



مقاله پژوهشی، دوره ۱، شماره ۲، پاییز و زمستان ۱۴۰۳، صفحات ۲۵۷ تا ۲۷۳
تاریخ دریافت: ۱۴۰۲/۰۲/۱۴ تاریخ پذیرش: ۱۴۰۳/۱۰/۱۵
DOI: 10.22106/PR.2025.2035494.1027 : شناسه دیجیتال (DOI)

نقض حق شخصیت اشخاص ثالث در شبکه‌های اجتماعی

محدثه قوامی پور سرشکه*، امیررضا محمودی**

چکیده

این پژوهش به بررسی جامع پدیده نقض حقوق شخصیت اشخاص ثالث در بستر رسانه‌های اجتماعی می‌پردازد. هدف اصلی، ارائه تحلیلی نظام‌مند از ماهیت و کارکردهای رسانه‌های اجتماعی، بررسی سازوکارهای نقض حقوق شخصیت، و ارزیابی پیامدهای حقوقی و اخلاقی این پدیده است. با استفاده از روش‌شناسی توصیفی-تحلیلی و رویکرد استقرایی، منابع کتابخانه‌ای، مقالات علمی-پژوهشی و اسناد حقوقی مرتبط مورد بررسی قرار گرفته‌اند. تجزیه و تحلیل داده‌ها با تکنیک‌های کدگذاری و تحلیل محتوای کیفی انجام شده است. نتایج نشان می‌دهد نقض حقوق شخصیت عمدتاً ناشی از کاستی‌های ساختاری در امنیت سکوها (پلتفرم‌ها) و اقدامات عامدانه کاربران با انگیزه‌های مجرمانه است. این مطالعه انواع نقض حقوق شخصیت را در چهار دسته طبقه‌بندی می‌کند: افشای غیرمجاز اطلاعات خصوصی، هتک حرمت، نشر اطلاعات کذب، و سوءاستفاده از هویت دیجیتال. پژوهش حاضر با تحلیل تعارضات میان حق آزادی بیان و حریم خصوصی، چالش‌های حقوقی و اخلاقی را برجسته می‌سازد. راهکارهای پیشنهادی شامل تدوین چارچوب‌های قانونی جامع، ارتقای سواد دیجیتال، توسعه فناوری‌های حفاظتی، و تقویت مسئولیت‌پذیری سکوهاست. یافته‌های این پژوهش می‌تواند مبنایی برای سیاست‌گذاری در حوزه حکمرانی دیجیتال و حقوق سایبری باشد و زمینه‌های جدیدی را برای مطالعات میان‌رشته‌ای در حقوق، فناوری اطلاعات و علوم اجتماعی پیشنهاد می‌کند. علاوه بر این، مطالعه حاضر به بررسی تأثیر فزاینده هوش مصنوعی و الگوریتم‌های یادگیری

* دانشجوی دکتری حقوق جزا و جرم‌شناسی، گروه حقوق، واحد لاهیجان، دانشگاه آزاد اسلامی، لاهیجان، ایران،
(نویسنده مسئول). mohadesheghavamipour@gmail.com

** استادیار گروه حقوق، واحد لاهیجان، دانشگاه آزاد اسلامی، لاهیجان، ایران. amirreza.mahmodi@gmail.com

ماشین بر حفظ حریم خصوصی و حقوق شخصیت در فضای مجازی می‌پردازد. همچنین، این پژوهش به ارزیابی نقش تنظیم‌کننده‌های ملی و بین‌المللی در تنظیم مقررات مربوط به حفاظت از داده‌های شخصی در رسانه‌های اجتماعی اختصاص یافته است. درنهایت، این مطالعه پیشنهادهایی برای ایجاد تعادل بین نوآوری تکنولوژیک و حفاظت از حقوق کاربران در عصر دیجیتال ارائه می‌دهد.

واژگان کلیدی: رسانه‌های اجتماعی، حقوق شخصیت، نقض حقوق اشخاص ثالث، تولید محتوا، جرائم سایبری.

مقدمه

به لطف زیرساخت رایانه و ارتباطات الکترونیکی، یک جو ارتباطی جدید و مصنوعی متشکل از لینک‌های رادیویی، اتصالات ماهواره‌ای و شبکه‌های کابلی که کل دنیا را احاطه کرده است، شکل گرفته است. این جو مصنوعی که «رسانه‌های اجتماعی» نامیده می‌شود، مانند یک یکپارچه و فراگیر جهانی، از یک مکان به مکان دیگر، به لطف فناوری‌های جدید ارتباطی، به‌طور مداوم اطلاعات / داده‌های صوتی، تصویری و نوشتاری را منتقل می‌کند. (Vural & Bat, 2010, 3350)

به موازات این پیشرفت، در حالی که تحقیقات فناورانه مربوط به زیرساخت سیستم و جستجوهای جدید شتاب گرفته است، در کنار بعد فناورانه این موضوع، روابط، ارتباطات و الگوهای رفتاری کاربران که هم مصرف‌کننده و هم تولیدکننده این محیط هستند نیز زیر ذره‌بین قرار گرفته‌اند. حرکات اساسی، گرانش‌ها، پویایی‌ها، اشتراک‌گذاری، تعامل و شیوه‌های ارتباطی کاربران در محیط رسانه‌های اجتماعی، روزبه‌روز موضوع بررسی حوزه‌هایی نظیر رسانه، روابط عمومی، ارتباطات، بازاریابی، تبلیغات، سیاست، روان‌شناسی، آموزش، جامعه‌شناسی و همچنین حقوق شده است. (انصاری، ۱۳۹۲: ۴۴)

تعریف واحد برای رسانه‌های اجتماعی وجود ندارد و درواقع هر تعریفی این پدیده را از زاویه دیگری توضیح می‌دهد. معمولاً متخصصانی که جنبه‌های ارتباطی، رسانه‌ای و بازاریابی موضوع را بررسی می‌کنند، تعاریف متفاوتی ارائه می‌دهند. برخی رسانه‌های اجتماعی را «گروهی از برنامه‌های اینترنتی مبتنی بر ساختارهای ایدئولوژیک و فناورانه وب که به تولید و تغییرات منبع کاربر اجازه می‌دهند» تعریف کرده‌اند. (Kaplan & Haenlein, 2010, 61) برخی دیگر آن را «خدمات وب‌محور که به افراد اجازه می‌دهند در یک سیستم محدود، نمایه‌های عمومی یا نیمه‌عمومی ایجاد کنند، فهرست اتصالات خود را با دیگر کاربرانی که با آن‌ها به اشتراک گذاشته‌اند اضافه کنند، و اتصالات دیگران در سیستم را مشاهده و بازدید کنند» تعریف کرده‌اند. (Boyd & Ellison, 2008, 211)

برخی رسانه‌های اجتماعی را «محیط اجتماعی که کاربران را به برقراری ارتباط با دیگر کاربرانی که سایت خود یا محیط مشابه را ایجاد کرده‌اند ترغیب می‌کند و به کاربران محیطی را برای به اشتراک‌گذاشتن محتوا یا برقراری ارتباط سوق می‌دهد» توصیف کرده‌اند. (Brunty & Helenek, 2013, 2) در تعریفی دیگر، رسانه‌های اجتماعی به «برنامه‌های تلفن همراه و وب‌محور که برای اشتراک‌گذاری، خلق مشترک، تغییر و بحث در مورد محتوای منبع کاربر از طریق افراد و جوامع با ایجاد سکوها تعاملی استفاده می‌شوند» اشاره دارد. (Kietzmann et al., 2011, 241)

برخی نیز در معنای گسترده، رسانه‌های اجتماعی را «وب‌سایت‌هایی که برپایه فناوری‌های وب بنا

شده‌اند و امکان تعامل اجتماعی عمیق‌تر، ایجاد جامعه و دستیابی به پروژه‌های همکاری را فراهم می‌کنند» تعریف می‌کند. (Akar, 2010, p. 17)

در کنار این تعاریفات برخی دیگر از صاحب‌نظران و علمای فن نیز مفهوم رسانه‌های اجتماعی را به‌عنوان یک مفهوم چتری در نظر می‌گیرند و می‌گویند که زیر این مفهوم، کاربردهای فرهنگی گوناگون و متفاوت برخط مرتبط با محتوا و افرادی که با محتوا به سیستم می‌پیوندند، وجود دارد. (Lietsala & Sirkkunen, 2008, 17-18)

به نظر می‌رسد رسانه‌های اجتماعی، محیط و ابزارهایی هستند که برپایه زیرساخت اینترنت و فناوری وب استوار بوده و امکان اجتماعی‌شدن افراد را از طریق تعامل، ارتباط، اشتراک‌گذاری، همکاری، ایجاد جامعه و خلق محتوای شخصی در زمینه علایق، دانش، احساسات و اندیشه‌های مشترک فراهم می‌آورند.

۱. حق بر شخصیت

حق بر شخصیت یکی از حقوق بنیادین و غیرمالی انسان است که به‌عنوان یک اصل محوری در نظام‌های حقوقی و اخلاقی شناخته می‌شود. این حق بر پایه احترام به کرامت انسانی، آزادی‌های فردی، و حفاظت از ارزش‌های ذاتی و اجتماعی هر فرد استوار است. حقوق شخصیت درواقع مجموعه‌ای از حقوق است که به تمامیت وجودی، عاطفی، اجتماعی و فرهنگی افراد تعلق دارد و به حمایت از ویژگی‌های غیرقابل تفکیک از شخصیت انسانی می‌پردازد.

۱-۱. ابعاد اصلی حق بر شخصیت

۱. کرامت انسانی

حق بر شخصیت براساس اصل کرامت انسانی استوار است. این اصل بر این نکته تأکید دارد که هر انسان، صرف‌نظر از جنسیت، ملیت، مذهب، سن یا وضعیت اجتماعی، از حقوق ذاتی برخوردار است که باید محترم شمرده شود. این کرامت انسانی پایه‌ای برای تعریف و حمایت از حق شخصیت به شمار می‌رود.

۲. آزادی‌های فردی

حق بر شخصیت تضمین‌کننده آزادی‌های بنیادین فرد در حوزه‌های مختلف زندگی است. این آزادی‌ها شامل حق تصمیم‌گیری آزادانه در زمینه‌های شخصی و اجتماعی، حفاظت از استقلال فردی، و دفاع از حق انتخاب در مقابل دخالت‌های خارجی است.

۳. حریم خصوصی و داده‌های شخصی

یکی از عناصر مهم حق بر شخصیت، حفاظت از حریم خصوصی و داده‌های شخصی است. این موضوع شامل حفظ اطلاعات حساس، اسرار شخصی، و جلوگیری از افشای بدون اجازه آن‌ها

می‌شود. حریم خصوصی یکی از پایه‌های اصلی برای تحقق امنیت و احترام به شخصیت افراد است.

۴. حقوق غیرمالی و طبیعی:

حقوق شخصیت ازجمله حقوق غیرمالی محسوب می‌شوند که به‌واسطه ماهیت انسانی فرد ایجاد می‌شوند، نه دارایی‌ها یا منافع مادی. این حقوق، برخلاف حقوق مالی، قابلیت انتقال، واگذاری یا صرف‌نظرکردن را ندارند و همواره به شخصیت انسانی وابسته باقی می‌مانند. (مظهر قراملکی، قدرتی، نظری توکلی، ۱۳۹۵، ۲۸۱)

۱-۲. ویژگی‌های حقوق شخصیت

- غیرقابل انتقال‌بودن: این حقوق را نمی‌توان به دیگران منتقل کرد یا از آن‌ها صرف‌نظر کرد.
- ارتباط مستقیم با ذات انسان: حقوق شخصیت بخشی از وجود انسان است و از او جدا نمی‌شود.
- عدم شمول مرور زمان: این حقوق با گذشت زمان از بین نمی‌روند و همواره قابل اجرا و مطالبه هستند.
- محدودیت‌ناپذیری: هیچ‌کس نمی‌تواند این حقوق را حتی به اراده خود از بین ببرد یا اسقاط کند.

۱-۲. گستره حق بر شخصیت

حق بر شخصیت شامل تمامی ابعاد وجودی انسان است:

۱. ارزش‌های جسمانی: شامل حق بر حیات، سلامتی، و تمامیت جسمی.
 ۲. ارزش‌های عاطفی: مانند احترام به احساسات و ارتباطات خانوادگی.
 ۳. ارزش‌های اجتماعی: شامل اعتبار اجتماعی، شرافت، آزادی، و حیثیت.
- حق بر شخصیت نه تنها به فرد این امکان را می‌دهد که به‌عنوان یک موجود مستقل در جامعه شناخته شود، بلکه تضمین‌کننده تعامل سالم اجتماعی و جلوگیری از سوءاستفاده یا تعرض به ارزش‌ها و ویژگی‌های انسانی اوست. در محیط‌های مدرن، به‌ویژه در فضای مجازی، این حق اهمیت دوچندان یافته است. (پورسید، فرحزادی، حیدری هرستانی، ۱۴۰۳، ۴)

۲. ویژگی‌های حق شخصیت

ویژگی‌هایی که حق شخصیت را از سایر حقوق متمایز می‌کند عبارتند از: مطلق‌بودن حق شخصیت، مربوط به وجود شخص‌بودن آن، قابل‌انتقال به دیگری‌نبودن، مشمول مرور زمان‌نشدن، غیرقابل اسقاط‌بودن، وارد تصفیه امور ورشکستگی‌نشدن، فقط توسط صاحب حق قابلیت استفاده داشتن. شخص نمی‌تواند در مورد آن تصرف کند یا آن را منتقل کند، نمی‌تواند از آن صرف‌نظر کند و قاعدتاً به وارثان منتقل نمی‌شود. (Oğuzman/Seliçi/Oktay-Özdemir, 2012, 156)

تقسیم‌بندی ارزش‌های شخصیتی به ارزش‌های فیزیکی (مادی) شخصیت، ارزش‌های عاطفی شخصیت و ارزش‌های اجتماعی شخصیت، یک طبقه‌بندی پذیرفته‌شده در آموزه‌ها است. (Fren, 2012, 797)

براین اساس، حیات، تمامیت جسمی، حق سلامتی، تمامیت روانی شخص، ارزش‌های فیزیکی شخصیت را تشکیل می‌دهند. حق احترام به روابط شخص با افرادی که در جامعه با آن‌ها زندگی می‌کند و یکپارچگی خانوادگی، از ارزش‌های عاطفی شخصیت هستند. آنچه که روابط شخص را با دیگر اعضای جامعه توسعه و حفظ می‌کند، مانند شرافت و حیثیت، حریم خصوصی و آزادی‌ها، ارزش‌های اجتماعی شخصیت را تشکیل می‌دهند. (Kılıçoğlu, 2013, 6) در کل رویه قضایی نیز دیدگاه مشابهی را پذیرفته و معتقد است که حقوق شخصیت حقوقی هستند که زندگی، سلامت، تمامیت جسمی و روانی، و موقعیت شخص در جامعه را حفظ می‌کنند و شامل ارزش‌های فیزیکی، عاطفی و اجتماعی شخصیت می‌شوند. (خسروی، ۱۳۹۲: ۵۶- محمدزاده، ۱۳۹۶: ۱۰۵)

۳. نقض حق شخصیت در رسانه‌های اجتماعی

نقض حق شخصیت توسط اشخاص ثالث در رسانه‌های اجتماعی بخش مهمی از نقض حقوق شخصیت که در پلتفرم‌های رسانه‌های اجتماعی رخ می‌دهد و توسط اشخاص ثالث غیر از کاربر و ارائه‌دهنده خدمات رسانه‌های اجتماعی انجام می‌شود که یا کاربران دیگر پلتفرم‌های رسانه‌های اجتماعی مربوطه هستند یا اشخاص ثالثی که با گذر از تدابیر امنیتی، به سکو دسترسی پیدا می‌کنند. این نقض‌ها می‌تواند از طریق محتوای اشتراک‌گذاشته‌شده، مسائل امنیتی و جرائم رایانه‌ای رخ دهد.

نقض‌ها ناشی از محتوای اشتراک‌گذاشته‌شده بخش مهمی از محتوای متشکل از عناصری مانند متن، عکس، ویدئو و صدا در پلتفرم‌های رسانه‌های اجتماعی که از فناوری‌های وب استفاده می‌کنند، توسط کاربران ایجاد می‌شود. (رضوی‌فرد، موسوی، ۱۳۹۵: ۳۱) مفهوم محتوا بسته به ماهیت خدمات ارائه‌شده در هر سکوی رسانه‌های اجتماعی می‌تواند متفاوت باشد و با گذشت زمان، موارد جدیدی وابسته به فناوری‌ها به محدوده آن اضافه می‌شود. اما به‌طورکلی، محتوا شامل متن، عکس، ویدئو، کلیپ‌صوتی، نظرات، داده‌ها، اطلاعات، نرم‌افزار، دستورالعمل‌ها، گرافیک‌ها و سایر ویژگی‌های تعاملی است که از طریق خدمات رسانه‌های اجتماعی قابل‌دسترسی می‌شوند. محتوای اشتراک‌گذاشته‌شده، از سوی کاربران سکوی رسانه‌های اجتماعی تولید می‌شود و در سکوی رسانه‌های اجتماعی یا از طریق پیوند به خدمات سکوی رسانه‌های اجتماعی، اضافه، ایجاد، آپلود، ارسال، توزیع، یا از طریق پیوند به سایت‌ها یا خدمات اینترنتی دیگر ارائه می‌شود.

گرچه سکوی رسانه‌های اجتماعی به‌عنوان محیط‌هایی که اطلاعات به راحتی جریان دارد، همه به

اطلاعات دسترسی دارند و افراد می‌توانند آزادانه افکار خود را بیان کنند، معرفی می‌شوند، اما این واقعیت وجود دارد که این آزادی‌ها محدودیت‌های معینی دارند. یکی از این محدودیت‌ها «حقوق آزادی‌های دیگران» است که تجلی آن در حقوق خصوصی، حق شخصیت است. گرچه در قراردادهای استفاده از خدمات رسانه‌های اجتماعی، قواعد و اصول مرتبط با حق شخصیت برای محدودکردن محتوا وضع می‌شود، (عالی‌پور، ۱۳۹۰، ۱۳۹) اما همچنان امکان حمله به ارزش‌های تحت حمایت حق شخصیت مانند شرافت و حیثیت، اعتبار حرفه‌ای و تجاری، اسرار، نام، صدا و تصویر، حریم خصوصی و داده‌های شخصی دیگر کاربران از طریق محتوا وجود دارد.

شکل متداول نقض در سکوها رسانه‌های اجتماعی ناشی از محتوای اشتراک گذاشته‌شده توسط کاربران، دربرداشتن عناصر توهین‌آمیز، تهدیدآمیز یا افترازننده در محتوا و در نتیجه لطمه به شرافت، حیثیت و اعتبار دیگران است. (محسنی، قاسم‌زاده، ۱۳۸۵، ۳۰-۳۵) توهین می‌تواند از طریق ابزارهایی مانند توییت‌ها، پست‌های وبلاگ، نظرات در انجمن‌ها، اشتراک‌گذاری‌های فیسبوک و دیگر ابزارهایی که توسط سایر کاربران این سکوها استفاده می‌شود، با عناصر کتبی، تصویری و شنیداری موهن، آزاردهنده، کوچک‌کننده یا عداوت‌برانگیز صورت گیرد. علاوه‌براین، تمامیت معنوی اشخاص می‌تواند از طریق پیام‌های حاوی محتوای مستهجن یا آزار جنسی نقض شود. در کنار موارد توهین توسط محتوایی که توسط یک کاربر ایجاد شده است، امکان توهین از طریق اشتراک‌گذاری محتوای توهین‌آمیز متعلق به سایر کاربران با استفاده از امکاناتی مانند «ریتوییت» یا «اشتراک‌گذاری» یا ارسال پیوند به چنین انتشاراتی نیز وجود دارد. در این حالت مسئولیت، نه به‌عنوان صاحب محتوای توهین‌آمیز، بلکه به‌عنوان فردی که پیوند به محتوای متعلق به دیگری را ایجاد کرده است، مطرح می‌شود. (رحمدل، ۱۳۸۴: ۷۰) اگرچه قاعده این است که شخص مسئولیتی برای محتوای متعلق به دیگری ندارد، اما اگر از شیوه ارانه مشخص باشد که پیوند داده‌شده به محتوا پذیرفته شده و هدف دسترسی به آن محتوا بوده است، مسئولیت برای محتوای توهین‌آمیز متعلق به دیگری مطرح خواهد شد. در صورتی که محتوای کاربران دیگر در پلتفرم‌های رسانه‌های اجتماعی‌حاوی عنصر تهدید باشد، نیز با توجه به کاهش در دنیای معنوی و ارزش‌های شخصیتی فرد، حق شخصیت نقض خواهد شد. شیوه دیگر حمله به حق شخصیت، ارانه محتوای خلاف واقع و افترازننده است. محتوای مورد استفاده گاهی ممکن است ماهیت گفتار نفرت‌انگیز، تبعیض‌آمیز یا برانگیزاننده دشمنی دیگران را نیز داشته باشد. در تمام این موارد، ارزش‌های شخصیتی و در نتیجه حق شخصیت آسیب می‌بیند.

در پلتفرم‌های رسانه‌های اجتماعی‌همچون اشخاص حقیقی، حملاتی با محتوای توهین‌آمیز و خلاف واقع به اعتبار اشخاص حقوقی مانند شرکت‌ها، سازمان‌ها و نهادها نیز صورت می‌گیرد. به‌ویژه در وبلاگ‌ها،

انجمن‌ها یا بخش‌های نظرات مرتبط با این سکوها که در آن‌ها خدمات این اشخاص حقوقی ارزیابی می‌شود، با اشتراک‌گذاری‌ها می‌توان به ارزش‌های شخصیتی تجاری و حرفه‌ای آن‌ها حمله کرد. در نتیجه این حملات، با آنچه اشتراک گذاشته می‌شود، اعتبار تجاری آن‌ها متزلزل می‌شود، رقابت نامناسبی از طریق سیاه‌نمایی برخی و برجسته‌کردن شخص حقوقی دیگری ایجاد می‌شود، و امکان کاهش ارزش سهام آن‌ها در بورس به دلیل گزارش‌های خلاف واقع و بدنام‌شدن در بازار نیز وجود دارد.

با در نظر گرفتن اینکه اشخاص حقوقی نیز همانند اشخاص حقیقی از حمایت حق شخصیت بهره‌مند هستند، اعتبار آن‌ها تحت احکام مربوط به حق شخصیت محافظت خواهد شد. همچنین در صورتی که این وضعیت منجر به مواردی مانند رقابت نامناسب شود، می‌توان از احکام رقابت نامناسب نیز برای حمایت بهره برد.

محتوای توهین‌آمیز، تهدیدآمیز و افترازننده، علاوه بر اینکه براساس قوانین بسیاری از کشورها موجب مسئولیت کیفری یا حقوقی است، (رضوی‌فرد، موسوی، ۱۳۹۵، ۴۰) در زمره ممنوعیت‌های قوانین استفاده از تمام رسانه‌های اجتماعی نیز قرار دارد. علاوه بر این، گفته شده است که تمام مسئولیت ناشی از این‌گونه اشتراک‌گذاری‌ها متوجه کاربرانی است که محتوا را تأمین می‌کنند و ارائه‌دهندگان خدمات رسانه‌های اجتماعی مسئولیتی در نظارت بر این محتواها ندارند و در نتیجه از نظر کیفری و حقوقی مسئول نخواهند بود.

تشخیص هویت فرد مسئول، یعنی کاربر، در صورت نقض حق شخصیت ناشی از محتوا، همیشه آسان نیست. دلایل این دشواری عدم الزام کاربران به ارائه اطلاعات هویتی واقعی در رسانه‌های اجتماعی، استفاده برخی کاربران از نام‌های مستعار، حساب‌های جعلی یا دسترسی به رسانه‌های اجتماعی از طریق نرم‌افزارهای شخص ثالث است. در چنین مواردی، می‌توان با دستیابی به آی‌پی^۱ کاربران، هویت آن‌ها را تشخیص داد. اگرچه می‌توان اطلاعات هویتی کاربران را از ارائه‌دهندگان خدمات رسانه‌های اجتماعی که اطلاعات پروفایل را ذخیره می‌کنند نیز درخواست کرد، اما واقعیت این است که به جز در موارد جرائم مهم مانند تروریسم، این اطلاعات ارائه نمی‌شود. (حبیبی، ۱۳۹۵، ۶۰)

چگونگی حذف یا مسدودسازی محتوای توهین‌آمیز، تهدیدآمیز یا افترازننده از پلتفرم‌های رسانه‌های اجتماعی یکی از موضوعات مهم است. قبل از هر چیز، اگر این‌گونه محتوا توسط یک کاربر دیگر ایجاد شده باشد، گزینه‌هایی مانند ارتباط درون سکویی با صاحب محتوا و درخواست حذف محتوا، یا رسیدن مستقیم به ارائه‌دهنده خدمات از طریق فرم‌ها یا برنامه‌های مختلف و گزارش نقض

1. IP

ناشی از محتوا و شکایت وجود دارد. با ارائه تنظیمات مربوطه، امکان جلوگیری از برخورد با این کاربر صاحب محتوا در همان سکو و در نتیجه پیشگیری از حملات بعدی نیز وجود دارد. علاوه‌براین‌ها، می‌توان با مراجعه مستقیم به ارائه‌دهنده خدمات رسانه‌های اجتماعی، درخواست حذف محتوای تهاجمی را ارائه داد، اگرچه این موضوع کاملاً به اختیار ارائه‌دهنده خدمات بستگی دارد. بسیاری از ارائه‌دهندگان خدمات بدون حکم دادگاه این محتواها را حذف نمی‌کنند و گاهی حتی با وجود حکم دادگاه نیز ترجیح می‌دهند آن را اجرا نکنند. در دادگاه‌ها نیز می‌توان در مورد این‌گونه محتواها، یا برای متوقف کردن حمله مانند حذف محتوا، یا در صورت وجود شک به تکرار حملات در آینده، برای پیشگیری از حمله، یا در صورت وقوع نقض، برای اعمال تنبیهات حقوقی و کیفری، اقدام قضائی انجام داد. درخصوص درخواست‌های پایان دادن به این‌گونه نقض‌های صورت گرفته در رسانه‌های اجتماعی، می‌توان تصمیماتی مانند حذف محتوا یا مسدودسازی دسترسی را صادر کرد. علاوه‌براین، اگر به دلیل نقضی که رخ داده است جرمی واقع شده یا مسئولیت جبران خسارت ایجاد شده باشد، مسئولیت‌ها و تنبیهات حقوقی و کیفری نیز می‌تواند مطرح شود. (رضوی فرد، موسوی، ۱۳۹۵: ۴۲)

محتوای توهین آمیز، تهدیدآمیز یا افترازننده در رسانه‌های اجتماعی در دادگاه‌ها همانند نقض‌های در دنیای واقعی ارزیابی می‌شود و در صورت شناسایی متهم، با توجه به قوانین و مقررات مربوطه، تنبیهات حقوقی یا کیفری اعمال می‌گردد.

بدون شک، یکی از ارزش‌های شخصیتی که بیشترین تهدید را از سوی رسانه‌های اجتماعی متحمل می‌شود، حریم خصوصی است. در پلتفرم‌های رسانه‌های اجتماعی که براساس «دیدن» طراحی شده‌اند، برای برقراری ارتباط و تعامل با دیگران، ابتدا باید «وجود داشت»، به عبارت دیگر «دیده شد»، که این امر با ایجاد یک پروفایل حاوی برخی داده‌ها و اطلاعات درباره خود شروع می‌شود. در ادامه این رابطه، اشتراک‌گذاری‌هایی مانند اطلاعات، مستندات، نظرات و عکس‌ها درباره خود و زندگی فرد افزایش می‌یابد. علاوه‌براین، این اشتراک‌گذاری‌ها نه تنها توسط خود فرد، بلکه توسط دوستان او نیز می‌تواند انجام شود و تقریباً هیچ حریم خصوصی برای افراد در رسانه‌های اجتماعی باقی نمی‌ماند.

اشتراک‌گذاری عکس‌هایی مانند تصاویر از مکان‌های تفریحی، مهمانی‌ها یا ساحل توسط افراد برای همگان و به دست آوردن این عکس‌ها توسط افراد بدون نظر از طریق هک کردن رمزها، و سپس استفاده آن‌ها در سایت‌هایی مانند سایت‌های پورنو یا برای تبلیغات، می‌تواند منجر به آسیب به افراد شود. (شریعتی، زمانیان، خلیلی، ۱۴۰۰، ۴)

انتشار فیلم، عکس، ویدئو و موارد مشابه مربوط به حریم خصوصی دیگران در پلتفرم‌های رسانه‌های اجتماعی بدون کسب اجازه از آن‌ها، نقض حریم خصوصی محسوب می‌شود. بنابراین قبل از

انتشار چنین محتوایی باید از افراد مربوطه اجازه گرفته شود. اما این رضایت لزوماً هرگونه نقض حریم خصوصی را مشروع نمی‌کند. براساس قوانین موضوعه ایران حق شخصیت حتی در برابر خود فرد نیز محافظت شده است و محدودیت‌های رضایت برای حق شخصیت، قواعد آمره، اخلاق، نظم عمومی و ماهیت این حق می‌باشد.^۱

رسانه‌های اجتماعی همچنین می‌توانند برای انتشار اطلاعات، صدا و تصاویر به‌دست‌آمده از طریق فیلم‌برداری مخفیانه از زندگی خصوصی افراد، و در معرض دید عموم قرار دادن آن‌ها استفاده شوند. جمع‌آوری این‌گونه مواد نقض حریم خصوصی محسوب می‌شود و افشای آن‌ها نیز یک نقض جداگانه است. به‌عبارت‌دیگر، ایجاد مواد مکتوب، تصویری و شنیداری که حریم خصوصی افراد را نقض می‌کند، حتی اگر توسط کاربران پلتفرم‌های رسانه‌های اجتماعی انجام نشود، اما انتشار آن‌ها در این سکوها توسط کاربران، نقض حق شخصیت محسوب می‌شود. در سال‌های اخیر، انتشار تصاویر از روابط خصوصی افرادی مانند سیاستمداران، هنرمندان و ورزشکاران در پلتفرم‌های رسانه‌های اجتماعی یک نمونه کلاسیک از نقض حریم خصوصی است. (شریفی، صفایی، الماسی، ساورایی، ۱۴۰۲، ۸۹) همچنین مشاهده شده که اطلاعات محرمانه و اسناد محافظت‌شده تحت آزادی ارتباطات، مانند تماس‌های تلفنی و ایمیل‌های خصوصی افراد، به‌دست‌آمده و در پلتفرم‌های رسانه‌های اجتماعی منتشر می‌شوند. این موارد نقض حق شخصیت در زمینه حریم خصوصی ارتباطات و حریم داده‌های شخصی افراد محسوب می‌شوند.

شرکت‌های تجاری نیز برای معرفی خود و حضور در دنیای مجازی از پلتفرم‌های رسانه‌های اجتماعی‌مانند وبلاگ‌ها، تویتر و فیسبوک استفاده می‌کنند. بسیاری از شرکت‌ها از این طریق ارتباطات داخلی خود را مدیریت می‌کنند و شرکت‌ها و کارمندان می‌توانند در این محیط‌ها اخبار شرکت، تحولات صنعت، موضوعات روز و دستور کار رسانه‌های اجتماعی را دنبال کنند.

اشتراک‌گذاری‌های کارمندان شرکت در این‌گونه محیط‌های رسانه‌های اجتماعی در مورد زندگی کاری، همکاران و شرکت نیز می‌تواند منجر به نقض حق شخصیت شود. بنابراین در این‌گونه اشتراک‌گذاری‌ها باید از انتشار محتوایی که می‌تواند منجر به نقض حق شخصیت شرکت، مدیریت و کارمندان شود، خودداری کرد. به‌ویژه باید از به اشتراک‌گذاشتن پروژه‌ها، اطلاعات مالی، طراحی‌ها و ارائه‌ها خودداری شود و این نکته را مد نظر داشت که چنین اشتراک‌گذاری‌هایی می‌تواند به افشای اسرار شرکت منجر شود.

۱. هیچ‌کس نمی‌تواند حریت و آزادی را از خود سلب کند همچنان‌که هیچ‌کس نمی‌تواند حریت و آزادی را از خود اسقاط کند، به‌طوری‌که مانند بردگان خود نداشته باشد. کسی نمی‌تواند حقوق کلی مدنی و حق کلی اجرای حقوق مدنی را از خود سلب کند.

الف. نقض‌ها به دلیل مشکلات امنیتی

اگرچه ارائه‌دهندگان خدمات رسانه‌های اجتماعی در وبسایت‌ها و شرایط استفاده خود اظهار می‌کنند که اقدامات امنیتی کافی و لازم را برای استفاده ایمن از سکوها رسانه‌های اجتماعی اتخاذ کرده‌اند، اما واقعیت این است که حتی رایج‌ترین سکوها رسانه‌های اجتماعی نیز هک شده‌اند و اطلاعات کاربران به سرقت رفته یا از طریق فناوری اطلاعات، جرائم رایانه‌ای متعددی در این سایت‌ها رخ داده است. مشکلات امنیتی در سکوها رسانه‌های اجتماعی ناشی از عدم رعایت قوانین استفاده توسط کاربران یا نقاط ضعف و کمبودهای امنیتی در سیستم است. افرادی که از این مشکلات سوءاستفاده می‌کنند و حق شخصیت کاربران را نقض می‌کنند، می‌توانند کاربران دیگر یا مجرمان رایانه‌ای با نیت بد باشند.

داده‌های شخصی از مهم‌ترین ارزش‌های شخصیتی هستند که به دلیل کمبود اقدامات حفاظتی شخصی یا نقاط ضعف امنیتی در سکوها رسانه‌های اجتماعی، در معرض حمله قرار می‌گیرند. سکوها رسانه‌های اجتماعی محیط‌هایی هستند که در آن‌ها داده‌های شخصی، اطلاعات پروفایل و رمزهای عبور کاربران به راحتی می‌تواند به دست دیگران بیفتد. این امر تا حد زیادی ناشی از این واقعیت است که عضویت در سکوها رسانه‌های اجتماعی، یا به عبارت دیگر «وجود» در آن‌ها، مستلزم ارائه برخی اطلاعات است و این سکوها محیط‌هایی برای به اشتراک‌گذاری داده‌ها، اطلاعات و ارتباطات افراد هستند. داده‌ها و اطلاعات شخصی در سکوها رسانه‌های اجتماعی از طریق انواع حیل‌ها، روش‌های فنی یا ترکیبی از هر دو به دست می‌آیند. در این زمینه، اطلاعات موجود در سکو می‌تواند بدون اطلاع کاربر و از طریق فناوری اطلاعات به دست آید، یا حتی اطلاعاتی که به این شیوه قابل دسترسی نیستند، با رفتارهای متقلبانه و تضعیف اراده کاربر، توسط خود وی ارائه شوند. (Kaya, 2015, 297).

در دنیای امروز که حتی وبسایت سکوها رسانه‌های اجتماعی نیز می‌توانند جعلی باشند، این سایت‌های جعلی از کاربران درخواست می‌کنند تا اطلاعات، حساب‌ها و رمزهای عبور خود را وارد کنند و با این ترفند که کاربر در حال ورود به سکو است، این اطلاعات را به راحتی به دست می‌آورند. یک روش دیگر برای به دست آوردن اطلاعات و داده‌های کاربران از طریق حیل، ارسال پیام‌هایی از سوی سکوی رسانه‌های اجتماعی مبنی بر برنده شدن جایزه، هدیه یا قرعه‌کشی است که از کاربران خواسته می‌شود فرم‌هایی حاوی اطلاعات شخصی را پر کنند یا درخواست‌های مشابهی را ارسال کنند. حساب‌های جعلی که به نام کاربران در سکوها رسانه‌های اجتماعی ایجاد می‌شوند نیز رایج هستند و این اقدامات امنیت داده‌ها و اطلاعات شخصی را نقض می‌کنند؛ زیرا در این حساب‌ها برای جلب اعتماد، از عناصری مانند اطلاعات هویتی واقعی یا عکس فرد استفاده می‌شود. در این

حساب‌های جعلی، اطلاعات شخصی بدون رضایت فرد منتشر می‌شود که این امر جرم افشا یا به‌دست‌آوردن داده‌های شخصی محسوب می‌شود و ارزش‌های تحت حمایت حق شخصیت نیز آسیب می‌بینند. با استفاده از این داده‌ها در سکوه‌های رسانه‌های اجتماعی، حریم داده‌های شخصی نقض می‌شود و اگر در هنگام ایجاد حساب از نام، نام خانوادگی یا عکس فرد بدون رضایت وی استفاده شده باشد، حق شخصیت بر نام و تصویر نیز نقض می‌گردد. همچنین با انتشار غیرمجاز عکس‌های خصوصی، ویدئوها یا اسرار فرد از طریق این حساب‌های جعلی، حریم خصوصی نیز نقض می‌شود.

(Yavanoğlu et al., 2012, 21)

حساب‌های جعلی که با جعل هویت به نام کاربران در محیط‌های رسانه‌های اجتماعی ایجاد می‌شود، می‌تواند برای ارتکاب برخی جرائم به‌عنوان پوشش استفاده شود. این حساب‌های جعلی که معمولاً برای توهین، تهدید، افترا یا آزار جنسی دیگران ایجاد می‌شود، اغلب برای پنهان‌کردن هویت واقعی مجرم استفاده می‌شود. باین‌حال، در این اعمال، گاهی می‌توان هویت فردی که حساب جعلی را ایجاد کرده و حق شخصیت را نقض نموده است را با بررسی تاریخ و آدرس آی پی اتصال به محیط الکترونیکی مشخص کرد.

یکی دیگر از رویدادهایی که منجر به نقض داده‌های شخصی و امنیت می‌شود، «نرم‌افزارهای شخص ثالث» استفاده‌شده در سکوه‌های رسانه‌های اجتماعی است. این نرم‌افزارها مستقل از سیستم عامل سکوه‌های رسانه‌های اجتماعی تولید شده و برای افزایش وابستگی کاربران به بازی‌ها، سرگرمی‌ها و موارد مشابه به‌صورت اختیاری نصب می‌شوند. این نرم‌افزارها معمولاً برای اجرا در یک رابط فلش^۱ یا جابوا^۲ در سکوی رسانه‌های اجتماعی طراحی شده‌اند و از سوی سکو به‌طور رسمی پشتیبانی نمی‌شوند و در خط‌مشی حریم خصوصی قرار نمی‌گیرند. این نرم‌افزارها به دلیل دسترسی به اطلاعات خصوصی کاربران و اطلاعات کارت اعتباری آن‌ها به دلیل خدمات ارائه‌شده، تهدید بزرگی برای کاربران محسوب می‌شوند.

ب. نقض‌ها به دلیل جرائم رایانه‌ای

یکی از موارد رایج در پلتفرم‌های رسانه‌های اجتماعی، سرقت هویت یا به‌دست‌آوردن حساب‌های دیگران است. به‌دست‌آوردن حساب‌های عضویت و پروفایل کاربران توسط اشخاص ثالث از طریق هک‌کردن رمزهای عبور در پلتفرم‌های رسانه‌های اجتماعی، یک جرم رایانه‌ای است که مصداق جرم «ورود و ماندن غیرقانونی در سیستم رایانه‌ای» تحت ماده ۷۲۹ قانون جرایم رایانه‌ای ایران می‌باشد. در این حالت، ارزش‌هایی مانند اطلاعات هویتی، تصویر، آدرس ایمیل و موارد مشابه که تحت حمایت حق شخصیت

1. Flash
2. Java

قرار دارند، آسیب می‌بیند و در نتیجه حق شخصیت نیز نقض خواهد شد. (قانون جرایم رایانه‌ای) همچنین اقداماتی مانند مختل کردن، آسیب‌رساندن به عملکرد سیستم رایانه‌ای، نابودکردن، تغییر، غیرقابل‌دسترس کردن داده‌های موجود در سیستم رایانه‌ای، قراردادن داده‌ها در سیستم یا ارسال داده‌ها به جای دیگر، جرم محسوب می‌شوند.

در پلتفرم‌های رسانه‌های اجتماعی با ورود به حساب‌های افراد و حذف ایمیل‌های آن‌ها، تغییر رمز عبور، ارسال اطلاعات و عکس‌های خصوصی به دیگران، یا ارسال مکاتبات محرمانه به‌جای دیگر، حریم خصوصی، داده‌های شخصی، حقوق بر تصویر، اسرار، آزادی ارتباطات و دسترسی به اطلاعات و در نتیجه حق شخصیت فرد نقض خواهد شد. (Kaya, 2015, 297)

در دنیای بازی مجازی، کاربران با محتوای دیجیتالی (ظاهر) موسوم به «شخصیت» در یک موضوع خاص یا «آواتار» در دنیای واقعیت مجازی در سکو حضور دارند. یک موضوع رایج در دنیاهای مجازی، «سرقت شخصیت» یا «سرقت آواتار» نامیده می‌شود که در آن اشخاص غیر از کاربر، با هک کردن رمز عبور و با استفاده از نرم‌افزارهای مناسب، این محتواها را به‌طور غیرقانونی به‌دست می‌آورند. (Dülger, 2014, 393)

در دنیای مجازی شبیه‌سازی‌شده، این محتواهای دیجیتالی توسط کاربر ایجاد می‌شوند و تمامی ویژگی‌هایی مانند نژاد، جنسیت، وزن، قد و غیره توسط کاربر تعیین می‌گردد. در سیستم‌های مبتنی بر توانایی و رده، کاربران می‌توانند با تکمیل وظایف خاص، توانایی‌های مختلفی را کسب کنند یا به درجات بالاتری ارتقا یابند. همچنین اگر سیستم امکان تجارت را فراهم کند، پول واریز شده به بازی می‌تواند به پول واقعی تبدیل شود. (Dülger, 2014, 393-394)

از دیدگاه حقوق خصوصی، در قراردادهای میان کاربر و ارائه‌دهنده خدمات رسانه‌های اجتماعی، مشخص می‌شود که مالکیت معنوی هرگونه شیء، لباس، انیمیشن، طراحی یا برنامه تولیدشده در این دنیای مجازی به‌طورکلی متعلق به کاربر خالق آن است. در زمینه حقوق مالکیت معنوی، حقوق ناشی از مالکیت اثر برای کاربر در خصوص این‌گونه محتواهای دیجیتالی «حای و ویژگی‌های مالک» قابل طرح است. (Dülger, 2014, 393) با اینکه در مطالعات حقوقی مؤلف کسی تعریف شده که اثر را ایجاد می‌کند، اما در حقوق، به‌طورکلی تمام افرادی که با مشارکت و سهم ویژه خود در خلق یک اثر نقش داشته‌اند، مؤلف محسوب می‌شوند. (Beşiroğlu, 2002, 121- Ateş, 2003, 79)

در صورتی که این‌گونه محتواها درآمدزا باشند، می‌توان آن‌ها را جزء حقوق مالی فرد در نظر گرفت و کاهش یا از دست رفتن درآمد ناشی از آن را با پرداخت خسارت مادی جبران کرد. از دیدگاه حق شخصیت در خصوص به‌دست آوردن غیرقانونی این محتواهای دیجیتال، به‌نظر می‌رسد که برای اینکه چنین اقدامی

نقض حق شخصیت محسوب شود، باید در حین به‌دست‌آوردن این محتوا، ارزش‌های تحت حمایت حق شخصیت نقض شده باشند یا این محتوای دیجیتال، ارزش‌های تحت حمایت حق شخصیت را در خود داشته باشد. به‌عنوان مثال، در صورت سرقت شخصیتی که یک راننده مشهور اتومبیل‌رانی به آن نام خود را داده، ویژگی‌ها و توانایی‌های واقعی خود را در آن منعکس کرده است، از آنجا که نام فرد بدون رضایت وی استفاده شده، می‌توان از نقض حق شخصیت سخن گفت. حمله به ارزش‌های تحت حمایت حق شخصیت، خود به خود نقض حق شخصیت محسوب می‌شود و در اینجا نیازی به کسب درآمد از محتوای دیجیتال نیست؛ اما اگر از دست‌رفتن درآمد یا خسارت مادی دیگری ناشی از چنین اقداماتی رخ دهد، می‌توان خواستار جبران این خسارات مادی شد. (Kaya, 2015, 298)

حساب‌های به‌دست‌آمده در رسانه‌های اجتماعی معمولاً برای فریب و کلاهبرداری از دیگران و کسب منفعت استفاده می‌شوند. به‌عنوان مثال، با دسترسی به دفتر آدرس، گروه‌ها یا فهرست دوستان یک حساب هک شده، به دوستان آن شخص پیام‌هایی مبنی بر اینکه وی بدون اعتبار، در خارج از کشور است یا هوشش به سرقت رفته، ارسال می‌شود و از آن‌ها درخواست پول، شماره کارت اعتباری بانکی، شارژ تلفن همراه و موارد مشابه می‌شود تا افراد را فریب دهند. یک مثال دیگر از حملات از طریق حساب‌های هک‌شده علیه سایر کاربران، ارسال پیام‌های «اسپم» به دوستان، اعضای گروه یا مخاطبان دفتر آدرس است. گاهی نیز با چنین پیام‌هایی، کدهای مخرب، ویروس یا نرم‌افزارهای جاسوسی به حساب افرادی که آن پیام را دریافت کرده‌اند، ارسال می‌شود تا با بازکردن پیام، اطلاعات مختلفی به‌دست‌آید یا به سیستم آسیب وارد شود. (Kaya, 2015, 298).

رسانه‌های اجتماعی علاوه بر فضاهای اشتراک متقابل و تعامل، با قابلیت‌هایی مانند پیام‌رسانی فوری و گفتگوهای زنده، محیط‌هایی هستند که افراد می‌توانند در آن‌ها ارتباط برقرار کنند. حملات به این محیط‌های ارتباطی از طریق فناوری‌های اطلاعات می‌تواند منجر به ارتکاب برخی جرائم رایانه‌ای و در نتیجه نقض حق شخصیت شود. با قراردادن نرم‌افزارهای مخرب مانند ویروس، کرم و بمب‌های منطقی در حساب‌های شخصی یا صفحات وب مانند وبلاگ‌ها در رسانه‌های اجتماعی، می‌توان به سیستم آسیب وارد کرد. این اقدامات غیرقانونی که موجب اختلال در ارتباطات کاربران یا توقف انتشارات در رسانه‌های اجتماعی می‌شوند، جرم ممانعت از ارتباطات را تشکیل می‌دهند.

اگر ارتباطات در رسانه‌های اجتماعی توسط اشخاص ثالث شوند، جرم نقض حریم ارتباطات محقق می‌شود. همچنین انتشار این ارتباطات در رسانه‌های اجتماعی بدون رضایت طرفین یا اشخاص ثالث نیز جرم نقض حریم ارتباطات محسوب می‌گردد.

منبسط مکالمات میان افراد بدون رضایت یکی از طرفین و انتشار غیرقانونی این داده‌ها در

رسانه‌های اجتماعی مانند یوتیوب، جرم «شنود و ضبط مکالمات» می‌شود. این عمل از آنجا که حریم ارتباطات و در نتیجه حریم خصوصی را نقض می‌کند، همچنین نقض حق شخصیت نیز هست. (Kaya, 2015, 298)

انجام اقداماتی که حریم خصوصی افراد را نقض می‌کند، مانند به‌دست‌آوردن پیام‌های فیسبوک، عکس‌های محافظت‌شده با تنظیمات حریم خصوصی یا هک‌کردن رمزها با استفاده از نرم‌افزارهای جاسوسی مانند اسپتروا در پلتفرم‌های رسانه‌های اجتماعی جرم نقض حریم خصوصی را تشکیل می‌دهد. همچنین بارگذاری مستقیم تصاویر و صداها یا مربوط به حریم خصوصی افراد در رسانه‌های اجتماعی از طریق برنامه‌های مختلف یا انتشار آن‌ها در این سکوها با استفاده از لینک‌های ارائه‌شده، جرم محسوب می‌شود. این جرائم با حمله به حریم خصوصی افراد، حق شخصیت آن‌ها را نیز نقض می‌کنند.

با استفاده از فناوری‌های اطلاعاتی مانند سیستم‌های ردیابی صفحه کلید،^۱ ویروس‌ها، اسپ‌های تروا و هک رمز عبور، امکان دسترسی به حساب‌های کاربران رسانه‌های اجتماعی و کسب داده‌ها و اطلاعات در این حساب‌ها بدون اطلاع و رضایت کاربر وجود دارد. این اقدامات غیرقانونی که بدون اطلاع و رضایت کاربر انجام می‌شوند، با ثبت داده‌های شخصی یا ثبت اطلاعات مربوط به عقاید سیاسی، فلسفی یا مذهبی، ریشه‌نژادی، گرایش‌های اخلاقی، زندگی جنسی، وضعیت سلامتی یا روابط اتحادیه‌ای افراد به‌عنوان داده شخصی، جرم «ثبت داده‌های شخصی» را تشکیل می‌دهند. علاوه بر این، انتقال داده‌های شخصی در رسانه‌های اجتماعی به دیگران، انتشار آن‌ها در این سکوها یا به‌دست‌آوردن آن‌ها از طریق نرم‌افزارهای جاسوسی، جرم «افشا یا به‌دست‌آوردن داده‌های شخصی» است. این اقدامات در عین حال از منظر حقوق خصوصی نقض امنیت داده‌های شخصی و در نتیجه نقض حریم خصوصی محسوب شده و نقض حق شخصیت را رقم می‌زنند. در اینجا باید به داده‌هایی مانند اطلاعات هویتی و عکس‌هایی که فرد با رضایت خود در رسانه‌های اجتماعی به اشتراک گذاشته است نیز پرداخت و مشروعیت ثبت، استفاده و انتشار آن‌ها توسط دیگران را بررسی کرد. در حالی که برخی نویسندگان ثبت داده‌های شخصی که با رضایت در رسانه‌های اجتماعی منتشر شده‌اند را از نظر حقوق کیفری مجاز می‌دانند، (Karagülmez, 2011, 354) نویسندگان دیگری معتقدند برای داده‌های شخصی منتشر شده در رسانه‌های اجتماعی افراد شناخته‌شده عمومی، به‌غیر از آنچه در خارج از محدوده حریم خصوصی قرار دارد، باید رضایت آشکار در مورد اینکه چه داده شخصی، توسط چه کسی، کجا و چگونه استفاده می‌شود، جلب شود.

اگر قاعده کلی را این‌گونه بپذیریم که افراد بر داده‌های شخصی خود حق تصرف دارند و این داده‌ها

1. keylogger

فقط با رضایت آن‌ها می‌تواند پردازش شود، اما موضوع را از منظر حقوق خصوصی بررسی کنیم، به نظر ما نمی‌توان نتیجه گرفت که در همه موارد استفاده و اشتراک‌گذاری محتوای منتشرشده در پلتفرم‌های رسانه‌های اجتماعی توسط دیگران، همواره مبتنی بر رضایت است و این رضایت در هر شرایطی به‌عنوان دلیل قانونی بودن عمل تلقی می‌شود.

داده‌های شخصی مانند اطلاعات هویتی، عکس‌ها، تصاویر خصوصی، ضبط صدا و غیره در پلتفرم‌های رسانه‌های اجتماعی مانند یوتیوب، فیسبوک و اینستاگرام با رضایت کاربر منتشر می‌شوند، اما پس از آن مشاهده می‌شود که کاربران دیگر یا اشخاص ثالث غیرعضو می‌توانند از آن‌ها استفاده کنند. استفاده از داده‌هایی که با تنظیمات حریم خصوصی محافظت شده و فقط به برخی افراد خاص دسترسی داده شده است، توسط افراد غیرمجاز، قانونی نیست؛ زیرا رضایت فقط برای استفاده افراد خاص معتبر است. محدودکردن دسترسی برای سایر افراد نیز نشانه این موضوع است. درواقع، دسترسی افراد غیر از آن‌هایی که اجازه دسترسی ندارند، فقط از طریق بهره‌گیری غیرقانونی از نقاط ضعف امنیتی یا با استفاده از فناوری‌های رایانه‌ای امکان‌پذیر است. اگر این‌گونه استفاده‌ها توسط کاربران دیگر انجام شود، نه تنها نقض قوانین استفاده و شرایط قراردادی با ارائه‌دهنده سرویس رسانه‌های اجتماعی است، بلکه یک عمل نادرست در قبال فردی است که داده‌هایش مورد سوءاستفاده قرار گرفته است. همچنین، از آنجا که استفاده از پلتفرم‌های رسانه‌های اجتماعی مستلزم اقداماتی مانند کسب مجوز عضویت، ایجاد حساب یا پروفایل است، افرادی که این اقدامات را انجام نمی‌دهند، حق استفاده از سرویس‌های ارائه‌شده در سکو و محتوای منتشرشده در آن را ندارند؛ بنابراین، عمل اشخاص ثالث که بدون عضویت اما با دستکاری غیرمجاز وارد سیستم می‌شوند، غیرقانونی است و استفاده غیرمجاز آن‌ها از داده‌هایی که کاربران با رضایت منتشر کرده‌اند نیز غیرقانونی است.

برای اینکه بتوان در مورد استفاده قانونی از داده‌هایی که با رضایت منتشر شده‌اند توسط کاربران دیگر که مجاز به استفاده هستند صحبت کرد، به نظر ما باید به هدف رضایت و محدودیت‌های عمومی که برای رضایت در نظر گرفته می‌شود، توجه کرد. در مواردی که هدف رضایت به صراحت بیان شده است، استفاده مطابق با آن هدف باید قانونی تلقی شود. اما در مواردی که هدف رضایت به صراحت بیان نشده است، نتیجه‌ای که از تعیین این هدف حاصل می‌شود، در قانونی بودن یا نبودن آن مؤثر خواهد بود. برای تعیین هدف رضایت، باید ارزیابی شود که آیا رضایت عمومی کافی است یا رضایت خاص موردنیاز است، محیطی که داده در آن استفاده می‌شود، هدف استفاده و نحوه آن باید مورد بررسی قرار گیرد. به‌عنوان مثال، یک کاربر می‌تواند انتظار داشته باشد که عکس منتشرشده در فیسبوک، در خط زمانی یا یک گروه که برای همه قابل مشاهده است، توسط سایر کاربران به اشتراک گذاشته

شود. بنابراین باید فرض کرد که این گونه موارد استفاده در چارچوب هدف رضایت قرار دارد و برای آن‌ها رضایت داده شده است. اما استفاده از این عکس منتشرشده برای تبلیغات محصولات خاص یا اهداف تجاری، نیازمند کسب رضایت خاص جداگانه خواهد بود و نمی‌توان فقط از روی انتشار آن، نتیجه گرفت که رضایت برای این موارد نیز داده شده است. از نظر اصول تبلیغاتی نیز، نقض حقوق شخصیت دیگران مجاز نیست و برای این کار باید رضایت فرد کسب شود. بنابراین در این زمینه رضایت خاص موردنیاز خواهد بود.

محیطی که داده در آن استفاده می‌شود نیز باید در تعیین هدف رضایت مدنظر قرار گیرد. به‌عنوان مثال، استفاده از تصاویر منتشرشده کاربران جوان در محیط‌های دوستانه برای اهداف جستجوی دوست یا بازاریابی محصولات جنسی، به این معنا نیست که آن‌ها برای چنین مواردی رضایت داده‌اند. استفاده از داده‌های منتشرشده در رسانه‌های اجتماعی به شکل‌های متفاوت با اضافات یا اِلِمان‌های تدوین، که باعث معرفی فرد به شکلی متفاوت با استفاده از آن به‌عنوان یک پیام می‌شود، نیز در تعیین هدف رضایت مؤثر خواهد بود.

محدودیت‌های عمومی که برای رضایت در حقوق خصوصی در نظر گرفته می‌شود، باید در ارزیابی اعتبار رضایت و قانونی‌بودن اقداماتی که با رضایت انجام می‌شود، مورد توجه قرار گیرد. در مورد انتشار محتوا در پلتفرم‌های رسانه‌های اجتماعی نیز، باید رضایت را به این شکل ارزیابی کرد که اگر محتوای منتشرشده با رضایت، در صورت استفاده توسط دیگران، منجر به ازبین‌رفتن حقوق شخصیت فرد شود یا غیرقانونی و خلاف اخلاق باشد، باید رضایت را نامعتبر در نظر گرفت. به‌عنوان مثال، اگر داده شخصی منتشرشده در یک پلتفرم‌های رسانه‌های اجتماعی، برای پروفایل یک حساب کلاهبرداری از دیگران استفاده شود، این رضایت معتبر نخواهد بود.

سکوی رسانه اجتماعی توسط کاربران کودک نیز مورد استفاده قرار می‌گیرند و سن عضویت می‌تواند تا ۱۳ سال کاهش یابد. (شریعتی، زمانیان، خلیلی، ۱۴۰۰: ۱۰۳) در پلتفرم‌های رسانه‌های اجتماعی کاربران با نیت بد، به‌ویژه آن‌هایی که کودکان را هدف قرار می‌دهند، می‌توانند با برقراری دوستی در این سایت‌ها، کودکان را به‌راحتی فریب دهند و از آن‌ها سوءاستفاده کنند. برخی کاربران که با کاربران کودک در سایت‌های رسانه‌های اجتماعی دوست می‌شوند، با ایجاد اعتماد و ترغیب، آن‌ها را به گفتگوهای جنسی وادار می‌کنند و از آن‌ها می‌خواهند نواحی خصوصی بدن خود را به دوربین نشان دهند و آن‌ها را ضبط می‌کنند. به این ترتیب، با استفاده از کودکان، جرم اخلاقی رخ می‌دهد. نه تنها تولید این محصولات جرم است، بلکه تکثیر، فروش، انتقال، ذخیره، صادرات، ارائه به دیگران، انتشار یا واسطه‌گری در انتشار آن‌ها نیز جرم محسوب می‌شود. در این اعمال، حق شخصیت مربوط به تصاویر

بدن و حریم خصوصی که از ارزش‌های شخصی کودک است، نقض می‌شود و رضایت کودک، حتی اگر قدرت تشخیص داشته باشد، از آنجا که با حيله به‌دست‌آمده، فرد نمی‌تواند با رضایت خود از اصل حقوق صرف‌نظر کند و رضایت نمی‌تواند غیرقانونی و خلاف اخلاق باشد، به‌عنوان دلیل قانونی‌بدون عمل پذیرفته نخواهد شد.

۴. علل و ابعاد نقض حق شخصیت

۴-۱. فقدان قانون جامع حمایت از داده‌های شخصی

یکی از مهم‌ترین علل نقض حق شخصیت، نبود قوانین جامع و الزام‌آور برای حفاظت از داده‌های شخصی است. این فقدان باعث می‌شود اطلاعات حساس افراد، به‌ویژه در فضای مجازی، به‌راحتی در دسترس دیگران قرار گیرد و مورد سوءاستفاده قرار گیرد.

۴-۲. انتشار بدون مجوز اطلاعات و داده‌های دیگران

اشتراک‌گذاری اطلاعات شخصی، تصاویر، و ویدئوهای دیگران بدون کسب اجازه از صاحب آن، یکی از رایج‌ترین موارد نقض حق شخصیت است. این عمل، نه‌تنها حریم خصوصی افراد را تحت تأثیر قرار می‌دهد، بلکه ممکن است آسیب‌های جدی به حیثیت و اعتبار آن‌ها وارد کند.

۴-۳. ضعف در سازوکارهای نظارتی پلتفرم‌های رسانه‌های اجتماعی

سکوهاي اجتماعي غالباً در نظارت بر محتوای منتشرشده و حذف سریع محتوای نقض‌کننده حقوق شخصیت کوتاهی می‌کنند. این ضعف باعث می‌شود محتوای آسیب‌زا مدت طولانی در دسترس عموم باقی بمانند.

۴-۴. عدم آگاهی و سواد دیجیتال کاربران

بسیاری از کاربران به دلیل ناآگاهی از پیامدهای انتشار اطلاعات شخصی یا استفاده از محتوای دیگران بدون اجازه، خود عامل نقض حقوق دیگران می‌شوند. ارتقای سواد دیجیتال می‌تواند از وقوع چنین مواردی پیشگیری کند.

۴-۵. وجود حساب‌های جعلی و سرقت هویت

ایجاد حساب‌های جعلی و سوءاستفاده از هویت دیگران یکی از مشکلات رایج در فضای مجازی است. این اقدام نه‌تنها حقوق شخصیت را نقض می‌کند، بلکه می‌تواند به جرائم جدی‌تری مانند کلاهبرداری منجر شود.

۴-۶. افشای داده‌های خصوصی توسط هکرها و جرائم سایبری

هک کردن سیستم‌های اطلاعاتی و افشای اطلاعات کاربران توسط افراد با نیت‌های مجرمانه، یکی دیگر از موارد مهم نقض حق شخصیت است. این نوع جرائم به دلیل پیشرفت فناوری، به سرعت در حال افزایش است.

۴-۷. مشکلات مربوط به قوانین بین‌المللی در فضای مجازی

در بسیاری از کشورها، هنوز قوانین ملی و بین‌المللی برای حفاظت از حقوق شخصیت در فضای مجازی به‌طور کامل هماهنگ نشده‌اند. این خلأ قانونی، مسئولیت‌پذیری کاربران و سکوها را کاهش می‌دهد.

۴-۸. عدم رعایت اصول اخلاقی در استفاده از اطلاعات دیگران

حتی در صورت وجود قوانین، گاه عدم رعایت اصول اخلاقی توسط کاربران یا سازمان‌ها باعث نقض حقوق شخصیت می‌شود. احترام به حریم خصوصی دیگران باید به یک فرهنگ تبدیل شود.

۴-۹. ضعف در استفاده از فناوری‌های پیشگیرانه

سکوها و کاربران اغلب از فناوری‌هایی مانند رمزنگاری داده‌ها یا ابزارهای حفاظتی استفاده نمی‌کنند که منجر به آسیب‌پذیری اطلاعات می‌شود.

۴-۱۰. عدم شفافیت در خط‌مشی‌های سکوها

بسیاری از کاربران از نحوه استفاده سکوها از اطلاعات شخصی‌شان مطلع نیستند. نبود شفافیت در این زمینه می‌تواند به نقض گسترده حقوق شخصیت منجر شود.

نتیجه‌گیری

حق بر شخصیت، یکی از حقوق بنیادین بشری است که در نظام‌های حقوقی به‌عنوان ضامن کرامت انسانی، آزادی‌های فردی، و حریم خصوصی مورد شناسایی قرار گرفته است. این حق، دربرگیرنده ارزش‌های فیزیکی، عاطفی و اجتماعی شخصیت است که حفاظت از تمامی ابعاد زندگی فردی و اجتماعی انسان‌ها را تضمین می‌کند. درعین‌حال، پیشرفت فناوری و گسترش استفاده از رسانه‌های اجتماعی، چارچوب سنتی حمایت از حقوق شخصیت را به چالش کشیده است. پژوهش حاضر نشان می‌دهد که نقض حق شخصیت در فضای مجازی، اغلب ناشی از فقدان قوانین جامع، ناآگاهی کاربران، ضعف در نظارت بر محتوای منتشرشده، و سوءاستفاده از پیشرفت‌های تکنولوژیکی است. مواردی همچون افشای اطلاعات خصوصی، انتشار محتوای توهین‌آمیز یا

اطلاعات نادرست، سوءاستفاده از هویت، و جرائم سایبری، نمونه‌های برجسته‌ای از نقض این حق در بستر دیجیتال هستند. این موارد نه تنها به فرد آسیب می‌رسانند، بلکه پیامدهای اجتماعی گسترده‌ای از جمله کاهش اعتماد عمومی به امنیت فضای مجازی و تضعیف انسجام اجتماعی را به دنبال دارند.

در بررسی تعارض‌های موجود، روشن است که آزادی بیان و حریم خصوصی دو مفهوم اساسی اما گاه متناقض در فضای مجازی هستند. از یک‌سو، آزادی بیان به‌عنوان یکی از حقوق اساسی کاربران، محیطی برای ابراز نظر فراهم می‌کند؛ اما از سوی دیگر، این آزادی نمی‌تواند توجیهی برای نقض حریم خصوصی و حقوق شخصیت دیگران باشد. تنظیم این تعارضات نیازمند تبیین دقیق اصول و چارچوب‌های حقوقی است که هم‌زمان از آزادی بیان حمایت کند و از تعرض به حقوق دیگران جلوگیری کند.

این مطالعه به این نتیجه می‌رسد که برای مقابله با نقض حق شخصیت در فضای مجازی، مجموعه‌ای از اقدامات ضروری است:

تدوین قوانین جامع و الزام‌آور در سطح ملی و بین‌المللی:

این قوانین باید به‌صراحت اصول حمایت از حقوق شخصیت را تعریف کنند، سازوکارهای نظارتی و تنبیهی مشخصی داشته باشند، و تعارضات میان حقوق مختلف کاربران را تنظیم نمایند.

افزایش مسئولیت‌پذیری پلتفرم‌های رسانه‌های اجتماعی:

پلتفرم‌ها باید نه تنها در حذف محتوای مضر، بلکه در پیشگیری از نقض حقوق شخصیت نقش فعالی ایفا کنند. این مسئولیت می‌تواند با استفاده از الگوریتم‌های هوش مصنوعی و فناوری‌های پیشرفته برای شناسایی سریع و حذف محتوای آسیب‌زا تقویت شود.

ارتقای سواد دیجیتال و آگاهی‌بخشی به کاربران:

آموزش کاربران درباره حقوق شخصیت، اهمیت حفظ اطلاعات شخصی، و مخاطرات فضای مجازی، یکی از گام‌های اساسی در کاهش نقض این حق است.

به‌کارگیری فناوری‌های حفاظتی و امنیتی:

توسعه ابزارهای حفاظتی مانند رمزنگاری داده‌ها، سیستم‌های احراز هویت پیشرفته، و فناوری‌های پیشگیرانه می‌تواند آسیب‌پذیری‌های موجود را کاهش دهد.

هماهنگی بین‌المللی در مبارزه با جرائم سایبری:

نقض حق شخصیت در فضای مجازی غالباً مرزهای جغرافیایی را در می‌نوردد. بنابراین، همکاری بین‌المللی میان دولت‌ها و سازمان‌های مرتبط، در تدوین قوانین، تبادل اطلاعات و تعقیب جرائم سایبری ضروری است.

توسعه مطالعات میان‌رشته‌ای در حوزه حقوق و فناوری:

بررسی جامع پیامدهای حقوقی، اخلاقی و اجتماعی فناوری‌های نوین و شناسایی روش‌های تعامل مؤثر میان این حوزه‌ها، به سیاست‌گذاران کمک می‌کند تا رویکردهای نوینی برای حفظ حقوق کاربران در فضای دیجیتال ارائه دهند.

به‌طورکلی، این پژوهش نشان می‌دهد که تعادل میان نوآوری تکنولوژیک و حفظ حقوق شخصیت، یکی از الزامات حیاتی حکمرانی دیجیتال در عصر حاضر است. برای دستیابی به این هدف، هم‌زمان نیاز به تغییرات ساختاری در قوانین، تقویت اخلاق دیجیتال، و توسعه فناوری‌های حمایتی است. درنهایت، ایجاد محیطی امن در فضای مجازی که حقوق و کرامت انسانی را در تمامی ابعادش حفظ کند، نیازمند همکاری فراگیر دولت‌ها، سکوها، رسانه‌ای، و کاربران است.

منابع

- اصلانی، حمیدرضا، (۱۳۷۹)، حقوق فناوری اطلاعات، نشر میزان، تهران.
- انصاری، باقر، (۱۳۹۲)، حقوق ارتباط جمعی، نشر سمت، تهران.
- پورسید، بهزاد، فرجزادی، محمدجواد، حیدری هرسثانی، محمدجواد، (۱۴۰۳)، مفهوم‌شناسی «شخص» و «شخصیت» و تأثیر اشتباه در آن‌ها بر وضعیت اعمال حقوقی، پژوهش‌نامه حقوق اسلامی
- حبیبی مجنده، محمد، (۱۳۹۵)، حق دسترسی به اطلاعات و کپی‌رایت در فضای مجازی، فصلنامه حقوق پزشکی، ویژه‌نامه حقوق مالکیت معنوی، ۷-۳۵.
- حبیبی، همایون، (۱۳۹۵)، حق بر حریم خصوصی در شبکه‌های اجتماعی، فصلنامه تحقیقات حقوقی، شماره ۷، ۳۹-۶۴.
- خسروی، حمیدرضا، (۱۳۹۲)، نظام شخصیت‌سازی، انتشارات سبز، تهران.
- رحمدل، منصور، (۱۳۸۴)، حق انسان بر حریم خصوصی، فصلنامه دانشکده حقوق و علوم سیاسی دانشگاه تهران، شماره ۷، ۴۶-۱۱۹.
- رضوی‌فرد، بهزاد، موسوی، سیدنعمت‌اله، (۱۳۹۵)، مسئولیت کیفری در فضای سایبر در ایران، فصلنامه پژوهش حقوق کیفری، دوره ۵، شماره ۱۶، ۲۹-۴۵.
- شریعتی، مریم، زمانیان، معصومه، خلیلی، میلاد، (۱۴۰۰)، انتشار تصاویر کودکان در فضای مجازی و تأثیر آن بر شخصیت‌سازی پیش از بلوغ در پرتو حقوق ایران و مقررات بین‌المللی، حقوق فناوری‌های نوین، دوره ۲، شماره ۱، ۱-۱۸.
- شریفی، علی‌اصغر، صفایی، حسین، الماسی، نجاد علی، ساوریایی، پرویز، (۱۴۰۲)، مسئولیت مدنی و اخلاقی با محوریت نقض حقوق مربوط به شخصیت اشخاص در فضای مجازی، اخلاق در علوم و فناوری، دوره ۱۸، شماره ۳، ۸۴-۹۱.
- شفیعی، فروزنده، دهقان‌چناری، مجید، (۱۳۹۸)، بررسی نقض مالکیت فکری در فضای مجازی، فصلنامه قانون یار، دوره ۳، شماره ۱۰، ۹۵-۱۳۴.
- عالی‌پور، حسن، (۱۳۹۰)، حقوق کیفری فناوری اطلاعات، نشر خرسندی، تهران.
- فتحی، یونس، شاهمرادی، خیراله، (۱۳۹۵)، گسترش قلمرو حریم خصوصی در فضای مجازی، مجله دادگستری، شماره ۹۹، ۲۲۹-۲۵۲.
- کریمی، حسین، (۱۳۹۵)، حقوق اخلاقی و جایگاه آن در فضای مجازی، فصلنامه اخلاق، دوره ۶، شماره ۷۱، ۸۸-۷۱.
- محسنی، فرید، قاسم‌زاده، فریدون، (۱۳۸۵)، حریم شخصی در فضای مجازی با تکیه بر حقوق ایران، فصلنامه شریف، شماره ۳۴.
- محمدزاده، صالح، (۱۳۹۶)، حریم شخصی و سرقت، نشر سمت، تهران.
- مظهر قراملکی، علی، قدرتی، فاطمه، نظری ترکلی، سعید، (۱۳۹۵)، شاخصه‌ها و احکام حقوق وابسته به شخصیت انسان، فقه و مبانی حقوق اسلامی، ۲۷۹- (۲)۴۹.
- Ateş, M. (2003). Fikir ve Sanat Eserleri Üzerindeki Hakların Kapsamı ve Sınırlandırılması.

- Ankara: Seçkin Yayıncılık.
- Beşiroğlu, A. (2002). Düşünce Ürünleri Üzerindeki Haklar Fikir Hukuku Birinci Cilt Mel Kurallar. Ankara: APB Yayınları.
 - Brunty, J., & Helenek, K. (2013). Social Media Investigations of Law Enforcement. Massachusetts.
 - Dülger, M. V. (2014). Bilişim Suçları ve İnternet İletişim Hukuku (4th ed.). Ankara: Seçkin Yayınevi.
 - Eren, F. (2012). Borçlar Hukuku Genel Hükümler (14th ed.). Ankara: Yetkin Yayıncılık.
 - Kaplan, A. M., & Haenlein, M. (2010). Users of the World, Unite! The Challenges and Opportunities of Social Media. *Business Horizons*, 53(1).
 - Karagülmez, A. (2011). Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri (3rd ed.). Ankara: Seçkin Yayınevi.
 - Kılıçoğlu, A. M. (2013). Şeref Haysiyet ve Özel Yaşama Basın Yoluyla Saldırlardan Hukuksal Sorumluluk (4th ed.). Ankara: Turhan Kitapevi.
 - Kietzmann, J. H., Hermkens, K., Mccarthy, I. P., & Silvestre, B. S. (2011). Social Media? Get Serious! Understanding the Functional Building Blocks of Social Media. *Busines Horizons*, 54(3).
 - Lietsala, K., & Sirkkunen, E. (2008). Social Media. Tampere.
 - Oğuzman, K., Selçi, Ö. & Oktay-Özdemir, S. (2012). Kişiler Hukuku (Gerçek ve Tüzel Kişiler) (12th ed.). İstanbul: Filiz Kitapevi.
 - Vural, Z. B. A., & Bat, M. (2010). Yeni Bir İletişim Ortamı Olarak Sosyal Medya: Ege Üniversitesi İletişim Fakültesine Yönelik Bir Araştırma. *Journal of Yasar University*, 20.
 - Yavanoğlu, U., Sağroğlu, Ş., & Çolak, İ. (2012). Sosyal Ağlarda Bilgi Güvenliği Tehditleri ve Alınması Gereken Önlemler. *Gazi Üniversitesi Politeknik Dergisi*, 15(1), 15-27.

