# حریم شخصی در فضای سایبر

محمد جعفری[۱]

[۱] کارشناسی ارشد مدیریت فناوری اطلاعات گرایش کسب و کار الکترونیکی، دانشکده مدیریت و حسابداری دانشکدگان فارابی دانشگاه تهران
jafarim584@gmail.com

**چکیده**

در عصر فناوری اطلاعات و ارتباطات تمام جنبه‌های زندگی جوامع بشری خواسته یا ناخواسته تحت تأثیر قرار گرفته‌اند. با گسترش روزافزون فضای سایبری، نگرانی‌های زیادی هم در این خصوص ایجاد می‌شود که یکی از آنها مربوط به حریم خصوصی افراد حقیقی و حقوقی می‌باشد. با افزایش کاربران فضای مجازی موضوعی که بیش از پیش اهمیت پیدا می‌کند مسأله حریم خصوصی افراد در این فضا می باشد. امروز نقض حریم افراد و مؤسسات با توجه به امکانات عصر فناوری اطلاعات و ارتباطات بصورت گسترده و آن هم در محدوده‌ای به وسعت جهان هستی فراهم شده است ما در این پژوهش ضمن بررسی مفهوم حریم خصوصی در فضای سایبری، کوشیده‌ایم تا مهمترین مصادیقی که حریم خصوصی در فضای سایبری را نقض می‌کند بیان کنیم. ضمن آن که باید بیان کنیم فضای سایبری همچون دیگر بسترهایی که بشر امروزی در آن به فعالیت می‌پردازد برای مصون ماندن از آسیب‌های مختلف نیازمند تدوین پروتکل‌ها و دستورالعمل‌های خاصی است.

**کلمات کلیدی:** فضای سایبری، حریم شخصی، تهدید.

## ۱ مقدمه

به لطف پیشرفت‌های فناوری ما وارد عصری شده‌ایم که آن را عصر اطلاعات می‌نامند. جامعهٔ بشری روزگار ما، جامعه‌ای اطلاعات محور است؛ بدین معنی که اطلاعات نقش محوری در آن ایفا می‌کند [۱]. پیشرفت سریع فناوری اطلاعات و انتقال تجربیات بشری منجر به تشکیل دنیای جدیدی به نام دنیای مجازی یا همان فضای سایبری شده است؛ دنیایی که در آن محدودیت‌های مرتبط با زمان و مکان بی‌اثر می‌شوند. این ویژگی‌های جدید به حریم شخصی و امنیت افراد خدشه وارد می‌کنند [۲].

امنیت همواره به عنوان یکی از اصلی‌ترین نیازهای بشر مورد توجه بوده است؛ به گونه‌ای که آدمی برای رسیدن به یک محیط مطلوب برای زیستن به تنهایی در آن تمایل دارد و این میلی است به مصون ماندن از دسترسی و اطلاع سایرین که مطلوب نوع بشری است؛ چنین حیطه‌ای از زندگی انسان را حریم خصوصی نامیده‌اند.

عصر اطلاعات جوامع بشری را با تاثیرات ارادی و غیرارادی مواجه کرده است. با گسترش روزافزون فضاي سـایبری، نگرانی‌هـای زیادی هم در این خصوص ایجاد می‌شود و در کنار آثار مثبتی که در بهبود زیست جهـانی دارد، برخی ابعاد منفی و قابل توجه دیگری نیز دارد که حتی ممکن است آثار آن مخرب‌تر از جنگ‌های نظامی بوده و امنیت و ساختارهای یک جامعه را به چـالش بکشـاند. فضای سایبر امکانات جدیدی در اختیار بشر قرار می‌دهد: جغرافیا را از بین مـی‌بـرد؛ انسان را از موثر بودن در محیط اجتماعی، به تاثیرپذیر بودن در محیط مجـازی سـوق مـی‌دهـد؛ ایده‌ها را گسترش می‌دهد؛ کنترل پذیری را کمرنگ می‌سازد و دولت را به عنوان نهاد ناظر بر روابط سیاسی، اجتماعی، فرهنگی و ... خلع سلاح می‌کند.

توسعه فضای سایبر همانند همه‌ی پیشرفت‌های دیگر در زندگی بشر با پیامدهای منفی و مثبت همراه بوده است که یکی از پیامدهای منفی، به خطر انداختن حریم خصوصی افراد و یکی از پیامدهای مثبت تسهیل و تسریع ارتباطات و تبادل اطلاعات است [۳]. در عصر فناوری اطلاعات و ارتباط نقض حریم خصوصی و امنیت افراد حقیقی و حقوقی با استفاده از امکانات این عصر به راحتی امکان‌پذیر شده است. سیستم‌های رایانه‌ای و فضایی سایبری این امکان را فراهم آورده‌اند که در گستره‌ی جهانی، اطلاعات افراد بدون اینکه خودشان مطلع شوند سرقت شود و ارزش ذاتی آن از بین برود [۴].

حریم خصوصی، یکی از بدیهی‌ترین حقوق افراد در جوامع بشری و یک جامعه دموکراتیک است. حریم خصوصی از منظر اسناد بین المللی و منطقه‌ای و نظام حقوقی داخلی کشورها مورد توجه قرار گرفته و در همه این اسناد حیثیت و محرمانگی افراد در جامعه مورد حمایت قرار گرفته است. این قوانین در راستای حفظ حیثیت افراد وضع شده‌اند و می‌توانند حریم خصوصی فضای مجازی افراد را نیز در بر گیرند.

حریم خصوصی و محرمانگی اطلاعات شخصی، مهم‌ترین و جنجالی‌ترین بحثی است که در حوزه فناوری اطلاعات وجود دارد. این موضوع قدمتی به بلندای زمانی دارد که اینترنت و شبکه‌های اجتماعی فراگیر شده است؛ در واقع همچنان که هیچکس در فضای واقعی نمی‌پذیرد که اطلاعات شخصی و خانوادگی خود را در اختیار دیگران قرار دهد، در این فضای جدید نیز کسی به این فکر نمی‌افتد که خود داده‌های شخصی خویشتن را افشا کند. در ادامه این پژوهش به بررسی دو مفهوم فضای سایبر و حریم خصوصی می‌پردازیم سپس رابطه آن‌ها را مورد کنکاش قرار داده و در پایان مهم‌ترین مصادیق نقض حریم خصوصی در فضای سایبری را بیان می‌کنیم.

## ۲ فضای سایبری

فضای سایبر، جدیدترین و در عین حال پیچیده‌ترین پدیده‌ای است که زنـدگی بشـر را به خود مشغول کرده است. رایانـه‌هـا، قبـل از ورود بـه حوزه شبکه، دستگاه‌های پردازشگری بودند که دورنمای سرعت و دقت را برای شرکت‌ها و نهادهای دولتی و غیردولتی فراهم کرده بودند. اما زمانی که این پردازشگرها بـرای اولـین‌بار به صورت شبکه‌ای در یکی از اتاق‌های وزارت دفاع آمریکا در آمدند، اولین بنیان تشکیل فضای سایبری را بنا نهادند.

فضای سایبر به عنوان مجموعه تعامل‌های انسان‌ها از طریق رایانه و فناوری‌های نوین ارتباطات، بدون در

نظر گرفتن زمان و مکان توسط ویلیان گیبسون نویسنده داستان علمی تخیلی در کتاب «نوروموتسر» در سال ۱۹۸۴ به کار برده شد. او فضای سایبر را بازنمایی گرافیکی از داده‌ها از نظام‌های رایانه می‌داند [۵]. کلمه فضاي مجازی (سایبر اسپیس) از درون کلمه سایبرنتیکس که بوسیله نوربرت وینر ابداع شده بود پدید آمد. سایبرنتیکس علم نظریه کنترل است و در مورد سیستم‌های پیچیده به کار می‌رود. فضای سایبر یا فضای مجازی در تعریف برخی نویسندگان عبارت است از: «مجموعه‌ای از ارتباطات درونی انسان‌ها از طریق رایانه و وسائل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی است. البته شاید بهتر باشد آن را چنین تعریف کنیم: «محیط الکترونیکی واقعی است که ارتباطات انسانی به شیوه‌ای سریع، فراتر از مرزهای جغرافیایی و با ابزار خاص، خود؛ در آن، زنده و مستقیم روی می‌دهد. قید (واقعی)، مانع از این است که تصور شود مجازی بودن این فضا به معنای غیر واقعی بودن آن است؛ چرا که در این فضا نیز همان ویژگی‌های تعاملات انسانی در دنیای خارج همچون مسئولیت وجود دارد. ضمن این که فضای سایبر در واقع یک «محیط» است که ارتباطات در آن انجام می‌شوند؛ نه صرف مجموعه ای از ارتباطات. از سوی دیگر، این ارتباطات گرچه ممکن است در همه حال بر خط نباشد، ولی زنده، واقعی و مستقیم است. از این رو، تأثیر و تأثر بالایی در این روابط رخ می‌دهد.

فضای سایبری یک دامنه سراسری در محیط اطلاعاتی است که شامل شبکه‌های مرتبط به هم از زیرساخت‌های فناوری اطلاعات، شامل اینترنت، شبکه‌های مخابراتی، سامانه‌های کامپیوتری، پردازنده‌ها و کنترل‌های توکار است. این تعریف از این نظر قابل توجه است که تنها به مولفه فناوری سخت افزاری اشاره می‌کند، با وجودی که نرم‌افزار و داده‌ها هم ممکن است از واژه‌های به کار برده شده استنباط شود. مورد قابل ذکر دیگر در تعریف فوق، فقدان مولفه انسانی است، در حالی که جزء مهمی در تعاریف وینر و گیبسون است [۶].

فضای سایبر در سند راهبردی امنیت فضای تبادل اطلاعات (افتا): به فضای سایبری، فضای تبادل اطلاعات گفته می‌شود و به صورت زیر تعریف می‌شود:

در عصر اطلاعات شاهد شکل‌گیری فضایی هستیم که در آن فعالیت‌های گوناگونی از قبیل اطلاع‌رسانی، داده‌ورزی، ارائه خدمات، مدیریت و کنترل و ارتباطات از طریق ساز و کارهای الکترونیکی و مجازی انجام می‌پذیرد. از این فضا با نام فتا یاد می‌شود.

نگرش فناورانه به فضای سایبر به مؤلفه‌هایی چون سخت افزار، نرم افزار، کیفیت و کمیت انتقال داده‌ها و تعامل در شبکه می‌پردازد. در حالی که رویکرد روانشناسانه مقوله‌هایی چون فضای ذهنی، الگوی رفتاری انسان و رایانه، تخیل، هویت و شخصیت، به مرز بین واقعیت و خیال و مانند آن توجه می‌کند. دیدگاه جامعه‌شناسانه درباره‌ی فضای سایبر نیز به دلیل پرداختن به جماعت‌های برخط، شبکه‌های اجتماعی سایبر، و آثار اجتماعی تعامل انسان و رایانه حائز اهمیت است.

با شکل‌گیری فضای سایبر، مرزها کمرنگ‌تر شده‌اند و جهانی‌شدن در کلیه امور اجتماعی به وضوح دیده می‌شود. سرعت، ارزانی، بالا بودن کیفیت، نزدیکی و در دسترس بودن، شفافیت و تنوع از ویژگی‌های فضای سایبر است. همچنین فضای سایبر باعث شکل‌گیری حجم انبوهی از داده‌ها و اطلاعات شده است؛ که خود نیازمند ایجاد پروتکل‌های امنیتی خاصی می‌باشد [۷].

# ۳ حریم خصوصی

حریم خصوصی یک مفهوم سیال است که معانی مختلفی از جمله آزادی اندیشه، کنترل بر جسم خود، کنترل بر اطلاعات راجع به خود، آزادی از نظارت‌های دیگران، خلوت و تنهایی، حمایت از حیثیت و اعتیاد و حمایت در برار تفتیش‌ها و تجسس‌ها را شامل می‌شود. حریم خصوصی حق افراد برای برخورداری از حمایت در برابر مداخله بی‌اجازه دیگران، در امور زندگی خود و خانواده‌شان است؛ خواه این عمل با ابزار مستقیم فیزیکی صورت پذیرد یا به وسیله نشر اطلاعات.

در لایحه حریم خصوصی که در زمان دولت هفتم از سوی کمیسیون لوایح دولت تهیه و به مجلس ارائه شد در بند اول ماده ۲ در تعریف حریم خصوصی قید شده بود: «حریم خصوصی قلمروی از زندگی هر شخصی است که آن شخص عرفا یا با اعلان قبلی در چارچوب قانون، انتظار دارد دیگران بدون رضایت وی بدان وارد نشوند یا بر آن نظارت نکنند، یا به اطلاعات راجع به آن دسترسی نداشته باشند، یا آن قلمرو را مورد تعرض قرار ندهند».

## ۱.۳ حریم خصوصی در فضای سایبر

بحث حریم خصوصی در فضای مجازی به حفظ داده‌ها از دسترسی افراد غیر مجاز تعریف می‌شود. منظور از داده‌ها در بحث حریم خصوصی نیز داده‌های شخصی است که همانا مشخصات، ممیزات و اطلاعات مربوط به یک شخص معین یا قابل تمایز که موجب تمایز او از سایر افراد گروه می‌باشد. در فضای سایبر حریم خصوصی اطلاعات و داده‌ها عبارت از اموری هستند که انسان تلاش می‌کند فاش نشوند؛ زیرا این حریم با شخصیت او در ارتباط است. برخی معتقدند حریم خصوصی مختص اشخاص حقیقی است؛ ولی واقعیت این است که اشخاص حقوقی هم نوعی حریم خصوصی داده دارند [۸].

دو اصطلاح حریم خصوصی و داده بیشتر مواقع در کنار هم به کار می‌روند در حالی که کاملا برابر نیستند. حریم قلمرو است، حتی اگر تهی باشد و کافی است تعلق آن به شخص ثابت شود که می‌بایست مورد حمایت واقع شود؛ به همین دلیل دسترسی غیر مجاز به داده‌های عمومی در حریم خصوصی جرم انگاشته شده است. مبنای ترسیم حریم، قانون و مقررات و قرارداد یا عرف است اما داده، پیکرده و مفهوم دارد و باید ارتباطش به شخص ثابت شود.

## ۲.۳ فضای سایبر از لحاظ حقوقی

فضای سایبر از دو جهت وجود و ماهیت قابل بررسی است. از نظر وجودی (فنی) عبارت است از شبکه‌های عنکبوتی و غیر ملموس الکترونیکی که با در هم تنیده‌شدن، این شبکهٔ سراسری و جهانی را شکل داده‌اند. از نظر فنی، این شبکهٔ جهانی سایبر از خود استقلال ندارد و حاصل در هم تنیده‌شدن و ادغام بخش‌های مختلف است که در نهایت یک قلمرو نامحدود سایبر را در فضای خلأ شکل داده است. فضای سایبر را از نظر وجودی می‌توان ظرف نامحدودی دانست که هر کس با دسترسی به آن، امکان وارد کردن یا تخلیهٔ مظروف (محتوا) را در آن دارد؛ بدون اینکه قدر آن اشباع شده یا محدودیتی برای سایرین ایجاد شود.

اما اینکه ماهیت حقوقی فضای سایبر، با تعریف ارائه‌شده چگونه است، نظریه‌های مختلفی بیان شده است که در ذیل بیان می‌کنیم:

الف) ماهیت ملی

برخی معتقدند، فضای سایبر در هر کشوری، همانند قلمرو مادی و فیزیکی آن تلقی می‌شود و جزو خاك آن کشور به حساب می‌آید، بنابراین در حاکمیت و کنترل کامل آن کشور است و هرگونه که خواست، می‌تواند برای کنترل آن، اقدام به وضع مقررات کند. یعنی اگر چه فضای سایبر، قلمروی سراسری در همهٔ نقاط جهان دارد، اما از نظر حاکمیت، در کنترل دولت کشوری است که در آن مورد استفاده قرار می‌گیرد و از این نظر تفاوتی با خاك آن کشور ندارد.

ب) ماهیت غیر ملی

به نظر این گروه، ذات فضای سایبر، به گونه‌ای است که ماهیت فراملی دارد و هیچ کشوری نمی‌تواند آن را کنترل و مدیریت کند، ادعای تشابه و محدودیت قلمرو سایبر به مرزهای واقعی یک کشور، قابلیت تحقق و امکان ندارد. بنابراین، دولت‌ها نمی‌توانند و نباید بر فضای سایبر کنترل و نظارتی داشته باشند، چون در اصل، فضای سایبر در قلمرو حاکمیت ایشان شکل نگرفته است.

ج) ماهیت عام جهانی

این گروه معتقدند، اگرچه فضای سایبر در قلمرو حاکمیت دولت و کشور خاصی نیست و هیچ دولتی نمی‌تواند ادعای حاکمیت مطلق بر آن را داشته باشد، اما نهایتاً در حاکمیت جامعهٔ جهانی است و دولت‌ها، به اتفاق، صاحب صلاحیت‌اند که در مورد آن تصمیم‌گیری کنند. به عبارت دیگر، فضای سایبر، همچون قلمرو دریاهای آزاد است که اگرچه هیچ کشوری توان وضع قانون و اعمال حاکمیت در خصوص آن را ندارد، اما جامعهٔ جهانی برای انتظام‌بخشی به آن، چاره‌ای جز وضع مقررات از طریق کنوانسیون‌ها و پروتکل‌های مختلف ندارد.

## ۳.۳ مصادیق نقض حریم خصوصی در فضای سایبر

در ادامه ۱۳ مصداق قانونی درباره نقض حریم خصوصی را مورد بررسی قرار می‌دهیم:

- دسترسی غیر مجاز به داده‌های رایانه‌ای یا مخابراتی نظیر هک ایمیل یا حساب کاربری.
- شنود غیر مجاز محتوای در حال انتقال در سیستم‌های رایانه‌ای و چت‌های اینترنتی.
- دسترسی غیر مجاز به داده‌های سری در حال انتقال در سیستم‌های رایانه‌ای.
- در دسترس قرار دادن داده‌های سری در حال انتقال در سیستم‌های رایانه‌ای برای اشخاص فاقد صلاحیت.

- نقض تدابیر امنیتی سیستم‌های رایانه‌ای و مخابراتی به قصد دسترسی به داده‌های سری.
- حذف، تخریب و یا غیر قابل پردازش کردن داده‌های دیگری از سیستم‌های رایانه‌ای به طور غیرمجاز.
- انتشار هرزنامه (Spam) و ارسال بدافزار از طریق پست الکترونیک که مدتی است توسط کلاهبرداران سایبر متداول شده را می‌توانیم مصداق این موضوع بدانیم.
- از کار انداختن سیستم‌های رایانه‌ای به طور غیر مجاز و ممانعت از دسترسی اشخاص به پورتال‌ها.
- ممانعت از دسترسی اشخاص مجاز به داده‌ها یا سیستم‌های رایانه‌ای به طور غیرمجاز.
- ربودن داده‌های متعلق به دیگری به طور غیرمجاز.
- هتک حیثیت از طریق انتشار صوت و فیلم تحریف شده دیگری توسط سیستم‌های رایانه‌ای و مخابراتی.
- نشر اکاذیب از طریق سیستم‌های رایانه‌ای یا مخابراتی به قصد تشویش اذهان عمومی.
- فروش، انتشار و یا در دسترس قرار دادن رمز عبور یا هر داده‌ای که امکان دسترسی غیر مجاز به داده‌ها یا سیستم‌های رایانه‌ای دیگران را فراهم کند.
- آموزش نحوه ارتکاب جرایم دسترسی غیرمجاز، شنود غیرمجاز، جاسوسی رایانه‌ای و تخریب و اخلال در داده‌ها یا سیستم‌های رایانه‌ای و مخابراتی. یکی از آشکارترین مصداق‌های نقض حریم خصوصی کاربران در اینترنت به ویژه در شبکه‌های اجتماعی، تبلیغ شیوه‌های هک تلگرام، اینستاگرام و نصب نرم‌افزارهای مربوطه است.

۱۳ موردی که در بالا به آن اشاره کردیم، مصادیق آشکار نقض حریم خصوصی کاربران در فضای سایبری هستند. شما باید در صورت برخورد با چنین مواردی، مراتب را به پلیس سایبر اطلاع دهید. برای حضوری فعال و استفاده فرصت‌آفرین از شبکه‌های اجتماعی داخلی و بین المللی، همانطور که بارها تاکید شده است، باید به حریم خصوصی خود و دیگران احترام گذاشت.

## ۴ نتیجه‌گیری

حریم خصوصی محدوده‌ای است که فرد تمایل دارد از نظارت، کنترل، مشاهده و زیر نظر داشتن توسط سایرین محفوظ بماند. این سایرین دربردارنده‌ی افراد حقیقی و حقوقی می‌باشد. فضای سایبری با توجه به ویژگی‌های ذاتی خود همانند دسترسی بالا، ناشناس بودن و نداشتن محدودیت زمان و مکان امکان نقض حریم خصوصی افراد و شرکت‌ها را فراهم می‌کند، که این امر نیازمند تدوین قوانین و رعایت پروتکل‌های خاصی می‌باشد. در این پژوهش سعی شد تا مفهوم حریم خصوصی در فضای سایبری مورد بررسی قرار گیرد و مهم‌ترین مصادیق نقض آن هم بیان گردد. با توجه به رشد فزاینده‌ی فضای سایبری در کشور، ما نیازمند تدوین قوانین و

پروتکل‌های مختص این فضای جدید می‌باشیم تا بتوانیم حریم خصوصی افراد حقیقی و حقوقی را محترم شماریم و از نقض آن جلوگیری کنیم.

## مراجع

[1] Seyyed Ahmad Khalili Juo Lorestani, (2017). Revisiting the Challenges and Threats of Cyberspace on Sustainable Security, , 14(42), 147-176. magiran.com/p1809682

[2] Ali Sadeghi, Zeinab Ameri, (2017). Social Networks and Social Damage Case Study: Public Safety., Journal of survey in teaching humanities, 2(5), 51-65. magiran.com/p2146143.

[3] M. Janparvar, T. Heidari Moselo, (2011). Pathology of cyberspace on social security, Order & Security Research Journal, 4(3), 141. magiran.com/p1055026.

[4] Yunes Fathi , Kheyrollah Shahmoradi, (2017). Area and territory of privacy in virtual space, The Judiciary Law Journal, 81(99), 227-250. magiran.com/p1791388.

[5] Zanettin, F. and C. Rundle (2022). The Routledge Handbook of Translation and Methodology.

[6] Ottis, R; Lorents, P. (2010). Cyberspace: Definition and Implications. Proceedings of the 5th International Conference on Information Warfare and Security: 5th International Conference on Information Warfare and Security, Dayton, Ohio, USA, 08-09.04.2010. Ed. Dr Leigh Armistead. Reading, UK: Academic Conferences Limited, 267–270.

[7] Jafari, Mohammad and Hashmati, Hamed, 2018, Investigating the impact of the Internet of Things, big data and artificial intelligence on the development of a smart city, the 8th International Conference on Information Technology, Computer and Telecommunications, https://civilica.com/doc/1010129M.

[8] Hamidreza Afshar, Seyyed Shamsoddin Hoseini, Mohammadreza Movahedisefat, (2020). Investigating Opportunities and Threats of Adoption and Development of Blockchain Technology in I.R.of Iran, National Security, 10(36), 307-348. magiran.com/p2158554.