

مسئولیت مدنی پلتفرم‌های اینترنتی در قبال نقض حریم خصوصی کاربران

سید امیر صدق^۱، نجمه دارنجانی شیرازی^۲

۱- کارشناسی حقوق، دانشگاه آزاد اسلامی، واحد شیراز، شیراز، ایران.

۲- پژوهشگر دوره دکتری حقوق خصوصی، واحد یاسوج، دانشگاه آزاد اسلامی، یاسوج، ایران. (مدرس دانشگاه آزاد).

چکیده :

پژوهش حاضر با هدف تبیین و تحلیل مبانی حقوقی مسئولیت مدنی پلتفرم‌های اینترنتی در قبال نقض حریم خصوصی کاربران، به بررسی عمیق ابعاد نظری و عملی این مسئله در عصر دیجیتال می‌پردازد. افزایش نفوذ فناوری‌های نوین و وابستگی روزافزون جوامع به پلتفرم‌های آنلاین، حوزه جمع‌آوری، پردازش و ذخیره‌سازی حجم عظیمی از داده‌های شخصی را به کانون توجه حقوق‌دانان تبدیل کرده است؛ این امر مستلزم بازتعریف مسئولیت مدنی در مواجهه با بازیگران جدیدی است که غالباً واسطه میان تولیدکننده داده و مصرف‌کننده نهایی هستند. بیان مسئله اصلی این پژوهش بر چالش‌های ناشی از خلاءهای قانونی موجود و پیچیدگی‌های اثبات تقصیر در محیط‌های سایبری متمرکز است؛ زیرا ماهیت ماهوی پلتفرم‌ها به عنوان میزبان (Host) یا واسطه، مرزهای مسئولیت سنتی را مخدوش ساخته و نیازمند رویکردهای نوینی در تفسیر قواعد مسئولیت مدنی مبتنی بر تقصیر، خطر و تضمین است. هدف اساسی این مقاله، تحلیل انتقادی ساختارهای مسئولیت مدنی در حقوق ایران و رویکردهای تطبیقی به منظور ارائه چارچوبی منسجم جهت حمایت مؤثر از حق بنیادین حریم خصوصی در فضای مجازی است. روش تحقیق به کار گرفته شده در این مطالعه، روشی تحلیلی - توصیفی و مروری است که با تکیه بر مطالعه اسناد بالادستی، قوانین ناظر بر فضای مجازی، رویه‌های قضایی و دکترین حقوقی، به تشریح جوانب مختلف مسئله می‌پردازد. یافته‌های اصلی پژوهش نشان می‌دهد که اتکای صرف به مسئولیت مبتنی بر تقصیر، در مواجهه با نقض حریم خصوصی توسط پلتفرم‌ها، به دلیل دشواری احراز رابطه سببیت و تقصیر در فرایندهای الگوریتمی، ناکارآمد است؛ در نتیجه، حرکت به سمت مسئولیت عینی یا شبه‌تضمینی (به‌ویژه در موارد نقض داده‌های شخصی) ضروری به نظر می‌رسد. نتیجه‌گیری نهایی حاکی از لزوم تدوین مقررات اختصاصی‌تر و تعریف دقیق‌تر الزامات امنیتی و نگهداری داده‌ها برای این نهادها است تا بتواند با انتظارات حقوقی کاربران همخوانی یابد و یک سازوکار جبرانی عادلانه را محقق سازد. واژگان کلیدی: مسئولیت مدنی، حریم خصوصی، پلتفرم‌های اینترنتی، داده‌های شخصی، حمایت از کاربران

مقدمه :

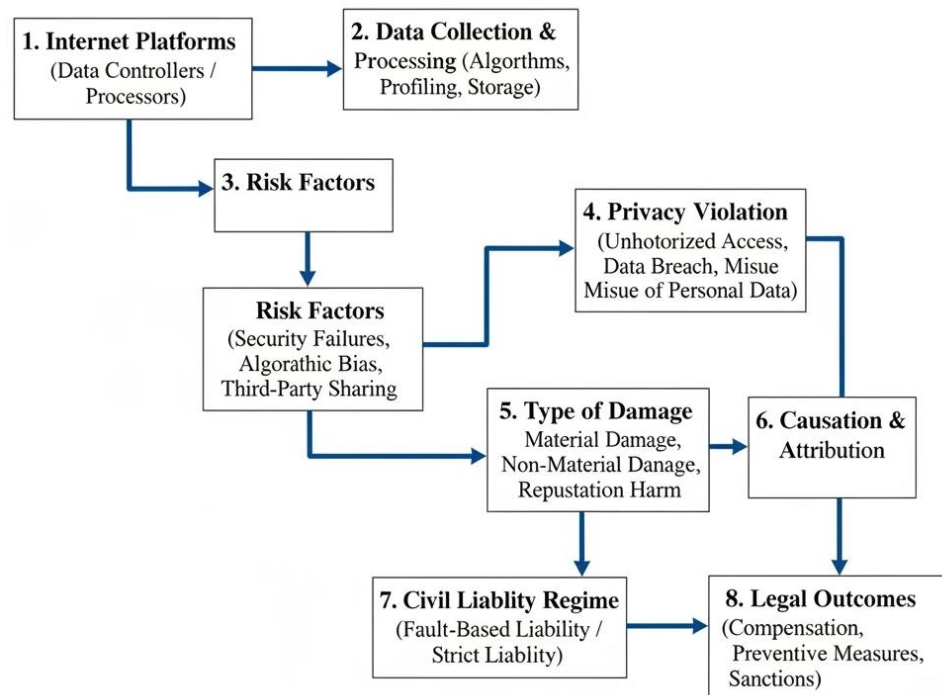
توسعه شتابان فناوری اطلاعات و ارتباطات، به‌ویژه ظهور و سلطه پلتفرم‌های اینترنتی عظیم، پارادایم‌های سنتی تعاملات اجتماعی، اقتصادی و حقوقی را دگرگون ساخته است (رضوی‌فرد و همکاران، ۱۳۹۵)؛ در این میان، حریم خصوصی افراد که زمانی محدود به مرزهای فیزیکی و ارتباطات خصوصی بود، اکنون به شدت تحت تأثیر جمع‌آوری، تحلیل و اشتراک‌گذاری مستمر داده‌ها قرار گرفته است (صادقی و همکاران، ۱۴۰۰). پلتفرم‌ها، به عنوان بازیگران محوری در این اکوسیستم، نقش دوتایی مهمی ایفا می‌کنند: از یک سو، تسهیل‌گر ارتباطات و خدمات هستند و از سوی دیگر، به دلیل تسلط بر زیرساخت‌های فنی، به متولیان اصلی اطلاعات حساس کاربران تبدیل شده‌اند؛ این موقعیت انحصاری، همراه با ماهیت پیچیده و غالباً غیرشفاف پردازش داده‌ها، پتانسیل عظیمی برای نقض گسترده و سازمان‌یافته حق حریم خصوصی افراد ایجاد نموده است (حق‌جو و همکاران، ۱۴۰۲). در چارچوب حقوقی مسئولیت مدنی، که اساساً بر جبران خسارت ناشی از نقض حقوق و تکالیف استوار است، ظهور این بازیگران جدید، سؤالات بنیادینی را پیرامون قلمرو و مبانی مسئولیت‌پذیری آنان مطرح می‌سازد؛ به ویژه آنکه قوانین سنتی مسئولیت مدنی که بیشتر بر رفتارهای مادی و مستقیم تمرکز داشتند، در تطبیق با آسیب‌های غیرمادی و داده‌محور با دشواری‌های جدی مواجه‌اند.

مسئله اصلی که این پژوهش سعی در کاوش آن دارد، چگونگی اعمال قواعد مسئولیت مدنی - چه مبتنی بر تقصیر و چه عینی - بر پلتفرم‌هایی است که نقض حریم خصوصی کاربران نه لزوماً از طریق اقدام مستقیم و عامدانه، بلکه از طریق سهل‌انگاری در تأمین امنیت زیرساخت‌ها، طراحی الگوریتم‌های مغرضانه یا فروش داده‌های شخصی به اشخاص ثالث، صورت می‌پذیرد. این نوع نقض، اغلب ماهیتی سیستمی و درونی دارد و ردیابی تقصیر فردی یا انتساب مستقیم علت خسارت به یک عمل مجرد را بسیار دشوار می‌سازد؛ بنابراین، ماهیت حقوقی پلتفرم‌ها - که آیا صرفاً واسطه فنی هستند یا به مثابه کنترل‌کننده (Controller) داده‌ها محسوب می‌شوند - تعیین‌کننده اصلی دامنه مسئولیت مدنی آنها خواهد بود. چالش اثبات خسارت نیز به نوبه خود پیچیده است؛ زیرا آسیب‌های ناشی از نقض حریم خصوصی، مانند سرقت هویت، تبعیض یا لطمه به اعتبار، غالباً غیرمادی بوده و ارزیابی دقیق مبلغ جبران خسارت مبتنی بر اصول فقهی و حقوقی سنتی، نیازمند توسعه مبانی جدیدی است.

هدف این مقاله، فراتر از توصیف وضعیت موجود، تحلیل انتقادی مکانیزم‌های حقوقی موجود در نظام حقوقی ایران و مقایسه آن با استانداردهای بین‌المللی (نظیر GDPR اروپا) جهت ارائه پیشنهادهایی برای تقویت بنیان‌های مسئولیت مدنی پلتفرم‌ها است. پژوهش در پی آن است که مشخص سازد آیا مسئولیت مدنی در این حوزه باید صرفاً بر جبران خسارت وارده متمرکز شود یا باید شامل اعمال تدابیر پیشگیرانه و تنبیهی نیز باشد تا از تکرار این تخلفات در مقیاس گسترده جلوگیری نماید. در این راستا، تفکیک میان مسئولیت ناشی از عملکرد خود پلتفرم (مانند نقض در طراحی امنیتی) و مسئولیت ناشی از محتوای بارگذاری‌شده توسط کاربران (مسئولیت میزبان) برای دستیابی به یک نظام حقوقی منصفانه و کارآمد ضروری است. روش‌شناسی مورد استفاده در این پژوهش، روشی تحلیلی - توصیفی و مبتنی بر مطالعات کتابخانه‌ای و اسنادی است؛ بدین معنا که ابتدا مفاهیم کلیدی نظیر حریم خصوصی در فضای مجازی، ماهیت حقوقی پلتفرم‌ها و عناصر مسئولیت مدنی به تفصیل تشریح و تعریف شده‌اند؛ سپس، قوانین و مقررات ملی و بین‌المللی مرتبط با حفاظت از داده‌ها مورد ارزیابی نقادانه قرار گرفته‌اند تا تناسب آنها با پیچیدگی‌های فنی پلتفرم‌ها سنجیده شود. این رویکرد مروری به ما امکان می‌دهد تا نظریه‌های مختلف حقوقی در خصوص انتساب تقصیر (از جمله مسئولیت مبتنی بر نظریه مراقبت استاندارد یا

ریسک) را بر داده‌محوری پلتفرم‌ها اعمال نماییم و نقاط قوت و ضعف هر نظریه را در تأمین حمایت کافی از قربانیان نقض حریم خصوصی مشخص کنیم.

یافته‌های اولیه حاکی از آن است که سیستم حقوقی ایران، هرچند در قانون مدنی و قوانین متأخر مانند قانون جرایم رایانه‌ای و قانون حمایت از داده‌های شخصی (در صورت تصویب)، اشاراتی به حمایت از حریم خصوصی دارد، اما فاقد یک چارچوب جامع و مشخص برای تعیین مسئولیت مدنی پلتفرم‌ها در قبال نقض‌های سیستمی و الگوریتمی است؛ این خلاء باعث می‌شود که بار اثبات سنگین‌تر از آنچه باید باشد، بر دوش کاربر آسیب‌دیده بیفتد. به طور خاص، مفهوم «رضایت آگاهانه» کاربران در پلتفرم‌ها که اغلب از طریق توافق‌نامه‌های کاربری طولانی و غیرقابل مذاکره (EULAs) اخذ می‌شود، در عمل کارکرد حمایتی خود را از دست داده و بیشتر به ابزاری برای سلب مسئولیت پلتفرم تبدیل شده است؛ لذا، تحلیل حقوقی این رضایت‌ها، یکی از محورهای اصلی این پژوهش است. در حوزه بین‌المللی، تحولاتی مانند مقررات عمومی حفاظت از داده‌ها (GDPR) اتحادیه اروپا، مسئولیت پلتفرم‌ها را به طور مستقیم و با تعریف دقیق وظایف کنترلی و پردازشی، افزایش داده است؛ این مقررات با تعیین جریمه‌های سنگین و تعریف مسئولیت عینی برای نقض اصول حفاظت از داده‌ها، الگویی برای بازنگری در قوانین داخلی ارائه می‌کنند. تحلیل این الگوها نشان می‌دهد که تفکیک دقیق نقش‌ها (پردازشگر در برابر کنترل‌کننده) و الزام به اجرای تدابیر امنیتی پیشینی (Privacy by Design)، کلید حل معضلات اثبات و انتساب مسئولیت در فضای پلتفرمی است؛ زیرا این امر، معیار تقصیر را از «عمل مجرمانه خاص» به «عدم رعایت استانداردهای مراقبت مقرر» تغییر می‌دهد.



شکل ۱. مدل مفهومی مسئولیت مدنی پلتفرم‌های اینترنتی در قبال نقض حریم خصوصی کاربران

مدل مفهومی ارائه شده در شکل (۱)، چارچوب تحلیلی پژوهش حاضر را برای تبیین مسئولیت مدنی پلتفرم‌های اینترنتی در قبال نقض حریم خصوصی کاربران نشان می‌دهد. مطابق این مدل، پلتفرم‌های اینترنتی به عنوان کنترل‌کنندگان یا پردازشگران داده، در فرآیند جمع‌آوری و پردازش اطلاعات شخصی از طریق الگوریتم‌ها، پروفایل‌سازی و ذخیره‌سازی داده‌ها ایفای نقش می‌کنند. این فعالیت‌ها در صورت مواجهه با عوامل خطرزا نظیر نقص‌های امنیتی، سوگیری‌های الگوریتمی و اشتراک‌گذاری داده‌ها با اشخاص ثالث، زمینه‌ساز بروز نقض حریم خصوصی از جمله دسترسی غیرمجاز، نشت داده و سوءاستفاده از اطلاعات شخصی می‌شوند. در ادامه، این نقض‌ها می‌توانند به ورود خسارات مادی و غیرمادی از جمله لطمه به حیثیت و اعتبار کاربران منتهی گردند که احراز رابطه سببیت و انتساب حقوقی آن به پلتفرم، امکان اعمال رژیم‌های مختلف مسئولیت مدنی اعم از مسئولیت مبتنی بر تقصیر یا مسئولیت محض را فراهم می‌سازد. نهایتاً، نتایج حقوقی این فرآیند در قالب جبران خسارت، اتخاذ تدابیر پیشگیرانه و اعمال ضمانت‌اجراهای قانونی متجلی می‌شود.

بنابراین، این مقاله استدلال می‌کند که مسئولیت مدنی پلتفرم‌ها در قبال نقض حریم خصوصی کاربران نباید محدود به قواعد عمومی مسئولیت مدنی سنتی باقی بماند؛ بلکه باید با تکیه بر مسئولیت مبتنی بر ریسک فعالیت‌های پرخطر دیجیتال و الزام به اجرای اصول حفاظت از داده‌ها، تعریفی نوین یابد. این رویکرد نوین، مستلزم تعریف دقیق‌تر مفهوم «داده شخصی»، تعیین وظایف مراقبتی در برابر سوءاستفاده‌های الگوریتمی، و تسهیل فرآیند جبران خسارت برای قربانیان است؛ در غیر این صورت، تداوم سلطه پلتفرم‌ها بدون پاسخگویی متناسب، به تضعیف مستمر حق بنیادین حریم خصوصی افراد در جامعه دیجیتال منجر خواهد شد. در نهایت، این پژوهش با جمع‌بندی تحلیل‌های نظری و عملی، پیشنهاداتی برای اصلاح ساختار تقنینی کشور در راستای همسویی با استانداردهای بین‌المللی و تقویت موضع کاربران در دعاوی حقوقی مرتبط با نقض حریم خصوصی ارائه خواهد داد.

۲. ماهیت حریم خصوصی در فضای مجازی و چالش‌های حقوقی آن

حریم خصوصی، به عنوان یک حق بنیادین انسانی، در طول زمان تکامل یافته و از معنای سنتی خود که شامل مصونیت از تعرض فیزیکی و حفظ اسرار شخصی در فضای مادی بود، فراتر رفته و اکنون شامل حق کنترل فرد بر انتشار و استفاده از اطلاعات شخصی خود در حوزه دیجیتال است؛ این تحول، ناشی از این واقعیت است که داده‌ها دیگر صرفاً بازنمایی واقعیت نیستند، بلکه به ابزاری قدرتمند برای پیش‌بینی، تأثیرگذاری و حتی مهندسی رفتار فردی تبدیل شده‌اند (محمدی، ۱۴۰۴). در فضای مجازی، حریم خصوصی نه تنها شامل ناشناس ماندن (Anonymity) است، بلکه ماهیت پیچیده‌ای از کنترل بر جریان اطلاعات (Information Flow Control) را می‌طلبد؛ جایی که کاربران به طور مداوم در حال تولید «ردپای دیجیتال» هستند که توسط الگوریتم‌های پیچیده پلتفرم‌ها جمع‌آوری و تجزیه و تحلیل می‌شود. این تبدیل شدن داده‌ها به دارایی اصلی، ماهیت حقوقی حریم خصوصی را از یک حق سلبی (Right to be Left Alone) به حقی ایجابی در زمینه مدیریت اطلاعات (Data Self-Determination) تغییر داده است (واثقی و همکاران، ۱۴۰۴).

چالش اصلی در حوزه فضای مجازی، عدم تقارن اطلاعاتی و قدرت متمرکز پلتفرم‌ها است؛ کاربران در تعامل با پلتفرم‌ها، اغلب فاقد درک کافی از حجم، نحوه پردازش و اهداف بلندمدت استفاده از داده‌هایشان هستند، امری که مفهوم «رضایت آگاهانه» را تحت الشعاع

قرار می‌دهد. رضایت در قراردادهای استاندارد پلتفرمی، معمولاً به صورت یک فرمول از پیش تعیین شده و بدون امکان مذاکره ارائه می‌شود که از منظر حقوقی، کمتر نشان‌دهنده رضایت ارادی و مبتنی بر علم کافی تلقی می‌گردد (منصوری و همکاران، ۱۴۰۴)؛ این امر، به ویژه هنگامی که نقض حریم خصوصی ناشی از افشاجاری‌های ناخواسته یا سوءاستفاده‌های ثانویه باشد، مسئله‌ساز می‌شود. علاوه بر این، ماهیت شبکه‌ای و جهانی اینترنت، مرزهای صلاحیت قضایی و اجرای قوانین ملی را به شدت تضعیف کرده و تعیین دادگاه صالح و قانون حاکم بر اختلافات مرتبط با نقض حریم خصوصی را به یک معمای حقوقی بین‌المللی تبدیل نموده است، هرچند تلاش‌هایی مانند قانون حاکم بر حمایت از داده‌ها در اتحادیه اروپا تا حدودی این خلأ را پر کرده است.

از منظر مسئولیت مدنی، دشواری اصلی در انتساب خسارت است؛ زیرا نقض حریم خصوصی در پلتفرم‌ها اغلب نتیجه یک خطای منفرد نیست، بلکه محصول تراکنش‌های سیستمی و خودکارسازی‌هایی است که توسط الگوریتم‌های یادگیری ماشین صورت می‌پذیرد؛ این الگوریتم‌ها ممکن است به دلیل آموزش بر روی داده‌های مغرضانه، منجر به تبعیض یا تصمیم‌گیری‌های ناعادلانه شوند که مستقیماً حریم خصوصی و کرامت افراد را نقض می‌کند، بدون آنکه بتوان یک «عامل» انسانی مشخص را مقصر دانست. بنابراین، نظام حقوقی نیازمند ابزارهایی است تا بتواند مسئولیت را نه فقط به عاملین انسانی، بلکه به نهادهای حقوقی مسئول (پلتفرم‌ها) که زیرساخت این تصمیم‌گیری‌ها را فراهم می‌کنند، منتسب نماید. این امر مستلزم گذار از مدل سنتی مبتنی بر تقصیر به سمت مدل‌هایی است که بر مسئولیت مبتنی بر ریسک فعالیت‌های داده‌محور تأکید دارند (ایران‌نژاد و همکاران، ۱۴۰۴). تعریف «داده شخصی» در عصر بیگ دیتا اهمیت فوق‌العاده‌ای یافته است؛ داده‌های غیرحساسی که به ظاهر بی‌خطرند، وقتی با هم ترکیب می‌شوند (Data Aggregation)، می‌توانند پروفایل‌های بسیار دقیقی از افراد ایجاد کنند که شامل ترجیحات سیاسی، وضعیت سلامت یا وضعیت مالی آنان است؛ این ترکیب‌سازی خود می‌تواند مصداق نقض حریم خصوصی تلقی شود، حتی اگر هیچ یک از داده‌های اولیه به تنهایی محرمانه نبوده باشند. حقوق ایران، همچنان در تعریف خود از داده‌های شخصی، به رویکردهای سنتی نزدیک است و کمتر به داده‌های استنتاجی (Inferred Data) پرداخته است؛ این شکاف مفهومی، مانع بزرگی در اعمال قواعد حمایتی در برابر تحلیل‌های پیشرفته داده توسط پلتفرم‌ها محسوب می‌شود.

مسئولیت مدنی در این حوزه باید دو کارکرد اصلی را پوشش دهد: اول، جبران خسارت (Compensation) برای آسیب‌هایی که وارد شده است و دوم، بازدارندگی (Deterrence) برای جلوگیری از نقض‌های آتی؛ در مورد پلتفرم‌ها، به دلیل ظرفیت بالای تکرار جرم و مقیاس گسترده فعالیت، جنبه بازدارندگی اهمیت ویژه‌ای می‌یابد. اگر مسئولیت مدنی تنها به جبران خسارت‌های اثبات‌شده محدود شود، هزینه‌های نقض حریم خصوصی برای پلتفرم‌ها بسیار پایین خواهد بود و انگیزه کافی برای سرمایه‌گذاری در امنیت سایبری و طراحی متناسب با حریم خصوصی (Privacy by Design) ایجاد نخواهد شد؛ اینجاست که لزوم اعمال مسئولیت‌های شدیدتر و شاید حتی جریمه‌های تنبیهی (Punitive Damages) در نظام‌های حقوقی مطرح می‌شود (پیشنماز و همکاران، ۱۴۰۲). پیچیدگی دیگر مربوط به حوزه داده‌های حساس است؛ هنگامی که پلتفرم‌ها به طور ناخواسته یا به دلیل ضعف امنیتی، داده‌های مربوط به نژاد، مذهب، گرایش جنسی یا سلامت افراد را افشا می‌کنند، آسیب وارده به اعتبار و امنیت روانی افراد بسیار فراتر از خسارات مالی قابل محاسبه است. حقوق سنتی در جبران این خسارات غیرمادی (Moral Damages) دچار ابهام است و تعیین میزان آن نیازمند معیارهایی است که فراتر از معیارهای عرفی خسارت معنوی در دعاوی سنتی حرکت کنند؛ این امر ایجاب می‌کند که نظام‌های حقوقی، ارزش انتزاعی حریم خصوصی را در محاسبه خسارت لحاظ نمایند. در نهایت، پلتفرم‌ها صرفاً دریافت‌کننده داده نیستند، بلکه

فعالانه در شکل‌دهی به حریم خصوصی کاربران از طریق تنظیمات پیش‌فرض و واسط کاربری (User Interface) مشارکت دارند؛ طراحی‌هایی که به طور ضمنی کاربر را به پذیرش اشتراک‌گذاری بیشتر داده‌ها ترغیب می‌کنند (Dark Patterns)، خود می‌تواند نقض تکالیف مراقبتی پلتفرم تلقی شود و مبنایی برای مسئولیت مدنی قرار گیرد (حسام و همکاران، ۱۴۰۲). زیرا این رفتار، اراده آزاد کاربر را به شکلی مهندسی‌شده تحت تأثیر قرار می‌دهد. این رویکرد نیازمند بازبینی در دکتترین تقصیر است تا سهل‌انگاری در طراحی رابط کاربری را نیز تحت پوشش قرار دهد.

۳. مفهوم‌سازی پلتفرم‌های اینترنتی و انواع مسئولیت‌پذیری آنها

پلتفرم‌های اینترنتی، بر خلاف وبسایت‌های سنتی که محتوای تولیدی خود را منتشر می‌کنند، ساختارهای چندوجهی هستند که دو یا چند گروه مستقل از کاربران را از طریق زیرساخت‌ها و ابزارهای مشترک به هم متصل می‌سازند؛ این مدل کسب‌وکار مبتنی بر «اثر شبکه‌ای» است، به این معنی که ارزش پلتفرم با افزایش تعداد کاربران آن، تصاعدی افزایش می‌یابد؛ این ماهیت واسطه‌ای، طبقه‌بندی حقوقی آنها را پیچیده می‌سازد؛ آنها می‌توانند نقش‌های متفاوتی ایفا کنند: ارائه‌دهنده خدمات میزبانی (Host)، واسطه اطلاعاتی (Intermediary)، بازار (Marketplace)، یا در برخی موارد، حتی منتشرکننده فعال (Publisher) محتوا. این تمایز نقش، سنگ بنای تعیین دامنه مسئولیت مدنی آنها در قبال اعمال کاربران و نقض حریم خصوصی است. در نظام حقوقی سنتی، تمایز میان «تولیدکننده» و «ناشر» محتوا، مبنای تقسیم مسئولیت بود؛ اما پلتفرم‌ها اغلب مدعی‌اند که صرفاً زیرساخت فنی فراهم می‌کنند و مسئولیتی در قبال محتوای تولیدشده توسط اشخاص ثالث ندارند، استدلالی که در حقوق آمریکا به عنوان دفاع «بخش ۲۳۰» مشهور است و در اروپا نیز تحت عنوان معافیت واسطه‌ها از مسئولیت محتوایی مطرح می‌شود. با این حال، هنگامی که سخن از داده‌های شخصی و حریم خصوصی به میان می‌آید، این ادعای خنثی بودن فنی دیگر قابل دفاع نیست؛ زیرا پلتفرم‌ها نه تنها میزبان داده‌ها هستند، بلکه فعالانه در جمع‌آوری، تحلیل و پروفایل‌سازی کاربران از طریق الگوریتم‌های خود نقش دارند و بنابراین، به عنوان «کنترل‌کننده» یا «پردازشگر» داده‌ها مطرح می‌شوند (مضانیان سیاهکلرودی و همکاران، ۱۳۹۹).

مسئولیت مدنی ناشی از نقض حریم خصوصی توسط پلتفرم‌ها را می‌توان به دو دسته کلی تقسیم کرد: مسئولیت ناشی از عملکرد خود پلتفرم و مسئولیت ناشی از عملکرد کاربران یا محتوای آنان. در دسته اول، مسئولیت زمانی متوجه پلتفرم است که نقض از طریق سهل‌انگاری در حفظ امنیت فنی (مانند حملات سایبری که به دلیل نقص امنیتی رخ می‌دهد) یا از طریق طراحی ناقص سامانه‌ها (مانند استفاده از تنظیمات پیش‌فرض نفوذپذیر) به وقوع می‌پیوندد؛ این نوع مسئولیت، اساساً مسئولیت ناشی از «تقصیر در ساختار» یا «نقص در انجام وظیفه مراقبت» است که در مباحث مسئولیت عینی (Strict Liability) جای می‌گیرد. در دسته دوم، یعنی مسئولیت پلتفرم در قبال محتوای کاربران، مسئله پیچیده‌تر می‌شود (ابهری و همکاران، ۱۳۹۱)؛ اگر کاربری اطلاعات خصوصی دیگری را در پلتفرم منتشر کند، پلتفرم باید چه واکنشی نشان دهد؟ در حقوق ایران و بسیاری از نظام‌های حقوقی، معیار سنجش مسئولیت پلتفرم در این موارد، میزان آگاهی و سرعت عمل آن در حذف محتوای غیرقانونی است؛ این رویکرد، اصل «عدم مداخله پیشگیرانه» را تا حدی می‌پذیرد، اما مسئولیت پس از اطلاع (Notice and Takedown) را بر دوش او می‌گذارد. با این وجود، در حوزه

حریم خصوصی، این رویکرد کافی نیست؛ زیرا افشای داده‌ها ممکن است حتی پیش از اعتراض رسمی، آسیب غیرقابل جبرانی وارد کرده باشد.

تحلیل ماهیت پلتفرم‌ها نشان می‌دهد که آنها صرفاً واسطه نیستند، بلکه در اقتصاد مبتنی بر داده، عاملی فعال در «تولید» ارزش از داده‌های کاربران هستند؛ این نقش فعال، ایجاب می‌کند که آنها فراتر از یک نهاد صرفاً فنی، مسئولیت مدنی حقوقی سنگین‌تری را متحمل شوند. در حقوق اتحادیه اروپا، تفکیک روشنی میان کنترل‌کننده (Controller) و پردازشگر (Processor) داده‌ها وجود دارد؛ کنترل‌کننده کسی است که اهداف و ابزارهای پردازش را تعیین می‌کند (که معمولاً پلتفرم است) و پردازشگر کسی است که داده‌ها را به نمایندگی از کنترل‌کننده پردازش می‌کند. این تفکیک، مسئولیت مدنی را به طور مشخص‌تری بر دوش نهادی می‌اندازد که قدرت تصمیم‌گیری در مورد داده‌ها را دارد. در حقوق ایران، اگرچه قانون حمایت از داده‌های شخصی (در صورت تصویب نهایی) می‌تواند این مفاهیم را وارد کند، اما در حال حاضر، دادگاه‌ها اغلب با اتکا به قواعد عمومی مسئولیت مدنی (ماده ۱ قانون مسئولیت مدنی: «هر کس به سبب تقصیر خود... موجب ضرر دیگری شود... مسئول جبران آن است») تلاش می‌کنند تا تقصیر پلتفرم را در چهارچوب سهل‌انگاری در مراقبت یا عدم اجرای تدابیر امنیتی اثبات نمایند؛ اما این رویکرد فاقد یک استاندارد مشخص و قابل سنجش برای فعالیت‌های پیچیده الگوریتمی است و به قاضی اجازه می‌دهد تا در غیاب ضوابط فنی مشخص، به سلیقه شخصی در تعیین تقصیر متکی شود (ملکوتی خلیل‌زاده و همکاران، ۱۳۹۹).

بنابراین، برای رسیدن به یک چارچوب مسئولیت مدنی منصفانه در قبال پلتفرم‌ها، باید تعریف حقوقی آنها را از یک نهاد خنثی به یک «نهاد دارای رابطه انحصاری و مبتنی بر قدرت» ارتقا داد؛ این تغییر دیدگاه، مسئولیت آنها را از حالت مبتنی بر تقصیر صرف به سمت یک مسئولیت مبتنی بر رعایت وظایف (Duty-Based Liability) سوق می‌دهد که در آن عدم انطباق با استانداردهای حفاظت از داده‌ها، خود به مثابه نقض تکالیف و مبنای مسئولیت قرار می‌گیرد، فارغ از اینکه آیا خسارت مستقیمی نیز در لحظه وقوع ناشی شده باشد.

۴. مبانی مسئولیت مدنی: تقصیر، خطر و تضمین حق در بستر سایبری

مبانی سنتی مسئولیت مدنی در حقوق ایران بر پایه «تقصیر» (Fault) استوار است، به این معنا که اثبات سوء رفتار یا سهل‌انگاری متعددی (چه در قالب فعل و چه ترک فعل) برای تحقق مسئولیت ضروری است؛ این مدل، که در ماده ۱ قانون مسئولیت مدنی تبلور یافته، برای دعاوی سنتی مانند حوادث رانندگی یا تعدی مستقیم مناسب است، اما در مواجهه با نقض حریم خصوصی توسط پلتفرم‌ها، کارایی خود را به شدت از دست می‌دهد. چالش اصلی، اثبات «تقصیر» در فرایندهای خودکار و الگوریتمی است؛ به عنوان مثال، اگر یک الگوریتم پیشنهاددهنده پلتفرم، داده‌های خصوصی کاربران را به طور ناخواسته برای مقاصد تبلیغاتی استفاده کند، اثبات اینکه مدیران پلتفرم مستقیماً در این طراحی مرتکب تقصیر شده‌اند، نیازمند دسترسی به کدهای منبع و فرایندهای داخلی پیچیده است که غالباً توسط قراردادهای محرمانگی پلتفرم‌ها مسدود می‌شود (شرفخواه و همکاران، ۱۴۰۴).

به دلیل دشواری‌های اثباتی مرتبط با تقصیر در محیط دیجیتال، دکترین حقوقی به سمت توسعه مسئولیت مبتنی بر «خطر» (Risk-Based Liability) یا مسئولیت عینی حرکت کرده است؛ در این رویکرد، تمرکز از رفتار زیان‌آور مرتکب به ماهیت فعالیت زیان‌آور منتقل می‌شود. پلتفرم‌های بزرگ اینترنتی که بر پایه جمع‌آوری، پردازش و بهره‌برداری تجاری از حجم عظیمی از داده‌های شخصی بنا شده‌اند، از منظر حقوقی نوعی «فعالیت پرخطر» محسوب می‌شوند؛ زیرا هرگونه نقص در این فعالیت، پتانسیل ایجاد خسارت گسترده و غیرقابل جبران را دارد. مسئولیت مبتنی بر خطر، ایجاب می‌کند که هرگاه فعالیت‌های مجاز، پتانسیل آسیب‌رسانی داشته باشند (صرف‌نظر از وجود تقصیر)، متصدی فعالیت باید مسئولیت نتایج را بپذیرد، مگر آنکه بتواند اثبات کند که زیان ناشی از قوه قاهره یا تقصیر کامل زیان‌دیده بوده است (رضوی‌فرد و همکاران، ۱۳۹۵). تطبیق این نظریه با حریم خصوصی، مستلزم این است که جمع‌آوری و پردازش داده‌های شخصی، به خودی خود، یک فعالیت پرخطر تلقی شود؛ زیرا همواره این ریسک وجود دارد که داده‌ها به اشتباه مورد استفاده قرار گیرند، نشت کنند، یا مورد بهره‌برداری غیرمجاز واقع شوند. این رویکرد، بار اثبات را از دوش کاربر برداشته و پلتفرم را ملزم می‌سازد که نه تنها از خود در برابر تقصیر دفاع کند، بلکه باید اثبات نماید که تدابیر امنیتی و حفاظتی کافی را برای مدیریت ریسک ذاتی فعالیت خود به کار بسته است، که این امر از طریق استانداردهای امنیتی خاص در قوانین حفاظت از داده‌ها قابل تعریف است.

مسئولیت مبتنی بر «تضمین حق» (Guarantee Liability)، رویکردی افراطی‌تر است که گاهی در قبال برخی فعالیت‌ها اعمال می‌شود، به این معنا که متعهد، فارغ از هرگونه تقصیر یا ریسک، باید نتیجه مورد انتظار ذی‌نفع را تضمین کند؛ اگرچه اعمال کامل این مبنا برای تمام فعالیت‌های پلتفرم‌های اینترنتی ممکن است نوآورانه و غیرعملی باشد، اما در مورد تضمین امنیت داده‌های حساس که کاربران انتظار مطلق حفاظت از آنها را دارند، می‌توان از این مبنا الهام گرفت. در واقع، این امر به معنای فرض وجود مسئولیت است مگر اینکه پلتفرم بتواند دفاعیات قوی مبتنی بر عدم وقوع نقض یا خارج از حوزه کنترل خود بودن نقض را ارائه دهد. در حقوق ایران، تلفیق این مبانی در حال وقوع است؛ هرچند قانون مدنی ریشه در تقصیر دارد، اما قانون‌گذار در حوزه‌های تخصصی‌تر مانند مسئولیت کارفرمایان در قبال اعمال کارکنان (ماده ۱۲ قانون مسئولیت مدنی) یا مسئولیت ناشی از استفاده از ابزار خطرناک، به سمت مسئولیت عینی متمایل شده است. در فضای مجازی، مسئولیت پلتفرم‌ها به عنوان متصدیان زیرساخت‌های جمع‌آوری داده، نیازمند پذیرش این تحول بنیادین است که جمع‌آوری داده‌های شخصی، به دلیل ارزش و حساسیت ذاتی این دارایی، باید به عنوان فعالیت دارای ریسک ذاتی شناخته شود (صادقی و همکاران، ۱۴۰۰).

علاوه بر این، باید به مسئولیت «اخلاقی» و «اجتماعی» پلتفرم‌ها نیز توجه داشت که این دو به طور فزاینده‌ای در ساختار مسئولیت مدنی ادغام می‌شوند؛ نقض حریم خصوصی منجر به تضعیف اعتماد عمومی به سیستم‌های دیجیتال می‌شود که این خود خسارت غیرمستقیمی به کل جامعه وارد می‌کند. در کشورهایی که جرمه‌های تنبیهی اعمال می‌شود، این جرمه‌ها عملاً به عنوان نوعی جبران خسارت اجتماعی و ابزاری برای تضمین رعایت استانداردهای سختگیرانه توسط نهادهای قدرتمند تلقی می‌گردند و از این حیث، فراتر از جبران خسارت سنتی عمل می‌کنند. در نهایت، حقوق قراردادهای نیز در اینجا نقش دارد؛ اگرچه مسئولیت مدنی مبتنی بر قواعد عمومی است، اما تعهدات قراردادی پلتفرم‌ها نسبت به کاربران (مندرج در شرایط خدمات) باید به عنوان حداقل استاندارد برای رعایت حریم خصوصی در نظر گرفته شود؛ هرگونه تخلف از این تعهدات قراردادی که منجر به نقض حریم خصوصی شود، باید به عنوان نقض تعهد تلقی شده و مسئولیت مدنی ناشی از آن محقق گردد، حتی اگر در ظاهر، تقصیر سنتی قابل احراز نباشد. این

امر، مسیر را برای اعمال مسئولیت مبتنی بر نقض تعهد قراردادی (Breach of Contract) فراهم می‌آورد که غالباً نیازی به اثبات تقصیر در کنار اثبات نقض ندارد.

۵. تعهدات قانونی و قراردادی پلتفرم‌ها در حوزه حفاظت از حریم خصوصی

تعهدات پلتفرم‌ها در قبال حریم خصوصی کاربران، یک ساختار دوگانه را تشکیل می‌دهد که از یک سو شامل الزاماتی است که مستقیماً از قوانین آمره (مانند قوانین حفاظت از داده‌ها و جرایم رایانه‌ای) نشأت می‌گیرد و از سوی دیگر، تعهداتی است که پلتفرم داوطلبانه یا از طریق اجبار قراردادی با کاربران متعهد شده است (حق جو و همکاران، ۱۴۰۲). در سطح قانونی، مهم‌ترین تعهد، الزام به فراهم آوردن امنیت فنی کافی برای محافظت از داده‌های جمع‌آوری شده در برابر دسترسی‌های غیرمجاز، افشاجری و تخریب است؛ این تعهد معمولاً شامل اجرای تدابیر فنی و سازمانی متناسب با ریسک است، که باید در طول چرخه عمر داده‌ها (از جمع‌آوری تا حذف) رعایت شود.

در حقوق ایران، اگرچه یک قانون جامع حفاظت از داده‌ها با قدرت اجرایی کامل هنوز به طور کامل مستقر نشده است، قوانین پراکنده‌ای مانند قانون تجارت الکترونیکی و قانون جرایم رایانه‌ای، وظایفی را برای ارائه‌دهندگان خدمات اینترنتی در زمینه حفظ امنیت اطلاعات کاربران تعیین کرده‌اند؛ این قوانین، هرچند کلی، مبنایی را برای انتساب مسئولیت در صورت سهل‌انگاری در اجرای تدابیر امنیتی فراهم می‌آورند. برای مثال، عدم اعمال رمزنگاری مناسب یا عدم اجرای پروتکل‌های احراز هویت قوی می‌تواند به عنوان نقض تکالیف قانونی تلقی شود. علاوه بر تکالیف قانونی، تعهدات قراردادی که از طریق شرایط و ضوابط خدمات (Terms of Service) ایجاد می‌شوند، بخش قابل توجهی از چارچوب مسئولیت پلتفرم‌ها را تشکیل می‌دهند (واثقی و همکاران، ۱۴۰۴)؛ این تعهدات معمولاً شامل اعلام صریح در مورد نوع داده‌هایی که جمع‌آوری می‌شوند، مدت زمان نگهداری و طرف‌هایی است که داده‌ها با آنها به اشتراک گذاشته می‌شوند. اگر پلتفرمی برخلاف تعهد صریح مندرج در T&S خود عمل کند (مثلاً استفاده از داده‌های تحلیلی برای اهداف تبلیغاتی در حالی که وعده داده بود این کار را نخواهد کرد)، این امر مستقیماً مبنای مسئولیت مدنی مبتنی بر نقض تعهد قراردادی قرار می‌گیرد.

چالش حقوقی مهم در این حوزه، اعتبار این تعهدات قراردادی است؛ به ویژه در مورد رضایت آگاهانه. اگر شرایط خدمات به گونه‌ای تنظیم شده باشد که کاربر عملاً مجبور به پذیرش شرایط غیرمنصفانه باشد (مانند شرایط «بگیر و برو»)، دادگاه‌ها می‌توانند با استناد به قواعد حمایت از مصرف‌کننده و اصل حسن نیت، این شروط را باطل یا غیرقابل اجرا بدانند، به خصوص اگر مفاد آن به طور ناعادلانه حقوق بنیادین حریم خصوصی کاربر را سلب نماید. مسئولیت مدنی پلتفرم باید حداقل به اندازه تعهدات اعلامی خود در قرارداد باشد، اما نمی‌تواند از حداقل استانداردهای قانونی لازم‌الاجرا فراتر رود. یکی از مهم‌ترین تعهدات قانونی که در نظام‌های پیشرو (مانند GDPR) الزام شده است، تعهد به «حریم خصوصی ذاتی طراحی» (Privacy by Design) و «حریم خصوصی پیش‌فرض» (Privacy by Default) است؛ این بدان معناست که در طراحی هر سرویس جدید یا ویژگی جدید، تدابیر حفاظتی باید از ابتدا تعبیه شوند و تنظیمات پیش‌فرض برای کاربر باید همواره محافظه‌کارانه‌ترین حالت ممکن را در نظر بگیرد. نقض این اصل طراحی، یک نقض

تکلیفی دائمی است و می‌تواند مبنای مسئولیت مدنی مستمر قرار گیرد، حتی اگر در لحظه خاصی داده‌ای نشت نکرده باشد، زیرا ریسک را به شکلی غیرقابل قبول افزایش داده است (محمدی، ۱۴۰۴).

در مواردی که داده‌ها بین پلتفرم و اشخاص ثالث (مانند تبلیغ‌کنندگان یا توسعه‌دهندگان اپلیکیشن‌های متصل) به اشتراک گذاشته می‌شوند، پلتفرم‌ها وظیفه دارند از اشخاص ثالث نیز تضمین‌های کافی را دریافت نمایند؛ این تعهد به زنجیره پردازش داده‌ها (Data Processing Chain) سرایت می‌کند. اگر پلتفرمی با یک شرکت وابسته یا پیمانکار فرعی داده‌ها را به اشتراک بگذارد و آن شرکت ثالث اقدام به نقض حریم خصوصی کند، پلتفرم اصلی به عنوان کنترل‌کننده اصلی داده‌ها، مسئولیت مدنی متوجه اشخاصی است که آنها را به زنجیره پردازش وارد کرده است (منصوری و همکاران، ۱۴۰۴)؛ این امر مسئولیت پلتفرم را گسترش داده و آن را از یک رابطه صرفاً دوطرفه، به یک مسئولیت چندجانبه تبدیل می‌کند. همچنین، پلتفرم‌ها تعهد دارند در صورت وقوع نقض داده (Data Breach)، ظرف مدت زمان مشخصی (که در قوانین پیشرو تعیین شده است) به مرجع نظارتی و در صورت لزوم به کاربران متأثر اطلاع‌رسانی نمایند؛ این تعهد به اطلاع‌رسانی (Notification Duty)، هرچند مستقیماً جبران خسارت محسوب نمی‌شود، اما بخشی از تکالیف مراقبتی است و عدم انجام آن می‌تواند دلیلی مضاعف برای اثبات سهل‌انگاری و افزایش دامنه مسئولیت مدنی باشد، زیرا تأخیر در اطلاع‌رسانی فرصت قربانی برای کاستن از خسارات آتی را از بین می‌برد. در مجموع، چارچوب تعهدات پلتفرم‌ها در حال تغییر از یک تعهد به «انجام کار» (به معنای فراهم کردن زیرساخت) به تعهدی به «حصول نتیجه» (حفظ امنیت و محرمانگی داده‌ها در طول عمر خود) است؛ این تغییر پارادایم، مستلزم آن است که دادگاه‌ها و قانون‌گذاران، تکالیف قراردادی و قانونی را به شکلی تفسیر کنند که پاسخگوی پیچیدگی‌های فنی و مقیاس فعالیت این نهادها در حوزه حفظ حریم خصوصی باشد.

۶. نقش رضایت آگاهانه کاربران و چالش‌های اثبات آن

رضایت آگاهانه (Informed Consent) به عنوان ستون فقرات مشروعیت پردازش داده‌ها در بسیاری از نظام‌های حقوقی، از جمله آنچه در حوزه حفاظت از داده‌ها مورد تأکید قرار می‌گیرد، شرط اساسی برای هرگونه اقدام پلتفرم بر روی اطلاعات شخصی کاربران محسوب می‌شود؛ این رضایت باید به صورت آزادانه، مشخص، آگاهانه و صریح (در برخی موارد) اخذ شود تا هرگونه تعامل بعدی پلتفرم با داده‌ها را مشروعیت بخشد و در نتیجه، از تحقق مسئولیت مدنی ناشی از نقض حریم خصوصی جلوگیری نماید. با این حال، در محیط پلتفرم‌های بزرگ فناوری، اجرای واقعی این اصل با موانع ساختاری و روانشناختی متعددی روبرو است که کارکرد حمایتی آن را تضعیف کرده است (ایران‌نژاد و همکاران، ۱۴۰۴).

مهم‌ترین چالش در این زمینه، ماهیت «اجباری» رضایت در اقتصاد پلتفرمی است؛ کاربران برای دسترسی به خدمات ضروری روزمره مانند ارتباطات، خرید یا اطلاعات، ناچار به پذیرش شرایط سرویس پلتفرم‌ها هستند؛ از آنجا که این شرایط معمولاً غیرقابل مذاکره هستند و اغلب در قالب متونی طولانی، فنی و مملو از اصطلاحات حقوقی ارائه می‌شوند، کاربر در موقعیتی نیست که بتواند به طور واقعی، منافع و خطرات مرتبط با هر بخش از پردازش داده‌ها را سنجیده و تصمیم‌گیری کند؛ این وضعیت، رضایت را از حالت «آزادانه» خارج ساخته و به نوعی «تسلیم اجباری» تبدیل می‌کند. از منظر حقوقی، رضایت آگاهانه مستلزم برخورداری کاربر از درک کافی نسبت به پیامدهای اقدام خود است؛ پلتفرم‌ها موظفند اطلاعات مربوط به جمع‌آوری داده‌ها، نحوه استفاده، مدت زمان ذخیره‌سازی

و اشخاص ثالث دریافت‌کننده را به زبانی ساده، واضح و قابل فهم ارائه دهند (پیشنماز و همکاران، ۱۴۰۲)؛ اما واقعیت این است که اکثر کاربران این متون طولانی را مطالعه نمی‌کنند، یا اگر مطالعه کنند، پیچیدگی فنی شیوه‌های پروفایل‌سازی و تحلیل داده‌های آن‌ها فراتر از درک عموم است؛ این امر نشان می‌دهد که رضایت اخذ شده غالباً «آگاهانه» نیست و می‌تواند در محاکم به عنوان رضایت صوری تلقی شود.

علاوه بر این، پلتفرم‌ها اغلب از ترفندهای طراحی روانشناختی (Dark Patterns) برای هدایت کاربران به سمت انتخاب‌هایی استفاده می‌کنند که بیشترین نفع را برای خود پلتفرم داشته و کمترین حفظ حریم خصوصی را برای کاربر به ارمغان می‌آورد؛ این ترفندها می‌توانند شامل دشوار ساختن فرآیند لغو اشتراک، پنهان کردن گزینه‌های امنیتی یا استفاده از طراحی‌هایی باشند که پذیرش اشتراک‌گذاری داده‌ها را به صورت پیش‌فرض جا بیندازند. اعمال این روش‌ها به منزله نقض اصل «حسن نیت» در روابط قراردادی است و می‌تواند مبنایی قوی برای رد اعتبار رضایت اخذ شده و در نتیجه، تحقق مسئولیت مدنی پلتفرم باشد. در مواردی که پلتفرم‌ها به صورت ضمنی و از طریق تحلیل رفتار کاربر (رفتارهای استنباطی)، به داده‌هایی دست می‌یابند که کاربر صراحتاً آنها را افشا نکرده است (مانند گرایش‌های سیاسی از روی فعالیت‌های مرور)، چالش اثبات رضایت برای پلتفرم دوچندان می‌شود؛ پلتفرم باید بتواند اثبات کند که کاربر به طور خاص رضایت داده است که این داده‌های استنتاجی نیز مورد پردازش قرار گیرند، که این امر در عمل تقریباً غیرممکن است، مگر آنکه کاربر به طور صریح در مورد تحلیل‌های الگوریتمی نیز رضایت داده باشد.

در صورت نقض حریم خصوصی، فقدان رضایت آگاهانه، مستقیماً پلتفرم را در موقعیت مسئولیت مدنی قرار می‌دهد؛ اگر رضایت به عنوان یک مجوز قانونی برای پردازش داده تلقی شود، هرگونه پردازش بدون رضایت معتبر، به خودی خود یک «نقض غیرقانونی» است و می‌تواند مبنای مسئولیت عینی قرار گیرد، حتی اگر خسارت مادی مشخصی بلافاصله قابل اثبات نباشد. این بدان معناست که صرف نقض اصل رضایت می‌تواند منجر به تحقق مسئولیت و تحمیل جبران خسارت شود. در نظام حقوقی ایران، با توجه به عدم وجود مقررات جزئی در مورد رضایت در حوزه داده، دادگاه‌ها اغلب به اصول عمومی قراردادها رجوع می‌کنند و این امکان را دارند که رضایت‌های کلی و غیرمشخص را در قراردادهای الحاقی بی‌اعتبار بدانند؛ با این حال، فقدان دکترین حقوقی مشخص برای «رضایت در فضای داده» باعث می‌شود قضات در قضاوت خود میان حفظ آزادی عمل پلتفرم در نوآوری و لزوم حمایت از کاربران سردرگم باشند. لذا، راهکار حقوقی قوی‌تر، نیازمند آن است که رضایت در زمینه حریم خصوصی، از یک شرط قراردادی به یک «لزام اساسی قانونی» ارتقا یابد، به نحوی که عدم رعایت استانداردهای سختگیرانه برای کسب رضایت (مانند شفافیت کامل و امکان لغو آسان)، به طور خودکار مسئولیت مدنی را فعال سازد و بار اثبات را از دوش کاربر برداشته و بر دوش پلتفرمی بگذارد که قدرت تنظیم و طراحی فرآیند کسب رضایت را در اختیار دارد (حسام و همکاران، ۱۴۰۲).

۷. نقض داده‌های شخصی و مسئولیت ناشی از عملکرد الگوریتم‌ها

نقض داده‌های شخصی (Data Breach) یکی از شایع‌ترین و مخرب‌ترین اشکال نقض حریم خصوصی توسط پلتفرم‌ها است که دو منشأ اصلی دارد: اول، نشت داده‌ها به دلیل ضعف‌های امنیتی یا حملات سایبری که مستقیماً به سرقت اطلاعات منجر می‌شود؛ و دوم، افشای داده‌ها به دلیل سوءاستفاده داخلی یا استفاده غیرمجاز توسط اشخاص ثالث مجاز. در هر دو حالت، مسئولیت مدنی پلتفرم

به طور مستقیم مطرح می‌شود؛ در حالت اول، مسئولیت بر پایه تقصیر در اجرای تدابیر امنیتی پایه استوار است، و در حالت دوم، مسئولیت ناشی از «انتخاب شریک» یا «نظارت ناکافی» بر پردازشگران ثانویه است. در سطح اثبات مسئولیت ناشی از نشت داده، در صورتی که پلتفرم ادعا کند تمام تدابیر امنیتی استاندارد را رعایت کرده است، این ادعا باید با ارائه مستندات فنی دقیق تأیید شود؛ با این حال، با توجه به پیچیدگی شبکه‌ها، بسیاری از نظام‌های حقوقی مدرن، به ویژه در مواجهه با نقض‌های گسترده، به سمت مسئولیت عینی سوق یافته‌اند (رمضانیان سیاهکلرودی و همکاران، ۱۳۹۹)؛ این یعنی هرگاه پلتفرم نتواند اثبات کند که نقض به هیچ وجه ناشی از قصور در نگهداری داده‌ها نبوده است، مسئول شناخته می‌شود. این رویکرد، پلتفرم را وادار می‌کند که نه تنها بهترین شیوه‌های امنیتی زمان خود را اعمال کند (Standard of Care)، بلکه فراتر از آن، تدابیر پیشگیرانه را برای کاهش آسیب‌پذیری‌های ساختاری به کار گیرد.

مسئولیت ناشی از عملکرد الگوریتم‌ها، چالش نوین‌تری را مطرح می‌کند؛ الگوریتم‌های پیچیده، به ویژه در حوزه‌هایی مانند رسانه‌های اجتماعی، تبلیغات هدفمند و رتبه‌بندی محتوا، می‌توانند با استفاده از داده‌های شخصی، به نتایجی برسند که تبعیض‌آمیز بوده یا به شکل ظریفی حریم خصوصی افراد را نقض کند. برای مثال، اگر یک الگوریتم، افراد دارای سابقه مالی خاصی را از دیدن آگهی‌های وام‌های کم‌بهره محروم سازد، این یک تصمیم الگوریتمی مبتنی بر پروفایل‌سازی است که می‌تواند نقض اصل عدم تبعیض و حریم خصوصی تلقی شود. چالش اثبات تقصیر در اینجا بسیار بالاست، زیرا کاربر نمی‌تواند به سادگی ثابت کند که الگوریتم به دلیل نقص در برنامه‌نویسی منجر به این تبعیض شده است؛ بنابراین، حقوق باید مدلهایی را برای انتساب مسئولیت در برابر خروجی‌های الگوریتمی توسعه دهد. یکی از رویکردها، مسئولیت مبتنی بر «اثر» است؛ اگر خروجی الگوریتم به طور سیستماتیک منجر به نتایج تبعیض‌آمیز یا نقض حقوق شود، مسئولیت متوجه طراح و مالک الگوریتم (پلتفرم) است، زیرا آنها مسئول طراحی سیستمی هستند که این نتایج را تولید می‌کند؛ این همان مفهوم «حریم خصوصی ذاتی طراحی» است که باید بر خروجی‌های الگوریتمی نیز اعمال شود (ابهری و همکاران، ۱۳۹۱).

در حقوق ایران، اگر نقض الگوریتمی منجر به ضرر مادی شود، می‌توان از قواعد عمومی مسئولیت مدنی استفاده کرد، اما چالش اصلی در اثبات رابطه سببیت میان تصمیم الگوریتم و ضرر کاربر است؛ مگر اینکه قانون‌گذار به صراحت، پلتفرم‌ها را ملزم کند که امکان «تفسیرپذیری الگوریتم» (Explainability) را برای مراجع قضایی فراهم آورند تا مشخص شود چرا یک تصمیم خاص اتخاذ شده است. این شفافیت الگوریتمی یک پیش‌نیاز اساسی برای اعمال مسئولیت مدنی کارآمد در این حوزه است. علاوه بر این، نقض حریم خصوصی می‌تواند از طریق «همبستگی‌سازی داده‌ها» (Data Correlation) اتفاق بیفتد؛ زمانی که پلتفرم‌ها از داده‌هایی که به طور مجزا غیرحساس تلقی می‌شوند، با ترکیب آنها، اطلاعات بسیار حساس و خصوصی را استخراج می‌کنند. این عمل، اگر بدون رضایت صریح کاربر صورت گیرد، می‌تواند به دلیل خلق داده‌های جدید که در حوزه کنترل فرد خارج شده‌اند، مبنای مسئولیت مدنی قرار گیرد. این امر نیازمند آن است که مفهوم داده شخصی را به «داده‌های استنتاجی» نیز تعمیم دهیم و پلتفرم را مسئول حفاظت از این داده‌های خلق شده بدانیم. در نهایت، مسئولیت پلتفرم‌ها در قبال نقض داده‌ها باید شامل جبران خسارت‌های پیشگیرانه نیز باشد؛ اگر یک نقض داده کوچک در یک بخش از پلتفرم رخ دهد، اما نشان‌دهنده یک نقص ساختاری وسیع‌تر باشد، پلتفرم باید ملزم به اصلاح کل سیستم خود باشد، حتی اگر این اصلاحات منجر به توقف موقت سرویس یا کاهش سودآوری شود؛ این الزام، نوعی

مسئولیت تکلیفی پیشگیرانه است که در حوزه مدنی با هدف کاهش ریسک‌های آتی اعمال می‌گردد و به مسئولیت سنتی جبران خسارت اضافه می‌شود (ملکوتی خلیل‌زاده و همکاران، ۱۳۹۹).

۸. چالش‌های اثبات تقصیر، جبران خسارت و رویه‌های قضایی

یکی از بزرگ‌ترین موانع در طرح دعاوی مسئولیت مدنی علیه پلتفرم‌های اینترنتی در خصوص نقض حریم خصوصی، دشواری اثبات تقصیر یا رابطه سببیت در یک محیط فنی بسیار پیچیده و کم‌شفاف است. در نظام حقوقی ایران که تکیه اصلی بر نظریه تقصیر است، کاربر باید نشان دهد که پلتفرم به طور مشخص، کوتاهی در مراقبت از داده‌ها کرده است؛ این اثبات نیازمند دسترسی به سوابق سرورها، گزارش‌های امنیتی، ساختار رمزنگاری و تصمیمات داخلی تیم‌های فنی است؛ اموری که معمولاً خارج از دسترس عموم و حتی تیم حقوقی شاکی قرار دارند و پلتفرم‌ها با استفاده از استناد به اسرار تجاری، از افشای آنها طفره می‌روند. برای غلبه بر این «چالش اثبات»، برخی نظام‌های حقوقی اقدام به انتقال بار اثبات (Burden of Proof) نموده‌اند؛ یعنی به جای آنکه کاربر تقصیر پلتفرم را ثابت کند، پلتفرم باید ثابت کند که تمام تدابیر لازم را برای جلوگیری از نقض به کار بسته است؛ این تغییر پارادایم، در صورت پذیرش در حقوق ایران، می‌تواند عدالت رویه‌ای را در دعاوی مربوط به فناوری به شدت ارتقا دهد، چرا که پلتفرم‌ها تنها نهادهایی هستند که کنترل کافی بر فرآیندهای فنی و داده‌ها دارند.

در زمینه جبران خسارت، آسیب‌های ناشی از نقض حریم خصوصی معمولاً ماهیت غیرمادی دارند؛ از دست رفتن اعتماد، نگرانی بابت سرقت هویت، آسیب به اعتبار اجتماعی و لطمه به آزادی‌های فردی، از جمله خساراتی هستند که ارزیابی آنها بر اساس رویه‌های سنتی خسارت معنوی دشوار است. قانون‌گذار ایرانی عموماً در مورد جبران خسارت معنوی، رویکرد نسبتاً محدودی دارد و میزان آن را به صلاحدید دادگاه واگذار می‌کند؛ این ابهام، منجر به عدم قطعیت در میزان جبران می‌شود و ممکن است پلتفرم‌ها را از اهمیت جبران خسارت بازدارنده نماند. از منظر تطبیقی، مقرراتی مانند GDPR اتحادیه اروپا، با تعریف مسئولیت عینی برای نقض اصول حفاظت از داده‌ها، نه تنها جبران خسارت مالی را برای قربانی تضمین می‌کنند، بلکه با اعمال جریمه‌های اداری سنگین (تا ۴ درصد از گردش مالی جهانی سالانه)، یک بازدارندگی اقتصادی قدرتمند ایجاد می‌نمایند؛ این جریمه‌ها، که به دولت پرداخت می‌شود، هدفشان حمایت از منافع عمومی و تضمین رعایت استانداردهای حریم خصوصی در مقیاس کلان است و اثر تکمیلی بر جبران خسارت فردی دارد.

رویکردهای قضایی در ایران در سال‌های اخیر، نشان‌دهنده تلاش برای انطباق قواعد سنتی با فضای مجازی است؛ دادگاه‌ها در مواردی که تخلفات سایبری منجر به ضرر آشکار شده باشد، به سمت مسئول شناختن متخلف حرکت کرده‌اند؛ با این حال، رویه قضایی منسجم و مشخصی که صرفاً بر اساس نقض در اجرای پروتکل‌های حفاظتی داده‌ها (بدون نیاز به اثبات تقصیر عرفی) حکم به مسئولیت پلتفرم دهد، هنوز تثبیت نشده است. این امر ناشی از عدم وجود قوانین تفصیلی در زمینه استانداردسازی امنیت سایبری برای پلتفرم‌ها است. چالش دیگر، جبران خسارت در دعاوی کلاس «دعوی جمعی» (Class Action) یا نمایندگی است؛ هنگامی که میلیون‌ها کاربر به طور همزمان متأثر از یک نقض داده قرار می‌گیرند، طرح دعاوی فردی عملاً غیرممکن می‌شود و اثربخشی جبران خسارت کاهش می‌یابد. فقدان یک سازوکار مؤثر برای طرح دعاوی جمعی در حقوق ایران، امکان اعمال فشار مؤثر بر پلتفرم‌ها برای

اصلاح رویه‌های خود را تضعیف می‌کند و جبران خسارت را به امری نمادین تقلیل می‌دهد. بنابراین، برای تحقق عدالت در این حوزه، لازم است که ابتدا یک چارچوب فنی استاندارد برای «مراقبت معقول» در حوزه امنیت داده‌ها تعریف شود تا معیار اثبات تقصیر یا عدم رعایت آن مشخص گردد؛ در صورت عدم وجود این استاندارد، باید مسئولیت عینی را برای نقض اصول محرمانگی داده‌ها پذیرا شد تا جبران خسارت به جای آنکه یک فرآیند طاقت‌فرسا باشد، به یک حق قابل اجرا تبدیل شود (شرفخواه و همکاران، ۱۴۰۴).

۹. جایگاه حقوق ایران و اسناد بین‌المللی در تعریف مسئولیت پلتفرم‌ها

تحلیل جایگاه مسئولیت مدنی پلتفرم‌ها در حقوق ایران نشان می‌دهد که این نظام حقوقی در مواجهه با اقتصاد داده‌محور، دچار «ناهمخوانی مفهومی» است؛ در حالی که قانون مدنی بر پایه مسئولیت فردی و مبتنی بر تقصیر بنا شده است، ماهیت فعالیت پلتفرم‌ها ماهیتی سیستمی، واسطه‌ای و مبتنی بر جمع‌آوری انبوه داده است که نیازمند چارچوب‌های حمایتی جدید است. قانون جرایم رایانه‌ای بخش‌هایی از حفاظت از حریم خصوصی را پوشش می‌دهد، اما بیشتر ماهیت کیفری دارد و سازوکارهای دقیق مسئولیت مدنی و نحوه جبران خسارت ناشی از نقض حریم خصوصی داده‌محور را به طور کامل تبیین نمی‌کند و عمدتاً بر اعمال مجرمانه سنتی تمرکز دارد. نقطه عطف حقوق بین‌الملل در این حوزه، ظهور سند جامع حمایت از داده‌ها، به ویژه مقررات عمومی حفاظت از داده‌ها (GDPR) اتحادیه اروپا است؛ این سند با تعریف دقیق نهادهای «کنترل‌کننده» و «پردازشگر» داده‌ها، مسئولیت مدنی را به طور صریح و بدون نیاز به اثبات تقصیر عام بر دوش کنترل‌کننده می‌گذارد، در صورتی که اصول بنیادین حفاظت از داده‌ها (مانند تناسب، شفافیت و امنیت) نقض شود. این مقررات، پلتفرم‌ها را ملزم به اجرای تدابیر فنی پیشگیرانه می‌دانند و عدم رعایت آنها به صورت مستقیم موجب تحقق مسئولیت مدنی می‌شود (رمضانیان سیاهکلودی و همکاران، ۱۳۹۹).

اسناد بین‌المللی همچنین بر مفهوم «حاکمیت داده» (Data Sovereignty) تأکید دارند و تلاش می‌کنند تا از طریق قواعد حل تعارض قوانین، دامنه شمول قوانین حمایتی را بر پلتفرم‌های مستقر در خارج از مرزها اعمال کنند، به شرطی که خدمات خود را به شهروندان آن کشور ارائه دهند؛ این رویکرد، تلاش می‌کند تا معضل صلاحیت قضایی را که در بخش دوم مطرح شد، تا حدی مرتفع سازد و مانع از پناه بردن پلتفرم‌ها به حوزه‌های قضایی با مقررات حمایتی ضعیف‌تر شود. در حقوق ایران، خلأ قانونی اصلی در زمینه تصویب یک قانون جامع حفاظت از داده‌های شخصی است که بتواند وظایف دقیق، استانداردهای فنی لازم‌الاجرا و سازوکارهای نظارتی مؤثری را برای پلتفرم‌ها تعریف کند؛ تا زمانی که چنین قانونی وجود نداشته باشد، دادگاه‌ها ناچارند با استناد به قواعد کلی، تفسیرهای خود را اعمال کنند که این امر منجر به رویه‌های قضایی ناهماهنگ و کم‌تأثیر خواهد شد.

مسئولیت ناشی از داده‌های شخصی در حقوق ایران، غالباً از طریق احکام مربوط به «اسرار» و «آبروی اشخاص» در قانون مدنی قابل پیگیری است، اما این مفاهیم به سختی می‌توانند پیچیدگی نقض حریم خصوصی در فرآیندهای الگوریتمی و جمع‌آوری داده‌های غیرعلنی را پوشش دهند؛ لذا، نیاز مبرمی به تفسیر گسترده‌تر مفهوم «ضرر» در دعاوی مدنی سایبری وجود دارد تا شامل خساراتی همچون از دست رفتن فرصت‌ها به دلیل پروفایل‌سازی ناعادلانه نیز گردد. علاوه بر این، کنوانسیون‌های بین‌المللی مانند کنوانسیون اروپایی حمایت از حقوق بشر و آزادی‌های اساسی (ماده ۸) و همچنین اعلامیه‌های سازمان ملل در مورد حق حریم خصوصی، به عنوان مبنایی برای تفسیر قوانین داخلی عمل می‌کنند؛ حقوق دانان ایرانی می‌توانند با ارجاع به تعهدات بین‌المللی پذیرفته‌شده کشور،

استدلال نمایند که حریم خصوصی دیجیتال مستلزم استانداردهای سختگیرانه‌تری از سوی نهادهای غالب بر فضای تبادل اطلاعات است. در نهایت، جایگاه فعلی حقوق ایران نیازمند یک تحول ساختاری است؛ این تحول باید شامل الزام قانونی پلتفرم‌ها به «شفاف‌سازی» در مورد استفاده از الگوریتم‌ها، تعریف وظایف دقیق برای مدیریت ریسک داده‌ها و پذیرش مسئولیت عینی در مواردی باشد که نقض حریم خصوصی ناشی از عدم اجرای تدابیر فنی پیشگیرانه است، همانند آنچه در سطح بین‌المللی به عنوان یک اصل پذیرفته شده درآمده است (ابه‌ری و همکاران، ۱۳۹۱).

نتیجه‌گیری و پیشنهادهای حقوقی و تقنینی

پژوهش حاضر نشان داد که مسئولیت مدنی پلتفرم‌های اینترنتی در قبال نقض حریم خصوصی کاربران، به دلیل ماهیت داده‌محور، پیچیدگی فنی و عدم تقارن قدرت میان پلتفرم‌ها و کاربران، نیازمند بازنگری بنیادین در مبانی نظری و ساختار تقنینی فعلی است. اتکای صرف به مسئولیت مبتنی بر تقصیر سنتی، به واسطه دشواری‌های اثباتی مرتبط با الگوریتم‌ها و فرایندهای خودکار، عملاً کاربران را در دستیابی به جبران خسارت مؤثر محروم می‌سازد. بنابراین، نتیجه‌گیری اصلی این است که برای تضمین حق بنیادین حریم خصوصی در عصر دیجیتال، نظام حقوقی باید به سمت پذیرش مسئولیت عینی یا شبه‌تضمینی در قبال فعالیت‌های پردازش داده‌های شخصی حرکت کند. اولین پیشنهاد تقنینی این است که قانون‌گذار ایران باید با الگوبرداری از اسناد بین‌المللی مانند GDPR، یک قانون جامع حفاظت از داده‌های شخصی را با هدف مشخص کردن دقیق نقش‌ها (کنترل‌کننده و پردازشگر) و تعهدات آنها تدوین نماید. این قانون باید به طور مشخص، «حریم خصوصی ذاتی طراحی» و «حریم خصوصی پیش‌فرض» را به عنوان الزامات فنی لازم‌الاجرا برای تمام پلتفرم‌هایی که خدمات به کاربران ایرانی ارائه می‌دهند، تعریف کند و عدم رعایت این الزامات را مبنای مسئولیت مدنی قرار دهد.

دومین پیشنهاد مربوط به اصلاح رویه اثبات است؛ لازم است که اصل «انتقال بار اثبات» به نفع کاربر متأثر از نقض حریم خصوصی پذیرفته شود؛ بدین ترتیب که در صورت وقوع نقض داده، پلتفرم موظف باشد اثبات نماید که تمام تلاش معقول فنی و مدیریتی را برای پیشگیری از نقض و همچنین اطلاع‌رسانی سریع به قربانیان به کار بسته است. این امر، سهولت طرح دعوی و امکان‌پذیری جبران خسارت را به طور چشمگیری افزایش خواهد داد. سومین گام، بازنگری در مفهوم رضایت آگاهانه و مبارزه با ترفندهای طراحی (Dark Patterns) است؛ پیشنهاد می‌شود که رضایت کسب شده توسط پلتفرم‌ها، تنها در صورتی معتبر تلقی شود که به صورت ماژولار (جزئی‌نگر) و برای هر نوع پردازش داده، به زبانی کاملاً شفاف اخذ شده باشد و امکان لغو آن به سادگی پذیرش فراهم باشد؛ هرگونه استفاده از رضایت کلی برای اهداف پیش‌بینی نشده یا غیرضروری، باید به عنوان نقض تعهد قراردادی و قانونی تلقی شده و مسئولیت مدنی را به دنبال داشته باشد.

چهارمین پیشنهاد، توسعه مبانی جبران خسارت است؛ در دعاوی نقض حریم خصوصی، باید دامنه خسارت معنوی را فراتر از آسیب‌های سنتی گسترش داد و معیاری برای ارزیابی «ارزش اطلاعاتی» از دست رفته و «ریسک‌های آتی» ناشی از پروفایل‌سازی فراهم آورد. همچنین، نهادهای نظارتی باید مجاز به اعمال جریمه‌های اداری تنبیهی سنگین باشند تا جنبه بازدارندگی مسئولیت مدنی تقویت شده و پلتفرم‌ها به سرمایه‌گذاری در امنیت سایبری ترغیب شوند. پنجمین پیشنهاد به حوزه شفافیت الگوریتمی مربوط

می‌شود؛ قانون‌گذار باید پلتفرم‌ها را ملزم نماید تا در صورت درخواست مراجع قضایی یا نظارتی، امکان دسترسی به گزارش‌های تفسیرپذیری الگوریتم‌های خود را فراهم آورند تا بتوان رابطه سببیت میان تصمیم الگوریتمی و آسیب وارده به حریم خصوصی را احراز نمود. این شفافیت، محدود به اسرار تجاری نیست، بلکه به عنوان یک تکلیف مدنی برای تضمین حقوق اساسی افراد در نظر گرفته شود.

ششمین نکته، تأکید بر مسئولیت زنجیره‌ای است؛ پلتفرم‌های اصلی باید مسئولیت مدنی خود را در قبال نقض‌هایی که توسط پردازشگران ثانویه یا شرکای تجاری آنها صورت می‌گیرد، به رسمیت بشناسند و تضمین‌های لازم برای رعایت استانداردهای حفاظت از داده در کل زنجیره را از طریق قراردادهای پشتیبانی و نظارت متعهد گردند. هفتمین پیشنهاد، ایجاد یک سازوکار مؤثر برای دعاوی جمعی (Class Action) در حوزه حقوق مصرف‌کننده و حریم خصوصی است تا کاربران متضرر بتوانند به صورت سازمان‌یافته حقوق خود را پیگیری کنند و از قدرت چانه‌زنی پلتفرم‌های بزرگ در دعاوی فردی کاسته شود؛ این امر به تحقق عدالت در مقیاس کلان کمک می‌کند. در نهایت، نتیجه‌گیری می‌شود که حقوق ایران برای انطباق با الزامات عصر دیجیتال و حمایت شایسته از حریم خصوصی کاربران در قبال پلتفرم‌های قدرتمند، نیاز به یک رویکرد حمایتی فعال و مبتنی بر مسئولیت عینی دارد که در آن، پیشگیری از طریق تعریف استانداردهای فنی دقیق، از جبران خسارت پس از وقوع حادثه اهمیت بیشتری یابد و بدین ترتیب، مسئولیت مدنی به ابزاری کارآمد برای حفظ حقوق بنیادین در اکوسیستم دیجیتال تبدیل شود.

منابع

- بهمن شرفخواه، مهدی فلاح خاریکی. (۲۰۲۵). مسئولیت مدنی اضرار ناشی از فروشگاه‌های اینترنتی در نظام حقوقی ایران. نشریه علمی مطالعات حقوق و علوم قضایی، ۲(۴)، ۵۳۱-۵۴۱.
- ملکوتی، خلیل‌زاده، مونا. (۲۰۲۰). مسئولیت مدنی و بین‌المللی دولت نسبت به خسارات حاصله در فضای اینترنت. حقوق خصوصی احرار، ۱(۱)، ۷۵-۸۸.
- ابهری، میری. (۲۰۱۲). پژوهشی تطبیقی پیرامون مسئولیت مدنی ارائه‌کنندگان خدمات اینترنتی با تأکید بر حقوق آمریکا و اتحادیه اروپا. پژوهش حقوق خصوصی، ۱(۱)، ۱-۳۸.
- رمضانین سیاهکلودی، ع.، دیانی، ع.، زرکلام، س.، ستار. (۲۰۲۰). مسئولیت مدنی واسطه‌های ارائه خدمات اینترنت با تأکید بر نقض مالکیت فکری در فضای سایبر. مطالعات حقوق بشر اسلامی، ۹(۱)، ۲۷۷-۲۹۷.
- حسام، غلامعلی زاده. (۲۰۲۳). مسئولیت مدنی بسترهای مجازی آنلاین در قبال اعمال کاربران. حقوق اسلامی، ۲۰(۷۹)، ۱۲۷-۱۴۵.
- پیشنهاد، سید امین، رکنی، امیر عباس. (۲۰۲۳). تعطیلی پلتفرم‌های مجازی؛ ضرورت تحلیل نظام حاکم بر داده‌های شخصی از منظر حقوق اموال. پژوهش‌های حقوقی، ۲۲(۵۳)، ۴۶۹-۵۰۶.
- ایران نژاد، مهداد، گل پرور. (۲۰۲۵). مقایسه اثربخشی آموزش حضوری و مجازی بسته جامع آموزش شهروندی بر رفتارهای شهروندی رسانه ای و دیجیتالی دانشجویان. پژوهش‌های راهبردی مسائل اجتماعی، ۱۴(۱)، ۲۱-۴۰.

- منصوری، فرنگیس. (۲۰۲۵). کوکی ها و قابلیت تجاوز به حریم خصوصی در فضای سایبر. حقوق فناوری های نوین، ۶(۱۱)، ۳۷۷-۳۹۵.
- محمدی، ف. (۲۰۲۵). بررسی تأثیر شبکه های اجتماعی بر افزایش جرائم سایبری و چالش های حقوقی آن. گفتمان حقوقی، ۱۳(۲۶)، ۳۳-۵.
- واثقی، روشن چراغ، کوثر. (۲۰۲۵). مسئولیت مدنی اضرار ناشی از اشخاص تأثیرگذار در شبکه های اجتماعی. پژوهش های حقوقی.
- حق جو، بابایی، داریوش، جانی پور. (۲۰۲۳). مقدمه ای بر مسئولیت مدنی واسطه ها و شبکه های اجتماعی ارتباطات فضای سایبری. جامعه شناسی سیاسی ایران، ۲۶(۵)، ۹۲۶-۹۳۳.
- صادقی، اسماعیلی، قاسمی. (۲۰۲۱). مسئولیت مدنی دولت در فضای سایبر با نگاهی به آموزه های اخلاق سایبری. فصلنامه اخلاق در علوم و فناوری، ۱۶(۱)، ۸-۱.
- رضوی فرد، موسوی، سید نعمت اله. (۲۰۱۶). مسئولیت کیفری در فضای سایبر در حقوق ایران. فصلنامه پژوهش حقوق کیفری، ۱۶(۱)، ۲۹-۴۵.