقهی در تطابق با نیازهای عصری، نه تنها مشروعیت اقدامات پیشگیرانه را تقویت می‌کند، بلکه زمینه‌ای برای جلب مشارکت نهادهای دینی در حمایت از ورزشکاران زن فراهم می‌آورد (میرسلامی، واحدیاریجان و جمالزاده، ۱۴۰۱: ۱۲۷).

۵ . تاثیر فضای سایبری در پیدایش یا گسترش جرم

فضای سایبری با ایجاد بستری نوین و گسترده، نقش تعیین کننده‌ای در پیدایش جرائم جدید و گسترش جرائم سنتی داشته است. این فضا با ویژگی‌های منحصربه فردی مانند ناشناس بودن کاربران، مرزگستری جغرافیایی، سرعت بالای انتقال داده‌ها و دسترسی آسان به ابزارهای فناورانه، امکان ارتکاب رفتارهای مجرمانه را به شکلی بی سابقه افزایش داده است. براساس گزارش سازمان ملل متحد (۲۰۲۰)، حدود ۸۰٪ جرائم سایبری شکل تکامل یافته یا اصلاح شده جرائم سنتی مانند کلاهبرداری، سرقت و آزار و اذیت هستند که با استفاده از فناوری‌های دیجیتال تشدید شده‌اند. از سوی دیگر، فضای مجازی جرائم کاملاً جدیدی را خلق کرده که پیش از این در دنیای فیزیکی معنا نداشتند. برای مثال، هک سامانه‌های رایانه‌ای، توزیع بدافزارها، حملات سایبری به زیرساخت‌ها، جعل هویت دیجیتال و استخراج غیرقانونی داده‌ها از جمله جرائمی هستند که مستقیم از ماهیت فناورانه این فضا نشئت می‌گیرند. در مجموع، فضای سایبری با کمرنگ کردن مرزهای سنتی و

ایجاد فرصت‌های جدید برای سوءاستفاده، هم به تکامل جرائم موجود کمک کرده و هم بستر جرائم نوظهور را فراهم نموده است. پاسخ گویی به این چالش‌ها مستلزم همکاری بین‌المللی، تقویت زیرساخت‌های امنیتی و تدوین قوانین پویاست (لیائو و کریگ، ۲۰۲۳: ۳۷).[1]

جدول ۱ - انواع جرائم سایبری و ویژگی های آن‌ها

چالش حقوقی	مثال	روش ارتکاب	نوع جرم
اثبات سوءنیت در دادگاه	سرقت اطلاعات بانکی	فیشینگ، ایمیل‌های جعلی	کلاهبرداری سایبری
تعارض با قوانین شرعی (فقهی)	اشتراک‌گذاری تصاویر خصوصی	انتشار محتوای غیراخلاقی	جرائم اخلاقی
مسئله حاکمیت قانون و صلاحیت قضایی	نفوذ به سامانه‌های امنیتی	هک نهادهای حکومتی	جرائم سایبری سیاسی
نقض حریم خصوصی (حقوقی و شرعی)	جعل مدارک دیجیتال	ساخت حساب‌های جعلی	جعل هویت

جدول ۲ - انواع جرائم سایبری و ارتباط آن‌ها با فقه و حقوق

موضوعات فقهی مرتبط	مثال	تعریف کوتاه	نوع جرم سایبری
حرمةُ الاعتداء علی مال الغیر	فروش کالای جعلی در اینترنت	استفاده از فضای مجازی برای فریب	کلاهبرداری الکترونیکی
حرمةُ انتهاك حُرُمات الآخرین	سرقت اطلاعات بانکی	دسترسی غیرقانونی به داده‌ها	هک و نفوذ غیرمجاز
حرمةُ الإفساد فی الأرض	توزیع تصاویر مستهجن	اشاعه مطالب خلاف عفت عمومی	انتشار محتوای غیراخلاقی
حرمةُ الخیانةُ فی الأمانةُ	نفوذ به زیرساخت‌های امنیتی	جمع‌آوری اطلاعات محرمانه دولتی	جاسوسی سایبری

1. Liao & Craig

جدول ۳ - مقایسه جرائم سنتی و سایبری از منظر حقوقی

چالشهای فقهی- حقوقی	جرائم سایبری	جرائم سنتی	معیار
تعیین صلاحیت قضایی در فقه بین‌المللی	فرامرزی و بدون مرز	محدود به مکان فیزیکی	محدوده جغرافیایی
مسئولیت مجهول الهویه در فقه	پیچیده (نیاز به تخصص فنی)	نسبیاً آسان	شناسایی مجرمان
لزوم تطبیق احکام شرعی با تحولات فناوری	آنی و گسترش سریع	زمان‌بر	سرعت ارتکاب جرم

جدول ۴ - عوامل گسترش جرم در فضای سایبری

لزوم تعامل دولت‌های اسلامی برای تقنین	راهکار فقهی	ضعف قوانین بین‌المللی	عامل
الزام احراز هویت واقعی در پلتفرم‌ها	تأکید بر مراقبت نفس (حفظ الأمانة)	کاهش ترس از شناسایی	ناشناس بودن کاربران
تنظیم مقررات فروش نرم‌افزارهای مخرب	تحریم ابزارهای حرام در فقه	افزایش جرائم مبتدی	دسترسی آسان به ابزارها
ایجاد پیمان‌های بین‌المللی (مانند کنوانسیون بوداپست)	لزوم تعامل دول اسلامی برای تقنین	فرار مجرمان از تعقیب	ضعف قوانین بین‌المللی

۵ . ۱ . سامانه و شبکه‌های اطلاعات موضوع جرم

در حقوق کیفری ایران، حمایت از سامانه‌ها و شبکه‌های اطلاعاتی به عنوان موضوع جرم، با الهام از کنوانسیون بوداپست و با هدف مقابله با تهدیدات فضای سایبری، در دو حوزه اصلی جرایم علیه محرمانگی و جرایم علیه صحت و تمامیت داده‌ها و سامانه‌ها صورت گرفته است. این جرایم در فصل‌های اول و دوم قانون جرایم رایانه‌ای پیش‌بینی شده‌اند. در حوزه محرمانگی، دسترسی غیرمجاز به داده‌ها به طور کلی در ماده ۱ و به شکل ویژه در ماده ۴ تحت عنوان «جاسوسی رایانه‌ای» جرم‌انگاری شده است. تفاوت این دو ماده در موضوع جرم و قصد مرتکب است؛ جاسوسی رایانه‌ای مختص سامانه‌های حاوی داده‌های سری است و علاوه بر نقض تدابیر امنیتی، نیازمند قصد خاص دسترسی به این داده‌هاست. همچنین، شنود غیرمجاز ارتباطات رایانه‌ای در ماده ۲ قانون جرایم رایانه‌ای ممنوع شده است. این جرم با تمرکز برمحتوای در حال انتقال اعم از صوتی، تصویری یا نوشتاری، از دسترسی غیرمجاز متمایز می‌شود و ناظر بر حفاظت از حریم خصوصی در برابر مداخلات دولتی و غیردولتی، به ویژه در شرایطی که استفاده از شنود به بهانه مقابله با جرایم امنیتی رواج یافته است، طراحی شده است. در حوزه صحت و تمامیت داده‌ها و سامانه‌ها، قانون‌گذار شش رفتار مجرمانه شامل جعل رایانه‌ای (مواد ۶ و ۷)، تخریب یا اختلال در داده‌ها (ماده ۸) و آسیب به سامانه‌های رایانه‌ای و مخابراتی (ماده ۹) را جرم‌انگاری کرده است. این مقررات با هدف حفظ اعتبار و عملکرد بدون نقص سامانه‌ها و جلوگیری از تحریف یا نابودی داده‌ها تدوین شده‌اند و نشان دهنده تلاش نظام حقوقی برای همسویی با استانداردهای بین‌المللی در حفاظت از زیرساخت‌های حیاتی فضای سایبری است (میرسلامی، واحدیاریجان و جمالزاده، ۱۴۰۱: ۱۲۵).

۵ . ۲ . سامانه و شبکه‌های اطلاعات پشتوانه ارتکاب جرم

امروزه نقش فناوری اطلاعات و ارتباطات در تسهیل ارتکاب جرایم غیرقابل انکار است. اینترنت بستر جدیدی برای جرایمی فراهم کرده که پیشتر عمدتاً از طریق رسانه‌های سنتی مانند مطبوعات یا صداوسیما انجام می‌شد. تنوع امکانات اینترنتی، پایه محکمی برای انواع جرایم ایجاد کرده است. شبکه‌های رایانه‌ای پشتیبان جرایم متعددی از جمله هرزه‌نگاری به ویژه هرزه‌نگاری کودکان، تشویق کودکان به فحشا، نقض حریم خصوصی، جرایم مطبوعاتی و جرایم علیه شخصیت معنوی افراد هستند. قانون جرایم رایانه‌ای در فصل‌های چهارم و پنجم به جرایم علیه عفت و اخلاق عمومی و نیز هتک حیثیت و نشر اکاذیب پرداخته و رفتارهای مجرمانه‌ای که از طریق سامانه‌های اطلاعاتی تسهیل می‌شوند را هدف قرار داده است. در حوزه جرایم علیه عفت و اخلاق عمومی، قانون‌گذار سه گروه رفتار را جرم‌انگاری کرده: تولید و انتشار محتوای مستهجن، معاونت در دسترسی به این محتوا

و تحریک یا آموزش افراد برای ارتکاب جرایم اخلاقی. محتوای مستهجن بر اساس قانون شامل تصاویر، صداها یا متونی است که برهنگی کامل، اندام تناسلی یا روابط جنسی را نمایش می‌دهند. ماده ۱۴ قانون جرایم رایانه‌ای دو گروه از رفتارها را جرم‌انگاری می‌کند: انتشار، توزیع یا معامله محتوای مستهجن بدون در نظر گرفتن قصد مرتکب و نیز تولید یا ذخیره این محتوا با قصد تجارت یا فساد اخلاقی. معاونت در دسترسی به محتوای مستهجن نیز به صورت جداگانه جرم محسوب می‌شود. مواردی مانند تحریک، ترغیب یا تهدید افراد برای دسترسی به محتوای مستهجن یا تشویق آن‌ها به ارتکاب جرایم منافی عفت، مصرف مواد مخدر، خودکشی، انحرافات جنسی یا خشونت نیز جرم شناخته شده است. بااین‌حال، استفاده از اصطلاحات کلی مانند «انحرافات جنسی» بدون تعریف دقیق، بااصل شفافیت قوانین کیفری مغایرت دارد. همچنین بهتر بود به جرایمی مانند قاچاق انسان که در آن شبکه‌های رایانه‌ای برای فریب قربانیان استفاده می‌شود، اشاره می‌شد. در زمینه جرایم علیه شخصیت افراد، قانون از حریم خصوصی، محرمانگی مکاتبات و هویت افراد در برابر افترا و سوءاستفاده حمایت می‌کند. قانون جرایم رایانه‌ای در فصل پنجم سه رفتار مجرمانه را هدف گرفته: تحریف و انتشار محتوای صوتی، تصویری یا نوشتاری مربوط به دیگران، افشای اسرار یا داده‌های خصوصی بدون رضایت فرد و نیز نشر اکاذیب. این جرایم هم به امنیت عمومی و هم به حیثیت افراد مرتبط هستند، مانند نسبت‌دادن اعمال خلاف واقع به اشخاص حقیقی یا حقوقی با هدف آسیب‌رساندن یاایجاد تشویش. هرچند مقابله با سوءاستفاده از شبکه‌های رایانه‌ای ضروری است، اما جرم‌انگاری‌های مبهم و کلی می‌تواند به ابهام در اجرای قانون بینجامد. شفافیت در تعریف جرایم و توجه به مصادیق جدید مانند قاچاق انسان می‌تواند اثربخشی قانون را افزایش دهد (اعظمی، محمد سعید و طارمیان، فرهاد, ۱۳۹۹: ۲۹)(میرسلامی، واحدیاریجان و جمالزاده، ۱۴۰۱: ۱۲۷).

۵ . ۳ . سامانه و شبکه‌های اطلاعات وسیله ارتکاب جرم

تحولات فناوری رایانه‌ای و مخابراتی موجب گسترش جرایمی شده که پیش از ظهور شبکه‌های دیجیتال در قوانین کیفری جرم‌انگاری شده بودند. این سامانه‌ها و شبکه‌های اطلاعاتی ابزارهای جدیدی برای ارتکاب جرائم سنتی فراهم کرده‌اند. مواردی مانند جرائم علیه اموال، نقض مالکیت معنوی، قمار اینترنتی و تبلیغات فریبنده از این دسته‌اند. در حوزه مالی، با دیجیتالی شدن مبادلات بانکی و تجاری، فرصت‌های مجرمانه جدیدی مانند کلاهبرداری از طریق کارت‌های بانکی ایجاد شده است. حتی جرائمی مانند سرقت، کلاهبرداری و خیانت در امانت نیز در بستر اینترنت قابلیت اجرا یافته‌اند. در حقوق فرانسه، مسئله استفاده شخصی از تجهیزات رایانه‌ای محل کار توسط کارمندان به عنوان خیانت در امانت مطرح شده است. دیوان عالی این کشور در یک رأی، بازدید از

پایگاه‌های اینترنتی در ساعات کاری را مشمول استفاده حرفه‌ای دانست، اما در رأی دیگری، دسترسی به محتوای مستهجن را تخلف انضباطی شدید محسوب و اخراج کارمند را موجه اعلام کرد. قانون جرائم رایانه‌ای ایران در فصل سوم به جرائم مالی مانند سرقت و کلاهبرداری رایانه‌ای پرداخته است. سرقت رایانه‌ای شامل ربایش غیرمجاز داده‌ها از طریق کپی یا انتقال آنهاست، در حالی که کلاهبرداری رایانه‌ای بر کسب منافع مالی از طریق اعمالی مانند وارد کردن، تغییر یا تخریب داده‌ها در سامانه‌های رایانه‌ای استوار است. ماده ۲۵ این قانون سه گروه رفتار مجرمانه را هدف قرار داده است: تولید و توزیع ابزارهای الکترونیکی مختص جرائم رایانه‌ای مانند بدافزارها، انتشار داده‌های نفوذی مانند رمزهای عبور برای دسترسی غیرمجاز، و آموزش روش‌های ارتکاب جرائم سایبری. برای جرائمی که در آن‌ها از شبکه‌ها به عنوان ابزار استفاده می‌شود اما مجازات خاصی در قانون پیش‌بینی نشده، مانند نقض مالکیت معنوی، ماده ۵۲ به قوانین جزایی عام ارجاع داده است. کمیته تعیین مصادیق مجرمانه نیز فهرستی از محتوای غیرقانونی را در حوزه‌های گوناگون مانند امنیت، اخلاق عمومی، انتخابات و مالکیت فکری تهیه کرده که مبنای اقدامات پلیس فتا قرار می‌گیرد. این فهرست شامل مصادیقی مانند تحریک به جرم، محتوای ضد دینی و تخلفات انتخاباتی است و به قوانین متعدد دیگر استناد می‌کند (رهامی، روح اله و اژدری، امیرحسین, ۱۴۰۱: ۲۸۱)(ضیایی، سید یاسر و شکیب نژاد، احسان, ۱۳۹۶: ۲۳۵).

۶. پیشینه پژوهش

در بررسی پیشینه پژوهش مرتبط با جرائم سایبری علیه ورزشکاران زن، مطالعات متعددی به تحلیل ابعاد حقوقی مزاحمت و حمایت از زنان پرداخته‌اند. احمدی (۱۳۹۱) با تأکید بر آسیب‌پذیری زنان و کودکان، رویکرد حمایتی ماده ۶۱۹ قانون مجازات اسلامی و ضرورت تشدید مجازات مرتکبین را تحلیل کرده و مطالعه‌ای تطبیقی با قوانین آمریکا و انگلستان انجام داده است، هرچند به خلاءهای قانونی در زمینه جرائم سایبری اشاره‌ای نشده است (احمدی، ۱۳۹۱: ۸۶). اسدی و همکاران (۱۴۰۰) در بررسی قوانین ورزشی زنان ایران دریافتند که اگرچه در وضع قوانین مشکل جدی وجود ندارد، اما ضعف در اجرا و کمبود ضمانت‌های اجرایی موجب ناکارآمدی شده است. (اسدی، تجاری و نیک آئین، ۱۴۰۰: ۵۶۶). امینی و نادریان (۱۴۰۳) نیز بر لزوم بازنگری قوانین ورزش زنان با حفظ ارزش‌های دینی و تطبیق با استانداردهای بین‌المللی تأکید کرده‌اند (امینی و نادریان، ۱۴۰۳: ۲۸۰). از سوی دیگر، پیلارینو (۲۰۲۰) در پژوهش تجربی خود در یونان و انگلستان، به بررسی جرم تعقیب پرداخته و نیاز به قانون‌گذاری خاص در یونان و افزایش آگاهی عمومی به ویژه در مورد مزاحمت سایبری و قربانیان مرد را خاطرنشان ساخته است (پیلارینو، ۲۰۲۰: ۱۲). این مطالعات نشان می‌دهد که علی‌رغم پیشرفت‌های قانونی، چالش‌های جدی در

زمینه اجرا، روزآمدسازی قوانین با توجه به تحولات فناوری‌های سایبری و توجه به ابعاد فرهنگی همچنان باقی است.

پژوهش‌ها نشان می‌دهند که آزار سایبری به عنوان یکی از شایع‌ترین اشکال جرائم سایبری، در قالب پیام‌های تهدیدآمیز، نظرات جنسیت زده، و حملات سازمان یافته در فضای مجازی علیه ورزشکاران زن ظهور یافته است (فورسدایک و گیلز، ۲۰۲۴: ۳۲۵۸)[1]. این رفتارها اغلب با هدف تحقیر، کاهش اعتمادبه نفس، و محدودسازی حضور حرفه‌ای زنان در ورزش صورت می‌گیرد. از منظر جرم‌شناسی، نظریه‌های فعالیت روزمره[2] توضیح می‌دهند که چگونه سه گانهٔ «فرصت»، «هدف مناسب»، و «نبود محافظت کافی» در فضای مجازی، ورزشکاران زن را به قربانیان ایدئال تبدیل می‌کند (کوهن-آلماگور، ۲۰۲۰: ۷۷). در حوزهٔ انتشار غیرمجاز تصاویر خصوصی، مطالعاتی مانند گزارش سازمان ملل متحد در سال ۲۰۲۱ (زنان سازمان ملل) تأکید می‌کنند که ورزشکاران زن به دلیل شهرت رسانه‌ای، بیشتر در معرض نقض حریم خصوصی از طریق هک دستگاه‌های شخصی یا نشت عمدی تصاویر قرار می‌گیرند. نمونه‌های بارز این موارد، همچون نقض حریم شخصی ورزشکاران المپیکی در پیاده‌سازی ابری[3] در سال ۲۰۱۴، نشان دهندهٔ ضعف قوانین کیفری در پیشگیری از جرائم سایبری است. از منظر حقوقی، کنوانسیون بوداپست (۲۰۰۱) به‌عنوان چارچوب بین‌المللی مبارزه با جرائم سایبری، هرچند به حمایت از قربانیان می‌پردازد، اما اجرای آن در موارد مرتبط با جنسیت و ورزش نیازمند اصلاحات خاص است (کنسول اروپا، ۲۰۱۸)[4]. از سوی دیگر، نقض حریم خصوصی ورزشکاران زن اغلب با سوءاستفاده از فناوری‌های نوین مانند نرم افزارهای جاسوسی یا دوربین‌های پنهان همراه است. پژوهش‌های جرم‌شناسی نشان می‌دهد که انگیزه‌های مجرمانه در این حوزه، از ترکیبی از حسادت، تفکرات پدرسالارانه، و تمایل به کنترل بدن زنانه نشئت می‌گیرد (پاول و همکاران، ۲۰۲۴: ۳۱). در حقوق کیفری ایران، ماده ۱۶ قانون جرائم رایانه‌ای (۱۳۸۸) انتشار غیرمجاز تصاویر خصوصی را جرم دانسته، اما ابهام در تعریف «حریم خصوصی» و فقدان سازوکارهای فنی برای اثبات جرم، چالش‌هایی در پی داشته است. مطالعهٔ تطبیقی در نظام‌های حقوقی نشان می‌دهد که کشورهایی مانند فرانسه و کانادا با تصویب قوانین خاص مانند «حق فراموشی»[5] و الزام پلتفرم‌ها به حذف محتوای غیراخلاقی، گام‌های مؤثری در حمایت از ورزشکاران زن برداشته‌اند (ویلسون و کر، ۲۰۲۳: ۲۸۲) (پارلمان اروپا، ۲۰۲۰)[6]. همچنین، پژوهش‌های جرم‌شناسی بر نقش سواد دیجیتال و آموزش مهارت‌های امنیتی به

1. Forsdike & Giles
2 .Routine Activity Theory
3. iCloud
4. Council of Europe
5. Right to be Forgotten
6. European Parliament

ورزشکاران برای کاهش قربانی شدگی تأکید دارند. در زمینهٔ روانشناسی قربانی، پژوهش‌هایی مانند مطالعهٔ سازمان بهداشت جهانی (۲۰۲۳) بیان می‌کنند که آزار سایبری موجب اضطراب، افسردگی، و حتی انزوا از فعالیت‌های ورزشی در میان زنان می‌شود. این در حالی است که نظریه‌های فمینیستی حقوقی، مانند نظریهٔ امنیت جنسیتی در فضای مجازی، لزوم بازتعریف قوانین را با توجه به تجارب خاص زنان پررنگ می‌کنند (فینک، ۲۰۱۵: ۳۳۷)(ویلسون و کر، ۲۰۲۳: ۲۸۴)[1]. در پایان، شکاف‌های پژوهشی موجود شامل کمبود مطالعات میدانی درباره تأثیرات بلندمدت جرائم سایبری بر مشارکت زنان در ورزش، و نیز نبود داده‌های آماری دقیق در کشورهای درحال توسعه است. مرور منابع نشان می‌دهد که ادغام یافته‌های حقوق کیفری، جرم‌شناسی، و فناوری اطلاعات می‌تواند به تدوین راهبردهای جامع تر برای مقابله با این پدیده بینجامد.

۷ . روش پژوهش

در بررسی روش شناسی جرائم سایبری علیه ورزشکاران زن، ابتدا رویکرد تحلیلیِ ترکیبی از حقوق کیفری و جرم‌شناسی با تمرکز بر سه محور اصلیِ آزار سایبری، انتشار غیرمجاز تصاویر، و نقض حریم خصوصی اتخاذ می‌شود. از منظر حقوق کیفری، تحلیل قوانین داخلی و بین‌المللی مرتبط با جرائم سایبری، مانند قانون جرائم رایانه‌ای ایران (مصوب ۱۳۸۸)، کنوانسیون بوداپست در مورد جرائم سایبری (۲۰۰۱)، و قوانین حمایت از داده‌های شخصی در اتحادیه اروپا (GDPR)، ضروری است. به ویژه، بررسی ماده ۷۴۴ قانون مجازات اسلامی ایران (تعزیرات مرتبط با انتشار تصاویر خصوصی) و ماده ۱۶ قانون جرائم رایانه‌ای (مجازات اخلال در حریم خصوصی) به عنوان مبانی حقوقیِ مقابله با این جرائم مورد توجه قرار می‌گیرد. در سطح بین‌المللی، اسنادی مانند قطعنامه ۲۰۲۱ سازمان ملل در مورد خشونت سایبری علیه زنان و دختران و رویه‌های قضایی کشورهایی مانند آلمان (مطابق §۲۰۱a قانون جزای آلمان) و ایالات متحده (قانون امنیت سایبری و حریم خصوصی ورزشکاران زن، ۲۰۲۲) نیز تحلیل می‌شوند. از دیدگاه جرم‌شناسی، نظریه‌های سنتی مانند نظریه فعالیت روزمره[2] که بر سه عنصر مجرمانِ انگیزه دار، اهداف مناسب، و نبود محافظت کافی تأکید دارد، برای تبیین علل وقوع این جرائم به کار می‌رود. همچنین، نظریه‌های فمینیستی جرم‌شناسی[3] که به تحلیل قدرت جنسیتی و ساختارهای مردسالارانه در شکل گیری جرائم علیه زنان می‌پردازند، به منظور بررسی ریشه‌های فرهنگی-اجتماعی آزار آنلاین ورزشکاران زن استفاده می‌شوند. در این زمینه، پژوهش‌های میدانی شامل مصاحبه با قربانیان، تحلیل پروفایل‌های

1. Fink
2. Routine Activity Theory
3. Feminist Criminology

شبکه‌های اجتماعی ورزشکاران زن، و بررسی آمارهای سازمان‌های بین‌المللی در مورد آزار سایبری مبتنی بر جنسیت، داده‌های تجربی لازم را فراهم می‌کند. علاوه بر این، مطالعه موردی پرونده‌های قضایی نظیر پرونده‌ی بازیکن فوتبال زن اسپانیایی جنیفر هرموسو[1] (۲۰۲۳) که با انتشار غیرمجاز تصاویر خصوصی مواجه شد، یا پرونده‌ی آزار سایبری بازیکن تنیس نائومی اوساکا[2] (۲۰۲۱)، به درک بهتر الگوهای رفتاری مجرمان و آسیب پذیری‌های خاص ورزشکاران زن کمک می‌کند. در بخش تحلیل فنی، روش‌های مورد استفاده مجرمان سایبری، مانند فیشینگ برای دسترسی به حساب‌های شخصی، استفاده از نرم‌افزارهای جاسوسی[3]، و سوءاستفاده از هوش مصنوعی برای ساخت محتواهای جعلی[4]، با استناد به گزارش‌های مرکز مبارزه با جرائم سایبری پلیس بین‌الملل (۲۰۲۲) و پژوهش‌های دانشگاهی مانند مطالعه‌ی لوک فلت و همکاران در مجله‌ی «جرائم سایبری و حریم خصوصی»، بررسی می‌شوند (لوکفلد و یار، ۲۰۱۶: ۲۷۳)[5]. همچنین، نقش پلتفرم‌های اجتماعی مانند اینستاگرام و توئیتر در تسهیل یا مهار این جرائم، با تحلیل سیاست‌های گزارش محتوای آزاردهنده[6] و همکاری این شرکت‌ها با نهادهای حقوقی، ارزیابی می‌گردد. در حوزه حقوق تطبیقی، مقایسه‌ی نظام‌های حقوقی کشورهای اسلامی (مانند عربستان سعودی با قانون جرائم سایبری ۲۰۰۷ و ماده‌ی ۳ قانون حریم خصوصی ۲۰۲۰) و کشورهای غربی (مانند فرانسه با قانون شوالیه ۲۰۲۰ در مورد انتشار غیرمجاز تصاویر خصوصی) نشان می‌دهد که تفاوت در تعریف «حریم خصوصی» و «آزار جنسیتی» چگونه بر سطح حمایت از ورزشکاران زن تأثیر می‌گذارد. در این زمینه، آرای فقهی مانند نظریه‌ی «حفظ العرض» در اسلام که طبق آیه‌ی ۱۲ سوره‌ی حجرات («...وَلَا تَجَسَّسُوا...») و روایات امام علی (ع) درباره‌ی حرمت تجسس، به حمایت از حریم خصوصی اشاره دارد، به عنوان مبانی دینیِ مقابله با جرائم سایبری تحلیل می‌شود. همچنین، اسناد بین‌المللی اسلامی مانند اعلامیه‌ی قاهره درباره‌ی حقوق بشر در اسلام (۱۹۹۰) که در ماده‌ی ۱۸ بر حق محرمانگی ارتباطات تأکید می‌کند، مورد بررسی قرار می‌گیرد. منابع مورد استفاده شامل متون حقوقی (کتاب «حقوق بین‌الملل و فضای سایبری » اثر تساگوریاس و بوکان ، ۲۰۲۱)[7]، مقالات علمی (مطالعه‌ی آلیسا کوئن در مجله‌ی «جرم‌شناسی جنسیتی»، ۲۰۲۱)، گزارش‌های سازمانی (گزارش یونسکو درباره‌ی امنیت سایبری زنان، ۲۰۲۲)، و اسناد قضایی (رأی دادگاه اروپایی حقوق بشر در پرونده‌ی سودرمن سوئد[8] درباره‌ی انتشار غیرمجاز تصاویر) است. داده‌های آماری نیز از

1. Jenni Hermoso
2. Naomi Osaka
3. Spyware
4. Deepfake
5. Leukfeldt & Yar
6. Content Moderation Policies
7. Tsagourias & Buchan
8. Söderman v. Sweden

پایگاه‌های معتبر مانند مرکز پژوهشی پیو[1] که نشان می‌دهد ۶۷٪ ورزشکاران زن حرفه‌ای در اروپا حداقل یکبار آزار سایبری را تجربه کرده‌اند، استخراج می‌شوند. این روش شناسیِ ترکیبی، با هدف ارائه‌ی تحلیلی جامع از ابعاد حقوقی، جرم‌شناختی، و فنیِ جرائم سایبری علیه ورزشکاران زن طراحی شده است (ضیایی و شکیب نژاد, ۱۳۹۶: ۲۳۳).

۸ . یافته‌های پژوهش

در نظام حقوقی ایران، جرائم سایبری علیه زنان ورزشکار تحت شمول قوانینی مانند ماده ۶۰۸ تعزیرات قانون مجازات اسلامی (توهین و فحاشی) و قانون جرایم رایانه‌ای مصوب ۱۳۸۸ قرار می‌گیرند. بر اساس ماده ۱۶ این قانون، انتشار تصاویر یا فیلم‌های خصوصی بدون رضایت فرد، حتی بدون ورود ضرر مادی، جرم محسوب شده و مجازات حبس تا دو سال یا جزای نقدی تا ۴۰ میلیون ریال دارد. همچنین، مطابق ماده ۱۸ قانون جرایم رایانه‌ای، انتشار اکاذیب با هدف تشویش اذهان عمومی یا هتک حیثیت، مجازات مشابهی را به دنبال دارد انتشار غیرمجاز تصاویر و اطلاعات شخصی ورزشکاران زن در فضای مجازی، نه تنها نقض حریم خصوصی است، بلکه تحت عنوان جرم سایبری قابل پیگرد است. در فقه اسلامی، حریم خصوصی به عنوان حقی ذاتی برای حفظ کرامت انسانی شناخته شده و آیاتی مانند «وَلَا تَجَسَّسُوا» (حجرات:۱۲) بر لزوم پرهیز از تجسس تأکید می‌کنند. آزارهای کلامی و تهدیدهای مبتنی بر جنسیت در فضای مجازی، مصداق خشونت روانی محسوب می‌شوند. در حقوق کیفری ایران، این رفتارها تحت عنوان توهین یا افترا قابل تعقیب هستند. برای مثال، طبق ماده ۶۰۹ تعزیرات قانون مجازات اسلامی، توهین به افراد با توجه به جایگاه اجتماعی آن‌ها، مجازات حبس تا شش ماه را در پی دارد . هنجارهای جنسیتی و نگرش های مردسالارانه در برخی جوامع، ورزشکاران زن را به‌ویژه در معرض جرائم سایبری قرار می‌دهد. مطالعات نشان می‌دهد که ۸۳٪ قربانیان آزار سایبری در ورزش را زنان تشکیل می‌دهند . در ایران، برخی محدودیت‌های قانونی بر حضور زنان در عرصه‌های ورزشی (مانند ممنوعیت مسابقات بدنسازی) به تشدید این آسیب پذیری کمک می‌کند . نبود نهادهای مستقل برای حمایت از قربانیان و گزارش دهی جرائم سایبری، باعث سکوت بسیاری از ورزشکاران زن می‌شود. پژوهش‌ها نشان می‌دهد تنها ۱۲٪ از موارد آزار سایبری به مراجع قضایی گزارش می‌شود. افزایش دسترسی به ابزارهای دیجیتال و نرم‌افزارهای هک، امکان نقض حریم خصوصی ورزشکاران را تسهیل می‌کند. برای نمونه، هک حساب‌های شخصی و انتشار تصاویر خصوصی، از رایج‌ترین جرائم گزارش شده است. قرآن کریم در آیات متعددی بر حفظ حرمت افراد تأکید دارد، از جمله «وَلَا يَغْتَب بَّعْضُكُم

1. https://www.pewresearch.org

بَعْضًا» (حجرات:۱۲) که از غیبت منع می‌کند. انتشار غیراخلاقی تصاویر یا اطلاعات خصوصی ورزشکاران زن، مصداق بارز نقض این اصل است . بر اساس آموزه‌های فقهی، هرگونه تعرض به حریم خصوصی دیگران، حتی در فضای مجازی، حرام تلقی شده و مسئولیت شرعی و حقوقی به همراه دارد (میرسلامی، واحدیاریجان و جمالزاده، ۱۴۰۱: ۱۰۷).

در عصر دیجیتال شاهد ظهور جرایم سایبری متنوع و نوظهوری هستیم که ماهیتی کاملاً جدید دارند. برای بهره‌برداری ایمن از فناوری‌های رایانه‌ای، ضروری است کاربران شخصی، سازمان‌ها و نهادهای حکومتی از امنیت داده‌ها، سامانه‌ها و فرآیندهای دیجیتال اطمینان حاصل کنند. در این راستا، نهادهای قضایی، انتظامی و وزارت اطلاعات و ارتباطات با وضع مقررات و قوانین، بستر امن فعالیت در فضای سایبری را فراهم می‌کنند و مجرمان را بر اساس چارچوب‌های قانونی مجازات می‌نمایند. پرسش اساسی این است که قوه قضاییه در چه حوزه‌هایی از امنیت سایبری مداخله می‌کند؟ با توجه به اینکه وضع قوانین کیفری (از جمله جرایم سایبری) در صلاحیت مجلس و اجرای آن بر عهده قوه قضاییه است، باید به قوانین مصوب مجلس که برای اجرا ابلاغ شده‌اند، مراجعه کرد. در این زمینه، لایحه جرایم سایبری که توسط قوه قضاییه تهیه و به دولت و مجلس ارسال می‌شود، مشخص می‌کند چه مواردی جرم‌انگاری شده و چه مجازات‌هایی برای آنها پیش‌بینی شده است. قوانین ماهوی جرایم سایبری به بررسی این موضوع می‌پردازند که آیا انواع جرایم سایبری در قوانین خاص یا حقوق جزای عمومی جرم انگاری شده‌اند یا خیر. این جرایم شامل طیف وسیعی از فعالیت‌های مجرمانه می‌شود: جرایم مرتبط با سامانه‌های رایانه‌ای، شبکه‌ها و تلفن‌های هوشمند؛ جرایم مربوط به نرم‌افزارها و داده‌های الکترونیکی؛ و استفاده از رایانه به عنوان ابزار ارتکاب جرم. نمونه‌های بارز این جرایم عبارتند از: دسترسی غیرمجاز، تخریب یا دستکاری داده‌ها، ایجاد اختلال در عملکرد سامانه‌ها، کلاهبرداری الکترونیکی (فیشینگ)، جعل اسناد الکترونیکی، تولید و انتشار محتوای مستهجن، نقض حقوق مالکیت فکری، انتشار اطلاعات نادرست، جرایم سازمان‌یافته و استخراج غیرقانونی داده‌های کلان. هرچند قانون فعلی عمدتاً بر جرایم سنتی متمرکز است، بسیاری از جرایم نوظهور در حوزه‌هایی مانند هوش مصنوعی، متاورس[1] و ارزهای دیجیتال به‌صورت شفاف جرم انگاری نشده‌اند. برخی از این جرایم مانند تشویق به خودکشی یا انتشار عمدی اطلاعات پزشکی غلط ممکن است تحت عناوین کلی‌تری مانند "تحریک به فساد" پیگیری شوند، اما در قانون مجازات اسلامی جرم مستقلی برای آن‌ها تعریف نشده است.

1. Metaverse

۹ . شیوه‌های ارتکاب جرم با فناوری‌های نوین سایبری

شیوه‌های مجرمانه متعددی در جرایم سایبری بکار می‌رود. بهره‌گیری از هوش مصنوعی سایبری افزون بر سودمندی‌های فراوان، به عنوان ابزاری برای کلاهبرداری و یا تخریب، توسط مجرمین سایبری بکار می‌رود. اصطلاح دیپ فیک در هوش مصنوعی نخستین بار در سال ۱۳۹۷ توسط یکی از مدیران شرکت ردیت ابداع شد. او یک زیر گروه ساخت که کاربران بتوانند پورنوگرافی و تصاویر دیپ‌فیکی افراد مشهور را با یکدیگر مبادله کنند و از همان زمان تاکنون اصطلاح دیپ فیک برای تولید نوعی از رسانه های جعلی توسط هوش مصنوعی رایج شد و همچنان بکار می رود (مسعود و همکاران، ۲۰۲۲: ۲۷)[1]. اگرچه کلاهبرداری سایبری جرم انگاری شده، اما استفاده از ابزارهای پیشرفته‌ای مانند دیپ فیک[2] برای فریب یا انتشار اخبار جعلی به صورت خاص که در ده سال گذشته بوجود آمده، در قوانین کیفری نیامده است. بدافزارها[3] نوع دیگری از ابزارهای مجرمانه سایبری هستند که مدام به روز رسانی، پیچیده تر و شیوه و نوع حمله آنها تغییر می‌کند. باج‌افزار نوعی نرم‌افزار مخرب (بدافزار) هستند که دسترسی سامانه‌های کامپیوتری یا فایل‌ها را محدود می‌کند و برای آزادسازی آنها اغلب مجرم درخواست باج می‌کند. مهاجمان معمولاً داده‌ها را رمزگذاری یا سامانه‌ها را قفل می‌کنند، سپس تهدید می‌کنند که در صورت عدم پرداخت باج، دسترسی را برای همیشه مسدود یا اطلاعات سرقت شده را منتشر می‌کنند. نمونه‌هایی از بدافزارها شامل ویروس‌ها، کرم‌ها، جاسوس‌افزارها و ابزارهای تبلیغاتی مزاحم هستند (الاختر و همکاران، ۲۰۲۰: ۱۳۷۲۹۵)[4]. فیشینگ و کلاهبرداری بهره گیری از نوعی بدافزار است که با بدست آوردن اطلاعات شخصی فرد مانند داده های کارت بانکی، و رمز ورود به حسابها انجام می شود. متن حمله فیشینگ با ایمیل عموما مبتنی بر طبیعت آدمی برای رسیدن به موفقیت و بر اصول مهندسی اجتماعی بنا نهاده شده است. در کلاهبرداری فیشینگ، ممکن است با دریافت ایمیلی آغاز شود که به نظر می‌رسد از یک کسب و کار قانونی است و از شما می‌خواهد با پاسخ دادن به ایمیل یا بازدید از یک وب‌سایت به ظاهر معتبر مشابه سایت موسسات مالی معتبر، اطلاعات شخصی خود را به‌روزرسانی یا تأیید کنید. آدرس وب ممکن است شبیه به آدرسی باشد که قبلاً استفاده کرده‌اید فیشینگ از واژه ماهیگیری اقتباس شده و ایمیل نقش طعمه و فرد نقش ماهی را در آن ایفا می کند. برنامه فیشینگ در چهارسال اخیر منتهی به ۱۴۰۴ به مقدار ۴۹٪ افزایش یافته است که ۶۵٪ حمله به سازمانها و ۳۵٪ حمله به افراد انجام شده است[5]. (مونسی و سیوباتارو، ۲۰۲۵: ۱۰۰۱۲۵)[6].

1. Masood
2. Deepfake
3. Malware
4. Al-Khater
5. https://hoxhunt.com/guide/phishing-trends-report
6. Mouncey & Ciobotaru

سرقت هویت زمانی رخ می‌دهد که مجرمان اطلاعات شخصی را برای سرقت وجوه، دسترسی به داده‌های محرمانه یا ارتکاب کلاهبرداری به دست می‌آورند. کیت‌های اکسپلویت برای به دست آوردن کنترل رایانه کاربر به یک آسیب‌پذیری (اشکال در کد یک نرم‌افزار) نیاز دارند. تعقیب سایبری از طریق وب‌سایت‌ها، موتورهای جستجو، رسانه‌های اجتماعی انجام می شود. تولید، نگهداری و انتشار محتوای غیرقانونی آنلاین، از جمله مطالب سوءاستفاده جنسی از کودکان، تحریک به نفرت نژادی، تحریک به اقدامات تروریستی و تجلیل از خشونت،... تزریق (SQL) [1] نوع رایجی از حملات سایبری است که در آن هکرها از یک آسیب‌پذیری امنیتی استفاده می‌کنند و به داده های موجود در بانک داده های سایت ها دسترسی پیدا می کنند و هر کاری را می توانند با داده ها ازجمله حذف یا تغییر آنها را انجام دهد. تزریق اس کیوال که جرمی سایبری بشمار می آید به طور مؤثر از کدهای مخرب استفاده می‌کند. تونل‌زنی DNS که حدود دو دهه است نخستین عمل مجرانه از طریق آن گزارش شده است اکنون یکی از تهدیدهای مهم بشمار می‌آید که دسترسی غیر مجاز به داده ها، استخراج داده ها، نقشه برداری و اکتشاف شبکه، اثرات مالی و عملیاتی و کانالهای فرمان و کنترل شبکه را ممکن است بدون شناسایی تحت تاثیر قرار دهد. تونل زنی نوعی حمله مجرمانه سایبری بشمار می آید که برای دور زدن اقدامات امنیتی سنتی رایانه ها و شبکه ها بکار می رود. تونل‌سازی DNS تکنیکی است که برای ارسال و دریافت داده ها از طریق فیلدهای میزبان یا زیر دامنه های آن استفاده می کند. برای پنهان کردن ترافیک، پروتکل‌ها یا نرم‌افزارهای مخرب به عنوان پرس‌وجوهای DNS و ... است از پروتکل DNS برای انتقال داده‌ها سوءاستفاده می‌کند و اغلب اقدامات امنیتی را دور می‌زند. اصطلاح اینترنت اشیا (IoT)[2] در سال ۱۳۷۸ توسط کوین اشتون[3] از دانشگاه MIT ابداع و برای ارتباط و کنترل اشیاء گوناگون استفاده شد. این ارتباط سایبری قابلیت‌های فراوان و سودمندی در ارتباط هوشمند میان اشیای موجود در منزل، محل کار، کارخانه های صنعتی، سازمان‌ها، خودروهای گوناگون، ... مانند دوربین‌های امنیتی، تجهیزات تولیدی، مانیتورهای کیفیت هوا یا ... برای افراد و سازمانها ایجاد می کند. برای نمونه به خودروهای خودران می توان اشاره کرد. با توسعه فناوری، کنترل همه اشیا به سمت الکترونیکی شدن و از راه دور به سرعت در حال پیشرفت است. از سوی دیگر، ممکن است شبکه اینترنت اشیا برای حمله به این سامانه‌ها برای ایجاد اختلال یا سرقت داده‌ها، مورد استفاده مجرمین سایبری قرار گیرند که عموما ایمنی ارتباطی کم دارند. جرائم سایبری مربوط به اینترنت اشیا که توسعه بسیار زیادی در جهان پیدا کرده است در قانون مجازات اسلامی جرم انگاری نشده است که امکان سوء استفاده مجرمین سایبری را بیشتر و آسان‌تر می‌کند. حمله انکار سرویس

1. SQL Injection
2. Internet of Things (IoT)
3. Kevin ashton

(DoS) نوعی حمله سایبری است که توسط مالویرها[1] انجام می‌شود، با این حمله، یا کلا سرویس قطع می‌شود و یا کند می شود. بعبارتی مالویر ارتباط رایانه با سرور، منبع، ماشین و یا شبکه را قطع و یا کند می‌کند. به این ترتیب اگر کاربری از سرور سرویسی درخواست نماید سرور پاسخ نمی دهد به همین دلیل انکارسرویس نامیده می شود. در این حالت سرور قابل دستیابی توسط کاربر نیست. مالویر این کار را با افزایش ترافیک در سرور ایجاد می کند. بعبارتی بجای یک درخواست، تعداد زیادی درخواست از کاربر به سرور ارسال می شود که امکان پاسخ به آنها را ندارد لذا کند عمل می کند یا قطع می شود. حال اگر تعداد زیادی رایانه با سرور ارتباط داشته باشد (این رایانه ها با هم تشکیل یک بات‌نت را می دهند) و این اتفاق بیفتد (سیلی از درخواست‌ها به سرور ارسال شود) شرایط بسیار بدتر خواهد شد. این حالت را انکار سرویس توزیع‌شده (DDoS[2])، می نامند. در این حالت، سرور با شبکه ای از رایانه های آلوده به مالویر ارتباط دارد که بات‌نت (BoTNET) نامیده می شود. در این حالت سرور آلوده به مالویر نیست اما بدلیل درخواست های زیاد امکان پاسخ را ندارد. این نوع حملات سایبری توسط کاربر قابل تشخیص نیست. در صورت شناسایی بات نت ها که شبکه ای از رایانه های کنترل شده توسط یک بازیگر بدخواه است، از قوانینی که دسترسی غیرمجاز به سامانه‌های رایانه‌ای، تغییر داده‌ها و توزیع نرم‌افزارهای مخرب را ممنوع می‌کنند، می توان در جرم نگاری آنها بهره گرفت. جرم نگاری این جرائم با بهره گیری از شبکه‌های رباتیک تاکنون توسعه کافی نیافته است. یک حمله انکار سرویس توزیع‌شده که سرور هدف را تحت الشعاع قرار می‌دهد با غرق کردن یک سرویس آنلاین با ترافیک بیش از حد، از مکان‌ها و منابع گوناگون، آن را از دسترس خارج می‌کنند و یا زمان پاسخگویی وب‌سایت کند می‌شود. اغلب برای ایجاد اختلال در مشاغل، وب‌سایت‌ها یا حتی کل شبکه‌ها به دلایل مختلف، از جمله اخاذی، اعتراض یا خرابکاری از این حملات استفاده می‌شود. در یک حمله انکار سرویس، مهاجم یک سامانه، سرور یا شبکه را با ترافیک و درخواست‌های دروغین پر می‌کند و آن را برای کاربران قانونی غیرقابل دسترس می‌کند. اسب‌های تروجان، مالویر دیگری است که از یک برنامه مخرب که درون یک برنامه به ظاهر مشروع پنهان شده است، استفاده می‌کند. حملات تروجان در پشتی شامل برنامه‌های مخربی است که می‌توانند به طور فریبنده‌ای بدافزار یا داده نصب کنند نخست به نظر می‌رسد یک نرم‌افزار مشروع است و شرایط را برای عملیات های دیگر مانند دسترسی به داده های رایانه و بات‌نت را فراهم می نماید. در کلیه شیوه های بهره گیری سایبری، میزان جرم سایبری افزایش داشته و در سالهای اخیر در حال رشد بوده است (مسعود و همکاران، ۲۰۲۲: ۲۷).

---

1. malware
2. Denial of service (DoS)

۱.۹. جرم‌های سایبری فراسرزمینی

بسیاری از جرایم سایبری از مکان‌های جغرافیایی مختلف خارج از مرزهای کشورها ارتکاب می‌یابند که پیگیری و اعمال مجازات آنها مستلزم توافقنامه‌های دوجانبه و چندجانبه بین‌المللی مانند کنوانسیون بوداپست، لانزاروته[1]، استانبول[2] و کنوانسیون جرایم سایبری سازمان ملل[3] است. با این حال، همکاری بین‌المللی در این حوزه با چالش‌های متعددی مواجه است، از جمله عدم توسعه زیرساخت‌های حقوقی کافی، تفاوت در فرآیندهای قضایی، ناهمخوانی قوانین کیفری، اختلاف در تعریف جرایم، مسائل صلاحیت قضایی و تفاوت در نظام‌های مجازات‌ها. علاوه بر این، موانع زبانی و تفاوت‌های ایدئولوژیک نیز بر پیچیدگی رسیدگی به پرونده‌های فرامرزی می‌افزاید. از سوی دیگر، مدیریت شرکت‌های ارائه‌دهنده خدمات اینترنتی و آموزش شهروندان درباره جرایم سایبری به صورت موردی و محدود انجام شده است. در این زمینه، توسعه «شهروندی دیجیتال» با نه بُعد اساسی شامل قانون دیجیتال، آداب دیجیتال، ارتباطات دیجیتال، حقوق و مسئولیت‌های دیجیتال، تجارت دیجیتال، سلامت دیجیتال، دسترسی دیجیتال، امنیت دیجیتال و فرهنگ دیجیتال، برای استفاده ایمن و مسئولانه از فناوری‌های دیجیتال ضروری است. این آموزش‌ها به ویژه برای گروه‌های آسیب‌پذیر مانند سالمندان، افراد کم‌سواد، ناآشنا با فناوری و همچنین ورزشکاران زن که به دلیل مشغله‌های حرفه‌ای در معرض خطر بیشتری هستند، حیاتی می‌باشد. آگاهی‌بخشی به کاربران از طریق نهادهایی مانند صدا و سیما، آموزش و پرورش، وزارت ارتباطات و نیروی انتظامی می‌تواند نقش مؤثری در پیشگیری از جرایم سایبری و کاهش آسیب‌پذیری‌های اجتماعی ایفا کند (صادقی، بدلی ملکی و اسلامی، ۱۴۰۳: ۴۸).

بحث و نتیجه‌گیری

پدیده جرائم سایبری علیه ورزشکاران زن، به ویژه در قالب آزارهای آنلاین، انتشار غیرمجاز تصاویر، و نقض حریم خصوصی، نه تنها به عنوان یک چالش فردی، بلکه به مثابه تهدیدی برای ساختارهای اجتماعی و ارزش‌های اخلاقی جوامع محسوب می‌شود. تحلیل حقوق کیفری و جرم‌شناختی این جرائم نشان می‌دهد که ماهیت چندلایه این آسیب‌ها نیازمند رویکردی جامع است که همزمان به ابعاد قانونی، فنی، فرهنگی، و اخلاقی توجه کند. از منظر حقوق کیفری، قوانین موجود در حوزه جرائم سایبری، مانند مواد ۱۶ و ۱۷ قانون جرائم رایانه‌ای ایران، انتشار محتوای مجرمانه و نقض

1. Lanzarote Convention
2. Istanbul Convention
3. United Nations Convention on Cybercrime

حریم خصوصی را جرم‌انگاری کرده‌اند. ماده ۷۴۲ تعزیرات قانون مجازات اسلامی نیز با تأکید بر «هتک حرمت اشخاص» و ماده ۶۶۹ تعزیرات در خصوص توهین و افترا، چارچوبی برای پیگیری قضایی این جرائم فراهم می‌کند. با این حال، چالش اصلی در اجرای مؤثراین قوانین نهفته است. برای مثال، انتشار غیرمجاز تصاویر ورزشکاران زن، اغلب با استفاده از پلتفرم‌های فراسرزمینی انجام می‌شود که پیگیری آن‌ها مستلزم همکاری‌های بین پایگاهی و تقویت زیرساخت‌های فنی مراجع قضایی است. افزون بر این، تعریف دقیق «آزار سایبری» در قوانین داخلی نیازمند بازنگری است تا مصادیقی چون «حمله سازمان یافته به ورزشکاران زن در فضای مجازی» یا «استفاده از ربات‌ها برای اشاعه توهین‌های جنسیتی» را به طور شفاف پوشش دهد. از نگاه جرم‌شناختی، جرائم سایبری علیه زنان ورزشکار ریشه در بسترهای فرهنگی و ساختارهای قدرت نابرابر جنسیتی دارد. نظریه «فرهنگ تجاوز»[1] توضیح می‌دهد که چگونه عادی سازی خشونت کلامی و جنسی در فضای مجازی، به ویژه در محیط‌های مردانه مانند برخی جوامع ورزشی، به تشدید این جرائم دامن می‌زند (آنگوا اومادوکو، ۲۰۲۴: ۷۴۰). پژوهش‌ها نشان می‌دهد ورزشکاران زنِ موفق و برجسته، به دلیل به چالش کشیدن کلیشه‌های جنسیتی، بیشتر در معرض حملات سایبری قرار می‌گیرند. این حملات نه تنها با هدف تحقیر فردی، بلکه برای بازتولید هنجارهای سنتیِ حاکم بر عرصه ورزش طراحی می‌شوند (فنک، ۲۰۱۵). از سوی دیگر، نظریه «فعالیت روزمره» بیانگر آن است که سه عامل «انگیزه مرتکب»، «هدف مناسب»، و «نبود محافظت کافی» در فضای مجازی، شرایط ارتکاب این جرائم را تسهیل می‌کند. ورزشکاران زن به دلیل حضور پررنگ در رسانه‌ها و دسترسی‌پذیری اطلاعات شخصی، به «اهدافی جذاب» برای مجرمان تبدیل می‌شوند، درحالی که ضعف سامانه‌های نظارتی پلتفرم‌های اجتماعی و ناآگاهی برخی قربانیان از سازوکارهای گزارش‌دهی، به بی توجهی به عامل سوم می‌انجامد. در حوزه فقه اسلامی، می‌توان با استناد به اصولی چون «نفی ضرر» (لَا ضَرَرَ وَلَا ضِرَارَ)، «حفظ نوامیس» (وَلاَ تُبْدِينَ زِينَتَهُنَّ إِلاَّ مَا ظَهَرَ مِنْهَا - النور:۳۱)، و «حرمت اهانت به مؤمن» (مَنِ اتَّقَى اللَّهَ لَمْ يُتْهَمْ)، چارچوبی اخلاقی-حقوقی برای مقابله با این جرائم ترسیم کرد. قاعده «لاضرر» به صراحت هرگونه اقدام آسیب‌رسان، از جمله آزار روانی از طریق فضای مجازی را ممنوع می‌داند. همچنین، مسئولیت نهادهای ورزشی در «امر به معروف و نهی از منکر» ایجاب می‌کند که با ایجاد سازوکارهای پیشگیرانه (مانند آموزش ورزشکاران و استخدام ناظران اخلاقی در پلتفرمهای مرتبط)، از اشاعه خشونت علیه زنان جلوگیری کنند. فقه امامیه با تأکید بر «حقّ العِرض» (حق حفظ آبرو)، حمایت کیفری از قربانیان را نه تنها جایز، بلکه واجب می‌داند؛ رویکردی که می‌تواند مبنای اصلاح قوانین داخلی برای تشدید مجازات مرتکبان جرائم سایبری علیه زنان

1 Rape Culture

باشد. در بُعد حقوقی-فنی، ضرورت طراحی سامانه‌های هوشمند شناسایی و حذف محتوای مجرمانه (مانند الگوریتم‌های مبتنی بر هوش مصنوعی) آشکار است. این سامانه‌ها باید با همکاری نهادهای ورزشی و پلتفرم‌های فضای مجازی توسعه یابند و معیارهای بومی (از جمله حساسیت به ارزش‌های اخلاقی و فرهنگی جامعه) را در اولویت قرار دهند. قانون‌گذار می‌تواند با الزام پلتفرم‌ها به «مسئولیت اجتماعی»[1] ، آن‌ها را ملزم به واکنش سریع به گزارش‌های مرتبط با ورزشکاران زن کند. همچنین، ایجاد «دادگاه‌های تخصصی جرائم سایبری ورزشی» با قضات آموزش‌دیده، می‌تواند فرایند رسیدگی به پرونده‌ها را تسریع و تخصصی تر کند. در پایان، مقابله با جرائم سایبری علیه ورزشکاران زن نیازمند عزمی سه جانبه است: تقویت چارچوب‌های قانونی از طریق اصلاح قوانین موجود و تدوین مقررات ویژه برای حمایت از زنان در فضای مجازی. فرهنگ‌سازی و آموزش در سطوح گوناگون جامعه، از جمله ورزشکاران، تماشاگران، و کاربران فضای مجازی، برای کاهش پذیرش اجتماعی خشونت آنلاین. به کارگیری فناوری‌های نوین برای رصد، گزارش، و مقابله با محتوای مجرمانه، همراه با حفظ تعادل میان حریم خصوصی و امنیت عمومی. این رویکرد جامع، نه تنها از ورزشکاران زن به عنوان قربانیان اصلی حمایت می‌کند، بلکه با هدف‌گذاری ریشه‌ای، به تضعیف بسترهای فرهنگی-اجتماعی تولید خشونت در فضای مجازی می‌انجامد. تنها در این صورت می‌توان امید داشت که عرصه ورزش، به جای آنکه بازتاب دهنده نابرابری‌های جامعه باشد، به پیش قراول برابری جنسیتی و احترام به کرامت انسانی تبدیل شود.

تقدیر وتشکر

بدین وسیله، نویسنده مراتب سپاس و قدردانی از سردبیر و داوران گرامی که سبب بهبود کیفیت این مقاله شده است را به عمل می‌آورد.

1 Social Responsibility

منابع

الف) منابع فارسی

۱. احمدی، علی رضا. (۱۳۹۱) حمایت کیفری از زنان و کودکان در برابر آزارهای جنسی در قوانین ایران. دانشگاه آزاد اسلامی واحد تهران مرکزی.

۲. اسدی، ندا، تجاری، فرشاد و نیک آیین، زینت. (۱۴۰۰) بررسی تحلیلی قوانین کشور در حوزه فعالیت‌های ورزشی زنان. نشریه مدیریت ورزشی. ۱۳(۲)، ۵۶۵-۵۸۰.

۳. اعظمی، محمد سعید و طارمیان، فرهاد. (۱۳۹۹). بررسی شیوع آزار سایبری و متغیرهای دموگرافیک آزارگران، آزاردیدگان و آزارگر-آزاردیده‌های سایبری. فصلنامه پژوهش در سلامت روانشناختی. ۱۴(۴)، ۱۹-۳۵.

٤. امینی، مهدی و نادریان، فاطمه. (۱۴۰۳) حق زنان بر ورزش در قوانین و مقررات ایران و اسناد بین‌المللی. پژوهش در ورزش زنان. ۱(۳)، ۲۷۹-۲۹۴.

٥. رهامی، روح اله واژدری، امیرحسین. (۱۴۰۱). امنیت سایبری اتحادیه اروپا: تهدیدات، فرصتها و اقدامات (از آغاز تا سال ۲۰۲۱). فصلنامه تحقیقات حقوقی. ۲۵، ۲۷۳-۳۰۲.

٦. صادقی، سالار، بدلی ملکی، محمد و اسلامی، طاها (۱۴۰۳). نقش نهاد آموزش و پرورش در پیشگیری اجتماعی و وضعی از جرائم سایبری دانش آموزان. پژوهشهای جرم شناسی کاربردی. ۲(۴)، ۴۳-۶۴.

۷. ضیایی، سید یاسر و شکیب نژاد، احسان. (۱۳۹۶). قانونگذاری در فضای سایبر: رویکرد حقوق بین‌الملل و حقوق ایران. مجله حقوقی بین المللی. ۳۴(۵۷)، ۲۲۷-۲۴۹.

۸. میرسلامی، سیدکامیار, واحدیاریجان، سیدیونس و جمالزاده، عبدالرضا. (۱۴۰۱). بررسی فقهی و حقوقی جرم در فضای مجازی. نشریه مطالعات راهبردی ناجا. ۲۳، ۱۰۵-۱۳۱.

ب) منابع انگلیسی

9. Al-Khater, W. A., Al-Maadeed, S., Ahmed, A. A., Sadiq, A. S., & Khan, M. K. (2020). Comprehensive Review of Cybercrime Detection Techniques. IEEE Access, 8, 137293–137311

10. Angwaomaodoko, E. (2024). Cyberbullying: Legal and Ethical Implications, Challenges and Opportunities for Policy Development. International Journal of Innovative Science and Research Technology (IJISRT), 738–744.

11. Babanina, V., Tkachenko, I., Matiushenko, O., & Krutevych, M. (2021). Cybercrime: History of formation, current state and ways of counteraction. Revista Amazonia Investiga, 10(38), 113–122.

12. Cohen-Almagor, R. (2020). Cyberbullying, Moral Responsibility, and Social Networking. European Journal of Analytic Philosophy, 16(1), 75–98.

13. Fink, J. S. (2015). Female athletes, women's sport, and the sport media commercial complex: Have we really "come a long way, baby"? Sport Management Review, 18(3), 331–342.

14. Forsdike, K., & Giles, F. (2024). Women's Experiences of Gender-Based Interpersonal Violence in Sport: A Qualitative Meta-Synthesis. Trauma, Violence, & Abuse, 25(4), 3254–3268.

15. Jenaro, C., Flores, N., Vega, V., Cruz, M., Pérez, Ma. C., & Torres, V. A. (2018). Cyberbullying among adults with intellectual disabilities: Some preliminary data. Research in Developmental Disabilities, 72, 265–274.

16. Kavanagh, E. J., Litchfield, C., & Osborne, J. (2023). Social Media and Athlete Welfare. International Journal of Sport Communication, 16(3), 274–281.

17. Leukfeldt, E. R., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. Deviant Behavior, 37(3), 263–280.

18. Liao, M., & Craig, K. (2023). Tackling violence against women and girls in sport. A handbook for policy makers and sports practitioners. UNESCO.

19. Masood, M., Nawaz, M., Malik, K. M., Javed, A., Irtaza, A., & Malik, H. (2023). Deepfakes generation and detection: state-of-the-art, open challenges, countermeasures, and way forward. Applied Intelligence, 53(4), 3974–4026.

20. Mouncey, E., & Ciobotaru, S. (2025). Phishing scams on social media: An evaluation of cyber awareness education on impact and effectiveness. Journal of Economic Criminology, 7, 100125

21. Pylarinou, N.-R. (2020). STALKING: PERPETRATION, VICTIMIZATION AND STALKING MYTH ACCEPTANCE IN GREECE AND THE UNITED KINGDOM. University of Huddersfield.

22. Powell, A., Scott, A. J., Flynn, A., & McCook, S. (2024). A multi-country study of image-based sexual abuse: extent, relational nature and correlates of victimisation experiences. Journal of Sexual Aggression, 30(1), 25–40.

23. Said, I., & McNealey, R. L. (2023). Nonconsensual Distribution of Intimate Images: Exploring the Role of Legal Attitudes in Victimization and Perpetration. Journal of Interpersonal Violence, 38(7–8), 5430–5451.

24. Tsagourias, N., & Buchan, R. (2021). Research Handbook on International Law and Cyberspace. Edward Elgar Publishing.

25. Voigt, P. and V. dem B. A. (2017). The eu general data protection regulation (gdpr). A Practical Guide, 1st Ed., Cham: Springer International Publishing, 10(3152676), 10–5555.

26. Willson, E., & Kerr, G. (2023). Gender-Based Violence in Girls' Sports. Adolescents, 3(2), 278–289.

27. Zhao, S., & Guo, L. (2024). Improving Athlete Data Protection: Tackling Privacy and Economic Risks in Digital Security. International Journal of Education and Humanities, 4(4), 417–429.

28. Ziaei, Y., & Shakibnejad, E. (2018). Legislation in Cyberspace from the Prospect of International Law and the Iranian Law. International Law Journal, 34(57), 227–249.