

حق بر امنیت داده‌های شخصی

به عنوان نسل جدید حقوق بشر

(تاریخ دریافت ۱۴۰۵/۰۲/۱۲، تاریخ تصویب ۱۴۰۵/۰۳/۱۲)

دکتر فرامرز امجدیان^۱

لیلا رزمجو

چکیده

حق بر امنیت داده‌های شخصی به عنوان یکی از مفاهیم نوظهور در نظام حقوق بشر معاصر، در پی تحولات گسترده فناوری‌های اطلاعاتی و ارتباطی و گسترش اقتصاد داده‌محور، اهمیت فزاینده‌ای یافته است. هدف این پژوهش، تحلیل مفهومی و حقوقی این حق، تبیین مبانی بین‌المللی آن و بررسی چالش‌ها و چشم‌اندازهای آینده در پرتو تهدیدهای نوین دیجیتال است. مسئله اصلی تحقیق آن است که نظام حقوق بین‌الملل تا چه اندازه توانسته است از حق بر امنیت داده‌های شخصی به عنوان یک حق مستقل و بنیادین حمایت مؤثر به عمل آورد. این پژوهش با روش توصیفی-تحلیلی و با تکیه بر منابع کتابخانه‌ای، اسناد بین‌المللی حقوق بشر، مقررات منطقه‌ای نظیر GDPR و رویه‌ها و هنجارهای نوظهور در حقوق بین‌الملل سایبری انجام شده است. یافته‌ها نشان می‌دهد که اگرچه اسناد کلاسیک حقوق بشر به طور مستقیم به امنیت داده‌ها اشاره نکرده‌اند، اما حق حریم خصوصی به عنوان مبنای اصلی این حق قابل تفسیر توسعه‌ای است. همچنین مقررات نوین و استانداردهای بین‌المللی نقش مهمی در شکل‌دهی به یک نظام نسبتاً منسجم در حوزه حفاظت از داده‌ها ایفا کرده‌اند. نتایج پژوهش حاکی از آن است که تهدیدهای نوینی مانند هوش مصنوعی، کلان‌داده‌ها و حملات سایبری، ماهیت نقض داده‌های

^۱ نویسنده مسئول



شخصی را پیچیده‌تر و فرامرزی‌تر کرده و خلأهای جدی در نظام حقوق بین‌الملل ایجاد نموده‌اند. در نهایت، پژوهش نتیجه می‌گیرد که حق بر امنیت داده‌های شخصی در حال تبدیل شدن به یک حق بنیادین مستقل در نظام حقوق بشر است و نیازمند تدوین چارچوب‌های الزام‌آور بین‌المللی و تقویت همکاری‌های جهانی در این حوزه می‌باشد.

واژگان کلیدی: امنیت داده‌های شخصی، حریم خصوصی، حقوق بشر، حقوق بین‌الملل، GDPR، فضای سایبری، کلان‌داده، هوش مصنوعی.

مقدمه

تحول شتابان فناوری‌های دیجیتال در دهه‌های اخیر، به‌ویژه با گسترش اینترنت، کلان‌داده‌ها، هوش مصنوعی و شبکه‌های اجتماعی، ساختارهای سنتی ارتباطی، اقتصادی و اجتماعی را به‌طور بنیادین دگرگون ساخته است. در این میان، داده‌های شخصی به‌عنوان یکی از مهم‌ترین دارایی‌های عصر اطلاعات، جایگاهی محوری در مناسبات فردی و جمعی پیدا کرده‌اند، به‌گونه‌ای که بخش قابل توجهی از هویت دیجیتال اشخاص در قالب داده‌هایی شکل می‌گیرد که در بسترهای مختلف تولید، پردازش و ذخیره می‌شوند. این وضعیت، در عین ایجاد فرصت‌های گسترده برای توسعه خدمات نوین، مخاطرات جدی نیز برای حقوق بنیادین افراد به همراه داشته است. در حقوق کلاسیک بشر، «حریم خصوصی» به‌عنوان مهم‌ترین مبنای حمایت از زندگی شخصی افراد شناخته می‌شود، با این حال، تحولات فناوری موجب شده است که مفهوم سنتی حریم خصوصی دیگر به‌تنهایی پاسخگوی پیچیدگی‌های جدید نباشد. امروزه مسئله صرفاً افشای اطلاعات شخصی نیست، بلکه موضوعاتی چون جمع‌آوری گسترده داده‌ها، پردازش الگوریتمی، تحلیل رفتاری، انتقال فرامرزی داده‌ها و حتی سوءاستفاده‌های مبتنی بر هوش مصنوعی، ابعاد جدیدی از تهدید علیه افراد را ایجاد کرده است. در نتیجه،



مفهوم «امنیت داده‌های شخصی» به عنوان مرحله‌ای فراتر از حریم خصوصی، در ادبیات حقوقی و اسناد بین‌المللی مورد توجه قرار گرفته است. از منظر نظریه‌های حقوق بشر، تحول مفاهیم حقوقی متناسب با نیازهای اجتماعی و فناورانه همواره امری پذیرفته شده بوده است. بر همین اساس، برخی حقوق‌دانان بر این باورند که امنیت داده‌های شخصی می‌تواند به عنوان «نسل جدیدی از حقوق بشر» یا دست کم به عنوان توسعه‌ای از حق بر حریم خصوصی تلقی شود، حتی که نه تنها بر عدم مداخله دولت‌ها، بلکه بر ایجاد سازوکارهای فعال حمایتی، نظارتی و پیشگیرانه در برابر تهدیدات دیجیتال تأکید دارد. این رویکرد، به ویژه در اسناد نوظهور حقوقی مانند مقررات عمومی حفاظت از داده‌ها (GDPR) و رویه‌های قضایی برخی نظام‌های حقوقی، به صورت پررنگ قابل مشاهده است. با وجود این تحولات، همچنان در سطح حقوق بین‌الملل، اجماع روشنی در خصوص شناسایی مستقل «حق بر امنیت داده‌های شخصی» به عنوان یک حق بنیادین وجود ندارد. پراکندگی مقررات، تفاوت رویکرد نظام‌های حقوقی، و چالش‌های ناشی از ماهیت فرامرزی فضای دیجیتال، موجب شده است که حمایت از داده‌های شخصی با نوعی عدم انسجام حقوقی مواجه باشد. این وضعیت، ضرورت بازاندیشی در جایگاه این حق و امکان‌سنجی شناسایی آن در قالب یک حق مستقل بشر را دوچندان کرده است. پژوهش حاضر در پی آن است که با رویکردی توصیفی-تحلیلی، ضمن بررسی مبانی مفهومی و نظری امنیت داده‌های شخصی، جایگاه آن را در نظام حقوق بشر تحلیل کرده و چالش‌ها و چشم‌اندازهای شناسایی آن به عنوان یک حق نوظهور را تبیین نماید. اهمیت این موضوع نه تنها در بُعد نظری و توسعه ادبیات حقوق بشر، بلکه در بُعد عملی و سیاست‌گذاری حقوقی دولت‌ها در عصر دیجیتال نیز قابل توجه است.



• سوالات پژوهش

الف) سؤال اصلی

۱. آیا «حق بر امنیت داده‌های شخصی» قابلیت شناسایی به عنوان نسل جدید حقوق بشر را در نظام حقوق بین‌الملل دارد؟

ب) سؤالات فرعی

۲. مفهوم و قلمرو «امنیت داده‌های شخصی» در مقایسه با حق سنتی حریم خصوصی چیست؟

۳. مهم‌ترین چالش‌های حقوقی و عملی در مسیر شناسایی و اجرای حق بر امنیت داده‌های شخصی کدام‌اند؟

بخش اول: مبانی مفهومی و نظری حق بر امنیت داده‌های شخصی

بند اول: مفهوم داده‌های شخصی و تحولات آن در عصر دیجیتال

داده‌های شخصی در ادبیات حقوقی و فناوری اطلاعات، به هر گونه اطلاعاتی اطلاق می‌شود که به طور مستقیم یا غیرمستقیم قابلیت شناسایی یک شخص حقیقی را فراهم کند. این داده‌ها می‌توانند شامل اطلاعات هویتی مانند نام و نام خانوادگی، شماره ملی، نشانی، شماره تماس، و همچنین داده‌های رفتاری، مالی، موقعیتی و حتی داده‌های زیستی نظیر اثر انگشت یا داده‌های ژنتیکی باشند. در نظام‌های حقوقی معاصر، به ویژه در مقررات نوینی همچون مقررات عمومی حفاظت از داده‌ها (GDPR)، تعریف داده شخصی به صورت گسترده و کارکردمحور ارائه شده است تا بتواند طیف وسیعی از اطلاعات قابل شناسایی را پوشش دهد. تحولات فناوری در عصر دیجیتال موجب شده است که مفهوم داده‌های شخصی از یک مفهوم ساده و ایستا به یک



مفهوم پیچیده، پویا و چندلایه تبدیل شود. در گذشته، داده‌های شخصی عمدتاً در قالب اسناد فیزیکی و پرونده‌های محدود اداری تعریف می‌شدند، اما در عصر حاضر، این داده‌ها به صورت گسترده در بسترهای دیجیتال تولید، ذخیره، پردازش و تحلیل می‌شوند. گسترش شبکه‌های اجتماعی، تجارت الکترونیک، خدمات آنلاین و فناوری‌های مبتنی بر هوش مصنوعی، حجم عظیمی از داده‌های شخصی را ایجاد کرده است که به‌طور مداوم در حال به‌روزرسانی و بازتولید هستند. یکی از مهم‌ترین تحولات در این حوزه، تغییر ماهیت داده‌های شخصی از «اطلاعات منفعل» به «منابع فعال اقتصادی و امنیتی» است. امروزه داده‌های شخصی نه تنها برای شناسایی افراد، بلکه برای تحلیل رفتار، پیش‌بینی الگوهای مصرف، هدف‌گذاری تبلیغاتی و حتی تصمیم‌گیری‌های الگوریتمی مورد استفاده قرار می‌گیرند. این تحول موجب شده است که داده‌های شخصی به یک دارایی ارزشمند در اقتصاد دیجیتال تبدیل شوند و در عین حال، آسیب‌پذیری افراد در برابر سوءاستفاده‌های احتمالی افزایش یابد. مفهوم داده‌های شخصی در عصر دیجیتال دیگر صرفاً یک مفهوم حقوقی محدود به حریم خصوصی نیست، بلکه به یکی از عناصر بنیادین در ساختار حقوق بشر نوین تبدیل شده است، به گونه‌ای که نحوه جمع‌آوری، پردازش و حفاظت از آن‌ها مستقیماً با کرامت انسانی و امنیت فردی افراد ارتباط پیدا می‌کند.

بند دوم: مفهوم امنیت داده‌های شخصی و تمایز آن با حریم خصوصی سنتی

امنیت داده‌های شخصی مفهومی فراتر از صرف «محرمانگی اطلاعات» است و به مجموعه‌ای از سازوکارهای حقوقی، فنی و نهادی اشاره دارد که هدف آن تضمین حفاظت جامع از داده‌های قابل شناسایی افراد در برابر دسترسی غیرمجاز، پردازش غیرقانونی، افشا، تخریب یا سوءاستفاده است. در این چارچوب، امنیت داده‌ها نه تنها ناظر بر جلوگیری از افشای اطلاعات است، بلکه عناصر مهمی همچون یکپارچگی داده‌ها، صحت اطلاعات، کنترل‌پذیری توسط صاحب داده و محدودیت در پردازش را نیز در بر می‌گیرد. به همین دلیل، در اسناد نوین حقوقی مانند مقررات عمومی حفاظت از داده‌ها (GDPR)، امنیت داده‌ها به عنوان یک تعهد فعال برای



کنترل کنندگان و پردازش گران داده تعریف شده است، نه صرفاً یک وضعیت منفعل. در مقابل، مفهوم سنتی حریم خصوصی عمدتاً بر «حق فرد بر عدم مداخله دیگران در زندگی شخصی» و حفاظت از خلوت فردی تمرکز دارد و بیشتر جنبه منفی (negative right) دارد، یعنی دولت‌ها و اشخاص ثالث باید از دخالت در حوزه خصوصی افراد خودداری کنند. این رویکرد در شرایطی شکل گرفته است که داده‌ها محدود، فیزیکی و قابل کنترل بودند. اما در عصر دیجیتال، صرف منع مداخله کافی نیست، زیرا داده‌ها به‌طور مداوم تولید و در شبکه‌های پیچیده دیجیتال جابه‌جا می‌شوند و خطرات ناشی از تحلیل و پردازش آن‌ها حتی بدون افشای مستقیم نیز وجود دارد. تمایز اساسی میان امنیت داده‌های شخصی و حریم خصوصی سنتی در همین نقطه آشکار می‌شود، به گونه‌ای که حریم خصوصی بیشتر بر «مرزهای ورود به زندگی شخصی» تأکید دارد، در حالی که امنیت داده‌ها بر «چرخه کامل حیات داده» از تولید تا حذف تمرکز می‌کند. بنابراین، امنیت داده‌ها رویکردی فعال، پیشگیرانه و ساختاری دارد، در حالی که حریم خصوصی سنتی بیشتر واکنشی و محدود به جلوگیری از افشا یا ورود غیرمجاز است. این تحول مفهومی نشان‌دهنده گذار حقوق بشر از حمایت صرف از فضای خصوصی به سمت مدیریت جامع داده‌ها در زیست دیجیتال انسان است.

بند سوم: جایگاه حق بر امنیت داده‌ها در نسل‌بندی حقوق بشر

نسل‌بندی حقوق بشر بر اساس تحولات تاریخی و نیازهای اجتماعی، حقوق بشر را به سه نسل کلاسیک (حقوق مدنی و سیاسی)، حقوق اقتصادی، اجتماعی و فرهنگی، و حقوق همبستگی تقسیم می‌کند. در این چارچوب، حق بر امنیت داده‌های شخصی را می‌توان در امتداد تحول حقوق نسل اول و به‌عنوان بخشی از توسعه مفهومی حق بر حریم خصوصی تحلیل کرد، با این تفاوت که این حق واجد ویژگی‌های نوینی است که آن را به‌عنوان یک «حق نوظهور یا نسل جدید» مطرح می‌سازد. در نسل اول حقوق بشر، تمرکز اصلی بر آزادی‌های فردی و حمایت در برابر مداخله دولت بود و حق بر حریم خصوصی نیز در همین چارچوب شکل گرفت. با این



حال، ظهور فناوری‌های دیجیتال موجب شد که این حق دیگر صرفاً برای حفاظت از خلوت فردی کافی نباشد. در نتیجه، حق بر امنیت داده‌های شخصی به عنوان توسعه‌ای از حریم خصوصی، با هدف پاسخگویی به تهدیدات پیچیده‌تر مانند نظارت دیجیتال گسترده، تحلیل الگوریتمی و اقتصاد داده‌محور مطرح شده است. از منظر تحلیلی، می‌توان گفت حق بر امنیت داده‌ها واجد ویژگی‌هایی است که آن را به حقوق نسل سوم نزدیک می‌کند، از جمله ماهیت فراملی، وابستگی به همکاری دولت‌ها و شرکت‌های فناوری، و ضرورت ایجاد سازوکارهای جمعی برای حمایت از آن. با این حال، برخلاف برخی حقوق همبستگی، این حق مستقیماً با کرامت انسانی و استقلال فردی نیز ارتباط دارد و از این جهت ریشه در نسل اول حقوق بشر دارد. جایگاه حق بر امنیت داده‌های شخصی را می‌توان «میان‌نسلی و تکاملی» دانست، به این معنا که این حق نه کاملاً جدید و مستقل از حقوق پیشین است و نه صرفاً ادامه ساده حریم خصوصی، بلکه مرحله‌ای تکامل یافته از حقوق بشر در عصر دیجیتال محسوب می‌شود که پاسخگوی واقعیت‌های نوین زیست اطلاعاتی انسان معاصر است.

بخش دوم: مبانی حقوقی و اسناد بین‌المللی مرتبط با امنیت داده‌ها

بند اول: اسناد جهانی حقوق بشر و ارتباط آن با داده‌های شخصی

اسناد جهانی حقوق بشر، به‌ویژه اعلامیه جهانی حقوق بشر ۱۹۴۸ و میثاق بین‌المللی حقوق مدنی و سیاسی ۱۹۶۶، بنیان‌های اولیه حمایت از حریم خصوصی و به تبع آن داده‌های شخصی را در نظام حقوق بین‌الملل تثبیت کرده‌اند. ماده ۱۲ اعلامیه جهانی حقوق بشر مقرر می‌دارد که هیچ‌کس نباید در معرض مداخله خودسرانه در زندگی خصوصی، خانواده، منزل یا مکاتبات خود قرار گیرد. این حکم، هرچند در زمان تدوین ناظر به ابزارهای سنتی ارتباطی بوده است، اما از حیث مفهومی ظرفیت آن را دارد که در عصر دیجیتال نیز به عنوان مبنای حمایت از داده‌های شخصی مورد تفسیر گسترده قرار گیرد. در میثاق بین‌المللی حقوق مدنی و سیاسی نیز ماده ۱۷ به صراحت حق هر فرد بر عدم مداخله خودسرانه یا غیرقانونی در زندگی خصوصی،



خانواده، خانه و مکاتبات را تضمین می‌کند. تفسیرهای تفسیری کمیته حقوق بشر سازمان ملل متحد نشان می‌دهد که مفهوم «مکاتبات» در این ماده صرفاً به ارتباطات سنتی محدود نیست، بلکه می‌تواند شامل ارتباطات الکترونیکی، داده‌های دیجیتال و اطلاعات ذخیره‌شده در سامانه‌های رایانه‌ای نیز باشد. این تفسیر پویا زمینه را برای توسعه مفهوم حریم خصوصی به سمت حمایت از داده‌های شخصی فراهم کرده است. با وجود این، باید توجه داشت که اسناد جهانی حقوق بشر به‌طور مستقیم به مفهوم «داده‌های شخصی» یا «امنیت داده‌ها» اشاره نکرده‌اند، زیرا این اسناد در دوره‌ای تدوین شده‌اند که فناوری‌های دیجیتال و اقتصاد داده محور هنوز شکل نگرفته بود. در نتیجه، ارتباط میان این اسناد و موضوع داده‌های شخصی، عمدتاً از طریق تفسیر توسعه‌ای و تطبیقی اصول کلی حقوق بشر صورت گرفته است. این امر موجب شده است که حمایت از داده‌های شخصی در سطح جهانی، بیشتر ماهیت ضمنی و تفسیری داشته باشد تا صریح و مستقل. اسناد جهانی حقوق بشر، اگرچه به‌طور مستقیم نظام جامع حمایت از داده‌های شخصی را ایجاد نکرده‌اند، اما با تثبیت اصل حریم خصوصی به‌عنوان یک حق بنیادین، زمینه حقوقی لازم برای شکل‌گیری و توسعه حق بر امنیت داده‌های شخصی را فراهم ساخته‌اند و نقش زیربنایی در تحول این حق در نظام حقوق بین‌الملل ایفا می‌کنند.

بند دوم: مقررات و استانداردهای بین‌المللی حفاظت از داده‌ها (مانند GDPR)

در کنار اسناد عام حقوق بشر، در دهه‌های اخیر نظام‌های منطقه‌ای و ملی پیشرفته‌ای برای تنظیم و حمایت از داده‌های شخصی شکل گرفته‌اند که مهم‌ترین آن‌ها «مقررات عمومی حفاظت از داده‌ها اتحادیه اروپا (GDPR)» است. این مقررات به‌عنوان جامع‌ترین چارچوب حقوقی در حوزه داده‌های شخصی، الگویی اثرگذار در سطح بین‌المللی ایجاد کرده و استانداردهای نوینی را در زمینه جمع‌آوری، پردازش، ذخیره‌سازی و انتقال داده‌ها معرفی نموده است. ویژگی



برجسته GDPR، رویکرد «حقوق محور» آن است که داده‌های شخصی را نه صرفاً یک دارایی اقتصادی، بلکه بخشی از حقوق بنیادین انسان تلقی می‌کند.

GDPR اصول اساسی مهمی مانند مشروعیت، شفافیت، محدودیت هدف، حداقل گرایی داده‌ها، دقت اطلاعات و محدودیت نگهداری را به عنوان مبانی پردازش داده‌ها تثبیت کرده است. همچنین حقوقی نظیر حق دسترسی، حق اصلاح، حق حذف (حق فراموش شدن) و حق انتقال داده‌ها را برای اشخاص به رسمیت شناخته است. این حقوق نشان‌دهنده گذار از حفاظت منفعلانه به سمت توانمندسازی فعال افراد در کنترل داده‌های شخصی خود است. از این منظر، امنیت داده‌های شخصی در GDPR صرفاً یک الزام فنی نیست، بلکه یک تعهد حقوقی چندلایه برای دولت‌ها و شرکت‌های فراملی محسوب می‌شود. تأثیر GDPR فراتر از مرزهای اتحادیه اروپا بوده و به دلیل رویکرد «اثر فرامرزی» آن، بسیاری از کشورها و شرکت‌های بین‌المللی ناگزیر به انطباق با استانداردهای آن شده‌اند. این امر موجب نوعی «استانداردسازی جهانی غیررسمی» در حوزه حفاظت از داده‌ها شده است. در نتیجه، GDPR را می‌توان یکی از مهم‌ترین منابع نرم حقوقی در شکل‌گیری هنجارهای بین‌المللی امنیت داده‌های شخصی دانست، هرچند از نظر حقوق بین‌الملل، ماهیت الزام‌آور جهانی ندارد.

بند سوم: رویه‌ها و هنجارهای نوظهور در حقوق بین‌الملل سایبری

در کنار مقررات منطقه‌ای، در سطح حقوق بین‌الملل نیز مجموعه‌ای از هنجارها، اصول و رویه‌های نوظهور در حال شکل‌گیری است که به طور مستقیم یا غیرمستقیم به امنیت داده‌های شخصی مرتبط هستند. گزارش‌های گروه کارشناسان دولتی سازمان ملل متحد (UN GGE) و گروه کاری باز (OEWG) از مهم‌ترین اسناد در این حوزه محسوب می‌شوند که بر ضرورت رفتار مسئولانه دولت‌ها در فضای سایبری تأکید دارند. این اسناد اگرچه الزام‌آور نیستند، اما نقش مهمی در شکل‌دهی به انتظارات رفتاری دولت‌ها و ایجاد هنجارهای اولیه در حوزه سایبر ایفا کرده‌اند. در کنار این اسناد، راهنمای تالین نیز به عنوان یک منبع دکترینال مهم،



تلاش کرده است قواعد موجود حقوق بین‌الملل را بر عملیات سایبری اعمال‌پذیر سازد. هرچند این سند از نظر حقوقی الزام‌آور نیست، اما در تفسیر اصولی مانند حاکمیت، عدم مداخله و مسئولیت دولت‌ها نقش مهمی داشته و به‌طور غیرمستقیم بر تحلیل امنیت داده‌های شخصی در بستر حملات سایبری و نقض‌های فرامرزی تأثیر گذاشته است. در سال‌های اخیر شاهد شکل‌گیری تدریجی «هنجارهای رفتاری دولت‌ها در فضای سایبری» هستیم که بر مبنای همکاری بین‌المللی، اعتمادسازی و حفاظت از زیرساخت‌های حیاتی و اطلاعات حساس شکل گرفته‌اند. این هنجارها، هرچند هنوز به سطح عرف بین‌المللی الزام‌آور نرسیده‌اند، اما نشان‌دهنده حرکت نظام حقوق بین‌الملل به سمت پذیرش تدریجی ضرورت تنظیم‌گری در حوزه داده‌ها و امنیت اطلاعات هستند. در مجموع، این روندها بیانگر شکل‌گیری یک رژیم حقوقی در حال تکوین است که می‌تواند در آینده مبنای شناسایی رسمی‌تر حق بر امنیت داده‌های شخصی قرار گیرد.

بخش سوم: چالش‌ها و چشم‌انداز آینده حق بر امنیت داده‌های شخصی

بند اول: تهدیدهای نوین علیه امنیت داده‌ها (هوش مصنوعی، کلان‌داده، هک)

در عصر دیجیتال، امنیت داده‌های شخصی با مجموعه‌ای از تهدیدهای پیچیده، چندلایه و به‌سرعت در حال تحول مواجه است که ماهیت آن‌ها با تهدیدات سنتی کاملاً متفاوت است. یکی از مهم‌ترین این تهدیدها، توسعه و به‌کارگیری گسترده فناوری‌های هوش مصنوعی است. سیستم‌های مبتنی بر هوش مصنوعی قادرند حجم عظیمی از داده‌های شخصی را در مدت زمان کوتاه تحلیل کرده و الگوهای رفتاری، ترجیحات فردی و حتی ویژگی‌های حساس روانی و اجتماعی افراد را استخراج کنند. این سطح از تحلیل، اگرچه در بهبود خدمات و تصمیم‌گیری‌ها مؤثر است، اما در صورت نبود چارچوب‌های حقوقی مناسب می‌تواند به نقض جدی حریم اطلاعاتی و کاهش کنترل افراد بر داده‌های خود منجر شود. تهدید دوم، گسترش کلان‌داده‌ها (Big Data) و اقتصاد مبتنی بر داده است. در این نظام، داده‌های شخصی



به عنوان یک منبع اقتصادی ارزشمند تلقی می‌شوند که توسط شرکت‌های فناوری، پلتفرم‌های دیجیتال و حتی دولت‌ها جمع‌آوری، ذخیره و پردازش می‌گردند. مسئله اصلی در این حوزه، نه صرف جمع‌آوری داده‌ها، بلکه ترکیب و تحلیل آن‌ها از منابع مختلف است که می‌تواند پروفایل‌های بسیار دقیقی از افراد ایجاد کند. این امر، خطر نقض امنیت داده‌ها را از سطح فردی به سطح ساختاری ارتقا داده و امکان نظارت گسترده و پنهان بر رفتار شهروندان را فراهم می‌سازد. در کنار این دو، تهدیدهای سایبری مانند هک، نفوذ غیرمجاز و حملات سازمان‌یافته سایبری نیز همچنان یکی از جدی‌ترین چالش‌ها برای امنیت داده‌های شخصی محسوب می‌شوند. حملات سایبری می‌توانند منجر به سرقت اطلاعات حساس، افشای داده‌های مالی و هویتی و حتی اختلال در زیرساخت‌های حیاتی اطلاعاتی شوند. ویژگی مهم این تهدیدات، فرامرزی بودن، ناشناس بودن عاملان و دشواری انتساب آن‌ها به اشخاص یا دولت‌های مشخص است که موجب پیچیدگی مضاعف در اعمال مسئولیت حقوقی می‌شود. در مجموع، این تهدیدهای نوین نشان می‌دهند که امنیت داده‌های شخصی دیگر صرفاً یک مسئله فنی یا اداری نیست، بلکه به یک مسئله بنیادین حقوق بشری و امنیتی تبدیل شده است که نیازمند پاسخ‌های جامع، چندسطحی و هماهنگ در سطح ملی و بین‌المللی است.

بند دوم: چالش‌های حاکمیتی و تعارض قوانین ملی در فضای دیجیتال

یکی از مهم‌ترین چالش‌های پیش‌روی حق بر امنیت داده‌های شخصی، مسئله حاکمیت دولت‌ها در فضای دیجیتال و تعارض قوانین ملی در این حوزه است. فضای سایبری ذاتاً فرامرزی است و داده‌های شخصی بدون محدودیت جغرافیایی میان سرورها، پلتفرم‌ها و کشورها در جریان هستند. این ویژگی باعث می‌شود که یک داده شخصی هم‌زمان تحت شمول چند نظام حقوقی مختلف قرار گیرد، امری که به تعارض قوانین و عدم انسجام در حمایت حقوقی از داده‌ها منجر می‌شود. در بسیاری از موارد، کشورها رویکردهای متفاوتی نسبت به میزان حفاظت از داده‌ها اتخاذ می‌کنند. برخی نظام‌های حقوقی مانند اتحادیه اروپا



رویکردی سخت‌گیرانه و حقوق‌محور دارند، در حالی که برخی دیگر رویکردی اقتصادی‌تر و مبتنی بر تسهیل جریان داده‌ها را دنبال می‌کنند. این تفاوت‌ها موجب ایجاد «شکاف تنظیم‌گری (Regulatory Gap)» شده و زمینه سوءاستفاده شرکت‌های فراملی از خلأهای حقوقی را فراهم می‌سازد. در نتیجه، داده‌های افراد ممکن است در انتقال میان حوزه‌های قضایی مختلف، از سطح حمایت قوی به سطح حمایت ضعیف‌تر منتقل شوند. افزون بر این، مسئله «حاکمیت داده (Data Sovereignty)» نیز به یکی از موضوعات چالش‌برانگیز تبدیل شده است. دولت‌ها تلاش می‌کنند کنترل بیشتری بر داده‌های تولیدشده در قلمرو خود اعمال کنند، اما این رویکرد در تعارض با ماهیت جهانی اینترنت و فعالیت شرکت‌های چندملیتی قرار می‌گیرد. این وضعیت نه تنها هماهنگی حقوقی را دشوار می‌سازد، بلکه اجرای مؤثر استانداردهای امنیت داده را نیز با چالش مواجه می‌کند و ضرورت همکاری بین‌المللی را بیش از پیش آشکار می‌سازد.

بند سوم: ضرورت شناسایی حق بر امنیت داده‌ها به عنوان حق بنیادین بشر در نظام حقوق بین‌الملل

با توجه به تحولات فناوری و افزایش تهدیدهای نوین، شناسایی حق بر امنیت داده‌های شخصی به عنوان یک حق بنیادین در نظام حقوق بین‌الملل ضرورتی اجتناب‌ناپذیر به نظر می‌رسد. این حق دیگر صرفاً یک موضوع فنی یا اداری نیست، بلکه مستقیماً با کرامت انسانی، آزادی فردی و امنیت روانی افراد در ارتباط است. در واقع، داده‌های شخصی بازتابی از هویت دیجیتال انسان‌ها هستند و نقض آن‌ها می‌تواند آثار عمیق و پایدار بر حقوق بنیادین افراد داشته باشد. در نظام حقوق بین‌الملل معاصر، اگرچه حمایت‌هایی پراکنده از حریم خصوصی و داده‌ها وجود دارد، اما هنوز یک چارچوب جامع، الزام‌آور و یکپارچه برای امنیت داده‌ها شکل نگرفته است. این خلأ حقوقی موجب شده است که سطح حمایت از داده‌های شخصی در کشورهای مختلف بسیار ناهمگون باشد و در بسیاری از موارد، افراد در برابر سوءاستفاده‌های فرامرزی فاقد حمایت مؤثر باشند. بنابراین، شناسایی صریح این حق می‌تواند به همسان‌سازی استانداردها



و تقویت حمایت بین‌المللی از افراد کمک کند. پذیرش حق بر امنیت داده‌ها به عنوان یک حق بنیادین بشر می‌تواند زمینه‌ساز توسعه هنجارهای الزام‌آور بین‌المللی، تقویت همکاری دولتها و ایجاد سازوکارهای نظارتی مؤثر در فضای دیجیتال باشد. چنین رویکردی نه تنها به ارتقای امنیت فردی و اجتماعی کمک می‌کند، بلکه به تثبیت نظم حقوقی پایدار در فضای سایبری جهانی نیز منجر خواهد شد. در نتیجه، آینده حقوق بشر ناگزیر به سمت به رسمیت شناختن امنیت داده‌ها به عنوان یکی از ارکان اصلی حمایت از انسان در عصر دیجیتال حرکت می‌کند.

نتیجه‌گیری

تحلیل حق بر امنیت داده‌های شخصی در پرتو تحولات معاصر نظام حقوق بین‌الملل نشان می‌دهد که این حق در نقطه تلاقی میان حقوق بشر سنتی، تحولات فناوری و الزامات نوین حکمرانی دیجیتال در حال شکل‌گیری و تثبیت است. یافته‌های این پژوهش بیانگر آن است که اگرچه اسناد کلاسیک حقوق بشر همچون اعلامیه جهانی حقوق بشر ۱۹۴۸ و میثاق بین‌المللی حقوق مدنی و سیاسی ۱۹۶۶ به طور صریح به مفهوم «امنیت داده‌های شخصی» اشاره نکرده‌اند، اما از طریق توسعه تفسیری حق بر حریم خصوصی، بستر حقوقی لازم برای شناسایی این حق فراهم شده است. در واقع، حق بر امنیت داده‌ها را می‌توان ادامه منطقی و تکامل یافته حق بر حریم خصوصی در عصر دیجیتال دانست که از سطح «حمایت از خلوت فردی» به سطح «حاکمیت فرد بر داده‌های خود» ارتقا یافته است. بررسی مقررات نوین به ویژه مقررات عمومی حفاظت از داده‌ها (GDPR) نشان می‌دهد که نظام‌های حقوقی منطقه‌ای توانسته‌اند این حق را از سطح یک مفهوم انتزاعی به یک نظام حقوقی عملیاتی، ساختارمند و الزام‌آور تبدیل کنند. اصول بنیادینی همچون مشروعیت پردازش، حداقل‌گرایی داده، شفافیت، امنیت پردازش و حقوق فردی داده‌محور، نشان‌دهنده گذار از رویکرد سنتی حریم خصوصی به رویکرد حکمرانی داده‌ها هستند. با این حال، پراکندگی نظام‌های حقوقی ملی و فقدان یک رژیم جامع بین‌المللی موجب شده است که حمایت از این حق در سطح جهانی با ناهمگونی و عدم انسجام



مواجه باشد. یافته‌های پژوهش همچنین نشان می‌دهد که تهدیدهای نوین از جمله هوش مصنوعی، کلان‌داده‌ها و حملات سایبری، ماهیت نقض داده‌های شخصی را از سطح فردی و موردی به سطح ساختاری، شبکه‌ای و فرامرزی ارتقا داده‌اند. این تحول موجب شده است که ابزارهای سنتی حقوق بین‌الملل برای پاسخ‌گویی به این چالش‌ها ناکافی باشند و نیاز به بازتعریف مفاهیم بنیادین همچون حاکمیت، مسئولیت و انتساب در فضای سایبری بیش از پیش احساس شود. در این میان، نقش شرکت‌های فراملی فناوری اطلاعات به‌عنوان بازیگران غیر دولتی، پیچیدگی مضاعفی در نظام حمایت از داده‌ها ایجاد کرده است. حق بر امنیت داده‌های شخصی در حال گذار از مرحله «حق نوظهور تفسیری» به مرحله «حق بنیادین مستقل» در نظام حقوق بین‌الملل است. تحقق این گذار مستلزم سه تحول اساسی است: نخست، توسعه هنجارهای الزام‌آور بین‌المللی، دوم، همگرایی نظام‌های حقوقی ملی در قالب استانداردهای مشترک، و سوم، تقویت سازوکارهای نظارتی و اجرایی در سطح جهانی. بدون این تحولات، شکاف میان پیشرفت فناوری و ظرفیت حقوق بین‌الملل در حمایت از کرامت انسانی در فضای دیجیتال روزبه‌روز افزایش خواهد یافت. بنابراین، آینده حقوق بشر به‌طور مستقیم به توانایی نظام حقوق بین‌الملل در به‌رسمیت شناختن و تضمین مؤثر حق بر امنیت داده‌های شخصی گره خورده است.

پیشنهادهای

۱. تدوین یک سند بین‌المللی جامع و الزام‌آور در حوزه حفاظت و امنیت داده‌های شخصی با الهام از الگوهایی مانند GDPR، به‌منظور ایجاد وحدت رویه در سطح جهانی.
۲. شناسایی صریح حق بر امنیت داده‌های شخصی به‌عنوان یک حق مستقل در اسناد حقوق بشری بین‌المللی و الحاق آن به میثاق‌های موجود یا تصویب پروتکل‌های الحاقی جدید.



۳. تقویت همکاری‌های بین‌المللی میان دولت‌ها در حوزه مقابله با جرایم سایبری و حملات فرامرزی با تأکید بر سازوکارهای مشترک انتساب و پاسخ‌گویی .
۴. ایجاد استانداردهای جهانی حداقلی برای شرکت‌های فناوری و پلتفرم‌های دیجیتال در زمینه جمع‌آوری، پردازش و ذخیره‌سازی داده‌های شخصی .
۵. توسعه نظام‌های نظارتی مستقل در سطح ملی و منطقه‌ای برای تضمین اجرای مؤثر مقررات حفاظت از داده‌ها و افزایش شفافیت در عملکرد نهادهای دولتی و خصوصی .



منابع و مآخذ

۱. کاتوزیان، ناصر. حقوق مدنی: وقایع حقوقی. تهران: شرکت سهامی انتشار.
۲. صفایی، سید حسین. حقوق مدنی (جلد مربوط به اشخاص و حمایت از شخصیت). تهران: نشر میزان.
۳. امامی، سید حسن. حقوق مدنی. تهران: انتشارات اسلامیه.
۴. رحیمی، محمد. «حریم خصوصی در حقوق ایران و اسناد بین‌المللی». «فصلنامه حقوقی دادگستری».
۵. شریعت‌پناهی، علی. حقوق ارتباطات و فناوری اطلاعات. تهران: سمت.
۶. ربیعا اسکینی. حقوق تجارت. تهران: سمت.
۷. اردبیلی، محمدعلی. حقوق جزای عمومی. تهران: میزان.
۸. گلدوزیان، ایرج. حقوق جزای عمومی. تهران: دانشگاه تهران.
۹. نجفی ابرندآبادی، علی حسین. «جرائم سایبری و حمایت از داده‌های شخصی». «مجله حقوقی دادگستر».
۱۰. حسینی، سید مهدی. حقوق فناوری اطلاعات. تهران: مجد.
۱۱. صالحی، محمد. «تحلیل حقوقی حریم خصوصی در فضای مجازی». «فصلنامه مطالعات حقوقی».
۱۲. قاضی‌زاده، سید علی. حقوق بشر در اسناد بین‌المللی. تهران: سمت.
۱۳. مهرپور، حسین. حقوق بشر و آزادی‌های اساسی. تهران: اطلاعات.
۱۴. زارعی، علی. «حفاظت از داده‌های شخصی در حقوق ایران». «مجله حقوقی بین‌المللی».
۱۵. کریمی، رضا. «جرائم رایانه‌ای در حقوق ایران». تهران: میزان.
۱۶. محسنی، عباس. «مسئولیت مدنی و کیفری در فضای سایبر». «فصلنامه حقوق خصوصی».



۱۷. جعفری لنگرودی، محمدجعفر. ترمینولوژی حقوق. تهران: گنج دانش.

۱. European Union. *General Data Protection Regulation (GDPR), Regulation (EU) ۲۰۱۶/۶۷۹*.
۲. United Nations. *Universal Declaration of Human Rights (۱۹۴۸)*.
۳. United Nations. *International Covenant on Civil and Political Rights (۱۹۶۶)*.
۴. Council of Europe. *Convention ۱۰۸+: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*.
۵. Solove, Daniel J. *Understanding Privacy*. Harvard University Press.
۶. Bygrave, Lee A. *Data Privacy Law: An International Perspective*. Oxford University Press.
۷. Kuner, Christopher. *Transborder Data Flows and Data Privacy Law*. Oxford University Press.
۸. Tallinn Manual ۲.۰ on the International Law Applicable to Cyber Operations. Cambridge University Press.