

# تحول مفهوم پنهان کاری: از ویژگی هستی‌شناختی تا ابزاری برای فعالیت اطلاعاتی

تاریخ دریافت: ۱۳۹۰/۱۲/۲۱

تاریخ پذیرش: ۱۳۹۱/۳/۱۵

غلامرضا سالار کیا\*

## چکیده

در مقاله پیش رو، پس از آنکه دلایل پنهان کاری در دولت‌ها، به ویژه در سازمان‌های اطلاعاتی تبیین می‌شود، این سؤال مطرح می‌گردد که در حال حاضر، پنهان کاری چه بخشی از هویت اطلاعات را به خود اختصاص داده و چه جایگاهی در اطلاعات دارد؟ نویسنده دو فرضیه رقیب را در پاسخ به این سؤال طرح می‌نماید. فرضیه اصلی، پنهان کاری را یکی از ویژگی‌های هستی‌شناختی اطلاعات می‌داند و فرضیه رقیب آن را ابزاری برای کار اطلاعاتی معرفی می‌کند. پس از بررسی دو ادعای فوق، نگارنده در آخر نتیجه‌گیری می‌نماید که پنهان کاری اساساً بخشی جدانشدنی از هویت اطلاعات است و ریشه‌ای هستی‌شناختی در آن دارد.

**کلیدواژه‌ها:** پنهان کاری، پنهان‌بودگی، شفافیت، طبقه‌بندی، حیطه‌بندی، ویژگی‌های اطلاعات، نظارت بر اطلاعات، سوءاستفاده از اطلاعات

\* دانشجوی کارشناسی ارشد مدیریت فناوری اطلاعات در دانشگاه آزاد اسلامی

فصلنامه مطالعات راهبردی • سال پانزدهم • شماره دوم • تابستان ۱۳۹۱ • شماره مسلسل ۵۶

## مقدمه

حفظ اسرار و توسل به پنهان‌کاری، سکه رایج همه حکومت‌ها در همه اشکال و همه دوره‌های تاریخی بوده است. این شیوه در همه حکومت‌ها، از دولت‌های دیکتاتوری و اقتدارگرا تا دولت‌های مبتنی بر مردم‌سالاری، امری رایج است. حکومت‌های دیکتاتوری از پنهان‌کاری در حفظ پایه‌های نظام نامشروع خود به صورت مستمر سود گرفته و به آن متوسلند. در این نوع نظام‌ها، اغلب فشار فزاینده‌ای برای پنهان‌کردن حقایق و تحریف واقعیات وجود دارد، اما تمایل به پنهان‌کاری در نظام‌های مردم‌سالار، بسته به شرایط و وضعیت تغییر می‌نماید. برای مثال، هنگامی که امنیت ملی کشوری دست‌خوش بحران می‌گردد، ساختار نظام سیاسی به سوی حفظ اسرار و ایجاد محدودیت در دسترسی به اخبار حساس متمایل می‌گردد که بروز چنین وضعیتی از سوی مردم نیز با اعتمادی که به ساختار منتخب خود دارند، پذیرفته می‌شود. در مقابل، هنگام وجود آرامش در تمامی شاخص‌های مادی و معنایی امنیت ملی، مردم با مطالبه حقوق خود، خواهان دسترسی معقول به اخبار و اطلاعات در مورد کارکردهای نظام سیاسی منتخب خود بدون سانسور دولتی هستند. با این همه، در نظام‌های مردم‌سالار نیز مکرر دیده می‌شود که با دست‌آویز قراردادن امنیت ملی، منطق نهفته در مردم‌سالاری قربانی مطامع گروه حاکم می‌گردد و آزادی‌های اساسی در بازی پنهان‌کاری به خطر می‌افتد.<sup>۱</sup>

در ساختار حکومت، اطلاعات به عنوان یکی از مهم‌ترین ابزارهای سیاست‌گذاری و متغیری وابسته به آن، با توجه به ویژگی‌های منحصر به فرد خود در میان دیگر ساختارهای نظام سیاسی، نقش تأثیرگذاری بازی می‌نماید (میرمحمدی: ۱۳۹۰). در عین حال، بایستی توجه داشت، اطلاعات حداقل به دو دلیل با سایر کارکردهای حکومتی تفاوت دارد. اول اینکه بیش‌تر جنبه‌های آن پنهان است. حیات اطلاعات به این دلیل است که حکومت‌ها به دنبال پنهان‌نمودن برخی از اطلاعات خود از سایر حکومت‌ها هستند که آن حکومت‌ها نیز به دنبال کشف اطلاعات پنهان به وسیله ابزاری هستند که خودشان میل دارند آن ابزارها را پنهان نگاه دارند. تمامی این پنهان‌کاری‌ها باعث

۱. نمونه بارز آن، اطلاعات تحریف‌شده سازمان‌های اطلاعاتی انگلیس و ایالات متحده آمریکا و رژیم اشغال‌گر قدس پیش از حمله به عراق در سال ۲۰۰۳ است. در ایالات متحده و بریتانیا که خود را مهد دموکراسی می‌دانند، اجازه داده شد اطلاعات به ابزار تأثیرگذاری سیاسی و تفسیر سوگیرانه در لوای پنهان‌کاری تبدیل شود.

می‌شود کارشناسان سیاسی باور داشته باشند که موضوعاتی وجود دارند که در مورد آنها نمی‌توانند چیزی بنویسند و یا اینکه اطلاعات کافی در مورد آنها وجود ندارد. تفاوت دوم، فعالیت است که اطلاعات بدان دست می‌یازد؛ فعالیت‌هایی که انجام آن تضمین‌کننده امنیت ملی کشور است، ولی از نظر کشور هدف، غیرقانونی است؛ اقداماتی نظیر شنود، جاسوسی و اقدام پنهان (لوونتال، ۱۳۸۷: ۱۳). به همین دلیل چنین فعالیت‌هایی از افکار عمومی مخفی نگاه داشته می‌شود و مهم‌ترین متغیر بازی‌گر در پنهان‌کاری نظام به شمار می‌آید. برای مثال، در اغلب دوران قرن بیستم، جامعه اطلاعاتی انگلیس مرد نامریی دولت، دولتی درون دولت و موجودیتی که هرگز سؤالی درباره آن در پارلمان مطرح نمی‌شد، بوده است (Moran, June ۲۰۱۱: ۳۵). البته، هر دو دلیل ذکرشده، تناقض‌نمایی جدی با اصول مردم‌سالاری را به نمایش می‌گذارند. این موضوعی است که به طور جدی از نیمه دوم دهه هفتاد میلادی پا به عرصه مباحثات سیاسی گذاشته و ریشه آن افشاگری‌های عمومی بوده است<sup>۱</sup>.

پنهان‌کاری و محرمانگی، اساس فعالیت اطلاعاتی است و جوهر این کار به شمار می‌رود. این ویژگی به طور مشخص در بسیاری از تعاریف اطلاعات گنجانده شده و در معدود تعاریفی که لفظ پنهان‌کاری در آنها مورد اغماض قرار گرفته است، ویژگی پنهان‌کاری، پیش‌فرض این حرفه انگاشته شده است (شولسکی، ۱۳۸۱: ۱۱ و لوونتال، ۱۳۸۷: ۳۴۵ و Kimbal, ۲۰۰۱). از همین رو، اکثر مأموران اطلاعاتی افشاشده افرادی هستند که یا از این جهان رخت برپسته‌اند یا از سازمان خود بریده‌اند و یا نویسندگان خاطرات اطلاعاتی هستند.

با این وجود، طی سال‌های اخیر و با گسترش ارزش‌های مردم‌سالارانه، بسیاری از نخبگان سیاسی و دانشگاهی و به طور کلی جامعه مدنی، خواستار کاهش پنهان‌کاری حکومت در ابعاد مختلف به ویژه درباره عملکرد و اقدامات سرویس‌های اطلاعاتی بوده‌اند. این شفافیت‌طلبی به طور

---

۱. برای مثال در ایالات متحده آمریکا کمیته‌های تحقیقات چرچ و پایک در سال‌های ۱۹۷۵ و ۱۹۷۶ به بررسی سوءاستفاده سازمان اطلاعات مرکزی از اطلاعات پرداختند که اولی در پی مقاله‌های سیمور هرش در نیویورک تایمز در دسامبر سال ۱۹۷۴ آغاز به تفحص کرد. (Warner & McDonald, ۲۰۰۵)

همچنین، در کانادا، کمیسیون مک‌دونالد به بررسی تخلفات سرویس امنیتی پلیس سوار این کشور پرداخت. این روند در استرالیا در طول دهه هشتاد به وقوع پیوست. (Davies, ۲۰۰۴, Weller, ۱۹۹۴: ۴۸۴-۵۰۳)

خاص اطلاعات را در معرض نوعی تناقض نما قرار داده است: از یک طرف، اگر پنهان‌کاری جوهر اطلاعات باشد، هر نوع شفاف‌سازی تهدیدی وجودی علیه آن خواهد بود، اما از طرف دیگر، اگر آن را ابزاری برای کار اطلاعاتی بپنداریم، دخل و تصرف در آن امری قابل پذیرش خواهد بود. سؤالی که در اینجا مطرح می‌شود این است که امروزه پنهان‌کاری چه بخشی از هویت اطلاعات را به خود اختصاص داده است؟ در نوشتار پیش رو، به دنبال بررسی دو فرضیه رقیب در پاسخ به سؤال فوق می‌باشیم. فرضیه اصلی، پنهان‌کاری را هم‌چنان ویژگی هستی‌شناختی اطلاعات<sup>۱</sup> می‌داند، در حالی که فرضیه رقیب مدعی است در عصر حاضر و به عبارت دقیق‌تر در قرن ۲۱ و در سایه افزایش مردم‌سالاری، انفجار اطلاعات و رشد و گسترش فن‌آوری‌های ارتباطی، پنهان‌کاری ویژگی ابزاری اطلاعات به شمار می‌رود. در ادامه، ابتدا به بررسی پنهان‌کاری به عنوان ویژگی هستی‌شناختی اطلاعات می‌پردازیم. سپس، پیش از آنکه فرضیه رقیب مورد بررسی قرار گیرد، تناقض‌نمای پنهان‌کاری و شفافیت در جوامع مردم‌سالار مطالعه شده و بحث برای بررسی فرضیه رقیب آماده خواهد شد.

### الف. پنهان‌کاری: ویژگی هستی‌شناختی اطلاعات

پنهان‌کاری، اطلاعات را پدیده‌ای ویژه می‌کند. اینکه دیگران اطلاعات مهمی را از رقبای پنهان می‌کنند؛ اینکه رقبای نیاز به دانستن برخی اطلاعات خاص از یکدیگر دارند و می‌خواهند نیازهایشان را پنهان نگاه دارند و اینکه سازمان‌های اطلاعاتی دارای ابزاری هستند که می‌توانند آن اطلاعات خاص را به دست بیاورند و همین‌طور می‌خواهند آن ابزار را پنهان بدارند و در آخر اینکه، علاقه دارند در برخی موارد نقش و تأثیرشان در موضوعی از دید رقبای یا افکار عمومی پنهان باقی بماند، همه و همه از دلایل اصلی وجود سرویس‌های اطلاعاتی می‌باشند (لونتال، ۱۳۸۷: ۱۹). بنابراین، اطلاعات به درستی درختی است که در تاریکی می‌روید

(Efraim Halevy in Shpiro, ۲۰۰۱, ۴۵۸).

۱. توجه نمایید در اینجا اطلاعات به معنای چهارگانه آن یعنی فعالیت، سازمان، فرآیند و محصول می‌باشد (ر.

ک. شولسکی، ۱۳۸۱)

مایکل هرمن سه دلیل برای پنهان کاری در فعالیتهای اطلاعاتی مطرح می‌نماید. در زمان جنگ، پنهان کاری به اجرا گذاشته می‌شود که هدف آن حفاظت از طرح‌های حساس در برابر افشاشدن است (Herman, ۱۹۹۶: ۸۸). نباید فراموش کرد که همه جنگ‌ها بر فریب‌کاری استوارند (وینر و همکاران، ۱۳۷۶: ۱۴).

دومین دلیلی که هرمن معرفی می‌کند، به بیان ریچارد پوزنر، عنوان "عامل خجالت" را یدک می‌کشد (Posner, ۲۰۰۶: ۱۸۷). امنیت ملی گاهی اوقات مستلزم فعالیت‌هایی است که در بهترین حالت می‌تواند فعالیت‌هایی سؤال‌برانگیز قلمداد شود (Herman, ۱۹۹۶: ۸۹). در این حالت، همواره این خطر وجود دارد که در صورت افشاشدن فعالیت اطلاعاتی، روابط خارجی به مخاطره بیافتد. بنابراین، برای جلوگیری از این خطر، دولت‌ها معمولاً به انکار موجه (قابل قبول)<sup>۲</sup> متوسل می‌شوند. انکار قابل قبول به معنای انکار آگاهی از به انجام رسیدن فعالیت اطلاعاتی ویژه است. بدیهی است، انکار قابل قبول به پنهان نگه‌داشتن اقدام اطلاعاتی بستگی دارد. در غیر این صورت، انکار قابل توجیه نخواهد بود (لوونتال، ۱۳۸۷: ۲۲۶ و ۱۴: ۲۰۰۹: Chinen).

حفاظت از منابع و روش‌های جمع‌آوری و تحلیل اطلاعات، سومین و مهم‌ترین دلیل پنهان کاری است. منابع و شگردهای اطلاعات می‌بایست مخفی نگاه داشته شود، چرا که در غیر این صورت توسط ضد اقدامات دچار آسیب خواهد شد (Herman, ۱۹۹۶: ۸۹). همچنین، ممکن است در صورت عدم توجه به پنهان کاری، عوامل و منابع اطلاعاتی، دستگیر شده یا اعدام گردند، رمزهای ارتباطی تغییر یابند و یا با استفاده از ضد اقدامات نظیر عدم استفاده از

#### ۱. Embarrassment Factor

#### ۲. Plausible Deniability

یک نمونه موفق از انکار قابل قبول در ایالات متحده به ماجرای ایران‌کنتراباز می‌گردد که ریگان از آن سود جست. جالب است بدانید، هنگامی که از الیور نورث در نوامبر ۱۹۸۷ در جلسه تحقیق کنگره درباره خردکردن مدارک ماجرا توسط وی سؤال می‌شود، او پاسخ می‌دهد، دلیل خردکردن مدارک و دلیل اینکه دولت ایالات متحده آمریکا به من دستگاه خردکن داد (و من خودم آن را نخریده‌ام) این بود که مدارکی را که دیگر مصرفی نداشت و یا نمی‌بایست افشا گردد، از بین برده شود. (جانسون، ۱۳۹۰: ۳۶۴)

نمونه ناموفق از انکار قابل قبول به ماجرای جاسوسی جانانان پولارد، تحلیل‌گر اطلاعات نیروی دریایی ایالات متحده که برای سازمان اطلاعاتی لاکام رژیم اشغال‌گر قدس اقدام به جاسوسی برای این رژیم نمود، باز می‌گردد.

موبایل یا پست الکترونیکی، هدف از منظر جمع‌آوری فنی و علائم به دور افتد و ناپدید شود. حتی این امکان وجود دارد که منابع توسط حریف تحت کنترل قرار گرفته و اطلاعات فریب انتشار یابد، ممکن است جاسوسان ترغیب به دوبل شدن شوند یا پیام‌های غیرواقعی در انتقال پیام‌های رمز شده به منظور فریب جای گیرند.<sup>۱</sup> به همین دلایل است که حتی موفقیت‌های سازمان اطلاعاتی بایستی پنهان باقی بماند تا تداوم آنها تضمین شود.

برای حفاظت از منابع و شگردها، دیوان‌سالاری پیچیده‌ای در سازمان‌های اطلاعاتی ایجاد می‌گردد که وظیفه آن با توجه به حساسیت موضوع، تصمیم‌گیری درباره این است که چه

۱. برای مثال در سال ۱۹۲۷ دولت سر استانی بالدوین در انگلستان، برای توجیه حمله خود به انجمن تعاونی روس‌ها یا همان هیأت اعزامی تجاری این کشور که همانند هیأت‌های اعزامی تجاری روسی قبلی از پوشش دیپلماتیک برای فعالیت‌های جاسوسی خود استفاده می‌کردند و قطع روابط دیپلماتیک با اتحاد جماهیر شوروی، اعلام کرد قادر به خواندن رمزهای روسی است. این کار بدون سابقه نبود و پیش از آن نیز دولت بریتانیا محتوای مطالب استراق سمع شده از روس‌ها را از سال ۱۹۲۰ تا ۱۹۲۳ برای اعتراض به حمایت مسکو از گروه‌های انقلابی و مخالف در بریتانیا و امپراتوری آن منتشر ساخته بود. نفع سیاسی بریتانیا از این اعلامیه این بود که به جای متهم شدن به نقض آشکار قانون بین‌الملل، درستی کار آن مورد تأیید قرار گرفت. اما از نظر اطلاعاتی هزینه اصلی این کار این بود که روس‌ها بلافاصله کدهای خود را با کدهای جدید غیرقابل شکستن که رمزخوان‌های بریتانیایی قادر به شکستن و خواندن آنها نبودند، تغییر دهند. نتیجه این شد که انگلیسی‌ها برای سال‌ها دیگر نتوانستند از ارتباطات روس‌ها آگاهی یابند. این حادثه که کریستوفر اندرو از آن به عنوان فاجعه سیگنیت ۱۹۲۷ نام برده است، این تفکر را در اذهان نسل‌هایی از مأموران اطلاعاتی انگلیس تقویت کرد که شفاف‌سازی سیاسی در زمینه اطلاعات چقدر برای عملیات‌های اطلاعاتی تهدیدآمیز است. هم‌چنین عقاید آنها را با این تجربه فراموش‌نشده مینی بر پنهان‌کاری استحکام بخشید. (Davies, ۲۰۰۴)

به مثال دیگری توجه کنید: یکی از ابزارهای موفق رژیم اشغال‌گر قدس بر اعراب در جنگ شش‌روزه سال ۱۹۶۷، جمع‌آوری اطلاعات مخابراتی بود. در این میان، یکی از شنودهای مهم به انجام رسیده، ردیابی و ضبط گفت‌وگوی تلفنی میان جمال عبدالناصر و شاه حسین بود. پخش مفاد این گفت‌وگو دو روز بعد، تأثیر سیاسی زیادی برجای گذاشت و اثر عظیمی در روحیه سربازان اسرائیلی داشت. با این همه، به گفته یکی از افسران اطلاعاتی این رژیم، پخش گفت‌وگوی مزبور به بهای از دست رفتن شصت درصد از توانایی‌های ردیابی اسرائیل ختم شد (بلک و موریس، ۱۳۷۵: ۲۹۱).

برای تبیین بیشتر، پیش از حمله غافل‌گیرانه ژاپنی‌ها به پرل‌هاربر در جنگ جهانی دوم، رمزهای دیپلماتیک آنان توسط آمریکایی‌ها رمزگشایی شده بود، پنهان‌کاری در جهت حفاظت از منابع و شگردها یکی از دلایل عدم به اشتراک گذاشتن اطلاعات مرتبط با حمله قریب‌الوقوع و نهایتاً یکی از دلایل بروز غافل‌گیری استراتژیک مزبور بود (Chinen, ۲۰۰۹: ۲۷).

اخباری می‌بایست پنهان باقی بمانند، درجه طبقه‌بندی آنها چیست و چه افرادی به کدام نوع از اخبار می‌توانند دسترسی داشته باشند، مشخص می‌گردد (لوونتال، ۱۳۸۷: ۱۱۰). طبقه‌بندی و حیطة‌بندی، دو نمونه از تمهیداتی است که به منظور حفظ اسرار سازمانی انجام می‌شود.<sup>۱</sup> در واقع، استمرار توانایی سازمان اطلاعاتی در کسب اطلاعات مورد نیاز بستگی تام به حفظ اسرار دارد (ترنر، ۱۳۸۷: ۶۲)

اطلاعات به پنج روش کلی جمع‌آوری می‌شوند. این روش‌ها عبارتند از: اطلاعات آشکار، اطلاعات انسانی، اطلاعات علائم، اطلاعات فضای زمین و اطلاعات اندازه‌گیری و تعیین کیفیت (۱۲: ۲۰۰۹، ODNI). هر کدام از این روش‌ها شامل فن‌آوری‌های متعدد و متفاوت و فعالیت‌هایی است که جزئیات آن از منظر عمومی پنهان نگاه داشته می‌شود. این توانایی‌ها ممکن است توسط رقبا و حریفان ارزیابی و حدس زده شود. برای مثال، در خصوص توانایی‌های کشورهای عضو اشلون و در رأس آنها ایالات متحده در ره‌گیری ارتباطات الکترونیکی، برآوردهایی توسط منابع متعدد وجود دارد، اما چنین برآوردهایی به منزله افشای روش‌ها و شگردهای اطلاعاتی نیست.

در سازمان‌های اطلاعاتی نیاز به پنهان‌کاری به سطح آسیب‌پذیری منابع و شگردها در مقابل ضد اقدامات حریف بستگی دارد. البته، غیرمحمتمل به نظر می‌رسد که منبعی در برابر افشاشدن به صورت کامل آسیب‌پذیری نداشته باشد. با این همه، آنگونه که هرمن ادعا می‌نماید، «شکنندگی<sup>۲</sup>» منابع هم سطوح متفاوتی دارد. افشاشدن اینکه رمزهای ارتباطی توسط رقبا شکسته شده است، باعث می‌گردد اقدامات متقابل برای تغییر رمزها به انجام رسد. مجموعه اطلاعات جمع‌آوری‌شده توسط روش جمع‌آوری فضای زمین که اطلاعات تصویری نیز زیرمجموعه آن است، از

---

۱. منظور از طبقه‌بندی، اقداماتی است که بر اساس آن اطلاعات و اسناد حسب اهمیتی که برای نظام اداری دارند، با درجات مختلف از هم متمایز می‌گردند (تبصره ۵ بند ۱ مصوبه شورای عالی امنیت ملی ۸۷/۶/۳۱ به نقل از ابوالحسنی، ۱۳۸۵: ۷).

حیطة‌بندی عبارت است از تعیین محدودیت‌های حفاظتی در گردش و نگاه‌داری اسناد و مشخص نمودن نحوه زمان واگذاری اطلاعات موجود در یک سند طبقه‌بندی‌شده به اشخاصی که صلاحیت دسترسی به مطالب آن را دارند (ابوالحسنی، ۱۳۸۵: ۴).

شکندگی کم‌تری برخوردار است. البته، با این نوع جمع‌آوری نیز می‌توان با استفاده از استتار یا انواع پدافند غیرعامل مقابله نمود. با این حال، در مقیاس‌هایی که تحولاتی غیرقابل انکار در حال وقوع است، نظیر جابه‌جایی نیروها، اقدامات متقابل نتیجه مفیدی نخواهد داشت. ترورتون معتقد است پیشرفت‌های حاصل‌شده در طول زمان بر روی آسیب‌پذیری تأثیر داشته است. برای مثال، در خلال جنگ سرد، اطلاعات به تعداد اندکی از روش‌های جمع‌آوری متکی بود که در این حالت، افشاشدن هر کدام نه تنها قابلیت بالای آن روش و مزیت پیش‌دستی او را تنزل می‌داد، بلکه این تیغ دو لبه، برنده دست صاحب اولیه آن می‌شد. در حال حاضر، تنوع روش‌های جمع‌آوری، اهداف متعدد و فراوان و اخبار بسیار زیاد، آسیب‌پذیری‌های منابع و روش‌ها را به اندازه قابل توجهی کاهش داده است (Treverton, ۲۰۰۵: ۲۸).

در اثر افشاشدن متعدد شگردهاست که تمامی رقبا این نکته را که تمامی ارتباطات الکترونیکی توسط حریفان ره‌گیری می‌شود، به عنوان یکی از پیش‌فرض‌های خود قرار می‌دهند؛ رقبا تمام تلاش‌های ممکن برای شکستن رمزهای ارتباطی را در دستور کار قرار می‌دهند؛ تمامی فعالیت‌های فیزیکی توسط جمع‌آوری‌کنندگان فضای زمین پی‌گیری می‌شود؛ هرگونه نقل و انتقال الکترونیکی اطلاعات قابل ردیابی خواهد بود و در آخر، احتمال اینکه سازمان‌های اطلاعاتی مورد رخنه قرار بگیرند، وجود دارد.

بروس، دانش و پیش‌شناخت به همراه دو مؤلفه جاسوسی و پنهان‌کاری را پایدارترین ویژگی حرفه اطلاعات بر می‌شمارد (Bruce, ۲۰۰۸). خلاصه آنکه، «جاسوسی به همراه پنهان‌کاری هستی یافته است. پنهان‌کاری همواره همراه بشر بوده است. چه آن زمان که انسان‌ها حیوانات را شکار می‌کرده‌اند، چه اکنون که حکومت‌ها از فن‌آوری‌های پیشرفته‌شان محافظت می‌کنند یا بعضاً به قصد سلطه‌جویی و غالباً به منظور دفاع در دیگر کشورها نفوذ می‌کنند» (پیر آل، ۱۳۷۰).

### ب. پنهان‌کاری و شفافیت: تناقض‌نمای نظام‌های مردم‌سالار

میان کار اطلاعاتی که پنهان‌کاری بخشی ضروری از آن است و مردم‌سالاری که ضروری‌ترین عنصر آن پاسخ‌گویی است، تناقض‌نمایی وجود دارد که کنترل اثربخش نهادهای نظارتی (که به طور عمده غیراطلاعاتی‌اند) بر روی فعالیت‌های اطلاعاتی را مخدوش می‌نماید.



پنهان کاری شکلی از قاعده حکومتی است که مردم را از داشتن آنچه منطقیاً منفعتمعمومی می‌باشد، محروم می‌نماید. برای مثال، رئیس پیشین سازمان اطلاعات مرکزی، جرج تنت برخی اخبار اطلاعاتی را که حتی مورد نیاز و استفاده اعضای کمیته بررسی اطلاعاتی مشترک بود از طبقه‌بندی خارج نکرده و در اختیار این کمیته که در حال تحقیق و تفحص از حملات ۱۱ سپتامبر بودند، قرار نداد (ترنر، ۱۳۸۸: ۱۵۶). این اولین یا آخرین باری نیست که سیا به سوءاستفاده از قاعده پنهان کاری می‌پردازد. رفتارهای متعدد از این دست توسط سیا باعث گردید که صفت «پیل وحشی»<sup>۱</sup> در دره ۷۰ به این سازمان اطلاق شود (Born, ۲۰۰۸).

مردم‌سالاری نیازمند شفافیت است تا رهبران را در مقابل تصمیمات سیاسی خود پاسخ‌گو نگاه دارد، با این حال برخی سیاست‌ها و فرایندهای سیاسی در صورت افشاشدن تأثیرگذاری خود را از دست می‌دهند و یا شاید به طور کلی قابل اجرا نباشند (Tompson, ۱۹۹۹: ۱۸۲).

ضرورت حفظ اسرار جزئیات عملیات‌های اطلاعاتی میان محدودترین افراد ممکن، می‌تواند مشکلات و انحراف‌های خسارت‌آوری را به مردم‌سالاری و امنیت ملی کشور وارد آورد. پنهان کردن اقدامات غیرمجاز، سوءاستفاده‌های احتمالی از قدرت اطلاعات، و مخفی کردن ناکارآمدی‌ها، از جمله مشکلات پنهان کاری است. اطلاعات در لوای پنهان کاری از یک عیب ذاتی رنج می‌برد و آن اینکه همواره در معرض پوچی و یاه‌بافی قرار دارد (آستانا، ۱۳۸۸: ۱۸۱).

همچنین، تجربه نشان داده است پنهان کاری بیش از حد و کارآمدی سازمان اطلاعاتی در تضاد با یکدیگرند. اکثر سازمان‌های اطلاعاتی به مشکل وسواس در پنهان کاری دچارند، یکی از جالب‌ترین مورد، اصرار سیا بر این نکته بود که شش سند مربوط به سال ۱۹۱۷ که شامل فرمول‌هایی برای جوهر نامرئی می‌شد باید محرمانه بماند چرا که افشای آنها در جنگ علیه تروریسم اخلال ایجاد می‌کند (Pateman, Roy, ۲۰۰۳, ۱۲۰ from Times, March ۲۷, ۲۰۰۲).

در بستر سازمان اطلاعاتی، پنهان کاری باعث محدودشدن دسترسی تحلیل‌گران به اخبار و داده‌ها و منابعی می‌شود که ممکن است برای تولید تحلیل‌های اطلاعاتی امری ضروری محسوب شود. برای مثال، پیش از آغاز جنگ یوم کیپور (رمضان) سال ۱۹۷۳، موساد از معرفی منبع به کلی سری خود، که هشدار حمله قریب‌الوقوع مصر را به رژیم اشغال‌گر قدس اعلام

کرده بود، به سازمان اطلاعات دفاعی (امان) که مسئولیت تولید تحلیل‌های اطلاعاتی و جلوگیری از غافل‌گیری استراتژیک در این رژیم را بر عهده دارد، به دلیل حفاظت از منبع خود اجتناب ورزید. این امر در کنار دیگر عوامل باعث شد خبر نادیده گرفته شود و یکی از غافل‌گیری‌های بزرگ اطلاعاتی که می‌توانست رژیم اشغال‌گر قدس را تا آستانه فروپاشی پیش برد، به وقوع بپیوندد (کاتز، ۱۳۷۵: ۴۵۰-۴۲۰).

محدود کردن دسترسی به اخبار، ایجاد سازمان‌هایی که در رقابت با یکدیگر محصولات اطلاعاتی تولید کنند را کاهش داده و در نتیجه، رقابت برای تولید محصولات باکیفیت را از بین می‌برد. به همین دلیل بود که کمیسیون آگرانات که وظیفه تحقیق درباره جنگ یوم کیپور را بر عهده داشت، پیشنهاد می‌نماید که واحدهای تحلیلی در کنار امان در دیگر سازمان‌های اطلاعاتی رژیم اشغال‌گر قدس تأسیس شود و این کار، تولید تحلیل‌های اطلاعاتی را از انحصار امان، حداقل در شکل قانونی خارج ساخت. «پنهان‌کاری و انزوای بیش از حد، دشمن اطلاعات بهنگام و موثق و دقیق است» (ترورتن به نقل از لاکوئر، ۱۳۸۱: ۴۸).

منتقدان پنهان‌کاری با پیروی از ماکس وبر، پنهان‌کاری را استراتژی قدرت یا بدتر از آن، نوعی وجدان سیاسی بد، نوعی تمایل به دفاع از تقلب‌ها و حتی سوءاستفاده از قدرت می‌نامند. در برخی دولت‌ها نظیر انگلیس (بر خلاف آمریکا) که پنهان‌کاری ریشه‌ای عمیق در آنها دارد، نیاز دولت به پنهان‌کاری را اساساً نشأت گرفته از نیاز پارلمانی و وزارتی در کنترل مستخدمین کشوری می‌دانند، بدین ترتیب که مستخدمین کشوری با اجبار به پنهان‌کاری دیگر نمی‌توانند از وزیرشان انتقاد کنند یا اقتدار او را به چالش بکشند. این کار سبب می‌شود مستخدمین کشوری نتوانند به عنوان قدرت ذی‌نفوذ بر روی مجلس یا افکار عمومی تأثیر گذارند. تأثیر این کار فرمان‌پذیری مطلق مستخدمین کشوری از وزیر مربوطه و پارلمانی است که وزرا را انتخاب کرده است (Davies, ۲۰۰۴).

سوءاستفاده از اطلاعات می‌تواند در شکل‌های زیر تجلی یابد:

- سوءاستفاده از سرویس اطلاعاتی برای کسب منافع سیاسی یا شخصی. برای مثال، جاسوسی درباره گروه‌های سیاسی مخالف و رقیب به نفع گروه خاص؛

- دست‌کاری سیاسی در اطلاعات در جهت تأمین نظرات و منافع گروه سیاسی بخصوص؛

- انکار قابل قبول در موارد اقدامات غیرقانونی از منظر قوانین داخلی؛<sup>۱</sup>

در مقام مقایسه میان انگلیس و ایالات متحده و بالطبع کشورهای الگوگرفته از این ساختارهای حکومتی، حفظ پنهان کاری اطلاعاتی در بریتانیا، اصولاً ناشی از کنترل وزارتی بوده و توسط نگرانی‌های موجود در زمینه امنیت عملیاتی تشدید شده است. این در حالی است که در ایالات متحده، تقسیم قدرت باعث شفاف‌سازی بیش‌تری در امر اطلاعات شده است. این شفاف‌سازی نشأت‌گرفته از رقابت قوای مجریه و مقننه برای کسب قدرت و نفوذ بیش‌تر از یک سو و سازمان‌های اطلاعاتی دولتی و ادارات از سوی دیگر می‌باشد. به گفته کن رابرتسون<sup>۲</sup>، کارشناس اطلاعاتی، ساختارهای سیاسی آمریکایی نسبت به ساختارهای انگلیسی محیط رقابتی‌تری را به وجود می‌آورند و در چنین محیطی است که ادارات برای جذب بودجه، نفوذ پرسنل و اعتبار بیش‌تر به افشای اطلاعات می‌پردازند. این‌گونه است که مستخدمین کشوری در ایالات متحده می‌توانند توسط ارتباط با نمایندگان منتخب خود به کانون قدرت و نفوذ نزدیک شوند، چیزی که مستخدمین کشوری در بریتانیا با الزام به پنهان کاری قادر به انجام آن نیستند. به همین خاطر است که فرصت ارائه دیدگاه‌های جایگزین و افشای اطلاعات در ایالات متحده نسبت به بریتانیا تهدید کمتری ارزیابی می‌شود، چرا که چنین کاری در بریتانیا نه تنها تهدیدکننده امنیت است، بلکه تهدیدکننده ساختار سیاسی، هماهنگی و کنترل نیز به حساب می‌آید. به عبارت دیگر، پنهان کاری رسمی در بریتانیا، الزامی کارآمد برای کابینه و برای یکپارچگی قدرت است. آنچه رابرتسون به آن اشاره کرده و با توجه به نیاز تمام حکومت‌ها به

۱. به چند نمونه از سوءاستفاده از اطلاعات توجه کنید:

مارگارت تاچر، کمیته مشترک اطلاعات را تهدید کرده بود تا نظر او را درباره دنیا بدون دلیل قانع‌کننده‌ای بپذیرند. رابرت گیتس، معاون وقت سیا (که بعدها رئیس سیا شد) از سوی مسئولان به دست‌کاری در ارزیابی‌های سیا برای تطبیق آنها با اولویت‌های کاخ سفید در زمان ریگان متهم شد. حتی رئیس سیا در آن زمان، ویلیام کیسی متهم گردید که تحلیل‌گران و جمع‌آوری‌کنندگان اطلاعات خود را برای تولید اطلاعات منطبق بر سیاست کاخ سفید تحت فشار قرار داده است (Davies, ۲۰۰۴).

۲. Ken Robertson

پنهان‌کاری نمی‌توان آن را نادیده گرفت، این است که حلقه پنهان‌کاری به افراد داخل آن، آزادی بررسی گزینه‌ها و مسائلی را می‌دهد که نمی‌توان آنها را به شکل عمومی بررسی کرد. «کشاندن اطلاعات به مباحث سیاسی روز» به اعتقاد رابرتسون، «سیاسی‌شدن سرویس‌های اطلاعاتی را که نتیجه مطلوبی ندارد، به همراه دارد و می‌تواند به تحت فشار قرار گرفتن آنها از سوی بازیگران سیاسی برای تولید اطلاعاتی که می‌تواند به نتایج مورد دلخواه آنها بیانجامد، منجر شود». بحث عمومی درباره موضوعات حساس سیاست خارجی می‌تواند عکس‌العمل‌های سیاسی و فشارهای خارجی‌ای به همراه داشته باشد که مانع رسیدن به سیاست جامع و تأثیرگذار برای بررسی تمام گزینه‌های موجود گردد. این فشارها الزاماً نباید گسترده باشند، بلکه حتی فشارهای گروه‌های جانبی و خاص ذی‌نفوذ از طریق مطبوعات یا نامه‌پراکنی می‌تواند فشار زیادی را بر تصمیم‌گیران و مشاوران آنان وارد سازد. چنین کاری حتی می‌تواند پیامدهای سیاسی را به همراه داشته باشد، چرا که رهبران کشور احتمالی که درباره آنها به شکل عمومی بحث می‌شود، می‌توانند تصور کنند که یک یا چند گزینه مورد نظر علیه آنان می‌باشد. بنابراین، سرویس‌های اطلاعاتی دیگر منع قابل اعتماد و بی‌طرف اطلاعات به حساب نمی‌آیند. رابرتسون هشدار می‌دهد که در این صورت، «سازمان‌های اطلاعاتی، استقلال خود را از دست می‌دهند و به بخشی از روند ایجاد اجماع سیاسی تبدیل می‌گردند». از این رو، شفاف‌سازی بیش از اندازه اطلاعات و مدیریت ضعیف این شفاف‌سازی می‌تواند تهدیدی علیه تحلیل تأثیرگذار اطلاعات و مشارکت آن در روند تصمیم‌گیری ملی و حتی تهدیدی علیه امنیت عملیاتی باشد. البته، خطری که از نادیده گرفتن محدودیت‌ها ناشی می‌شود، در مورد مدیریت صحیح اطلاعات نیز صدق می‌کند. رابرتسون با رویکردی عادلانه درباره پنهان‌کاری در بریتانیا اینگونه نتیجه‌گیری می‌کند: «اگرچه ما نمی‌توانیم گزارش‌های سرویس‌های اطلاعاتی به سیاست‌مداران را کنترل کنیم... اما این کار خطر ایجاد سرویس اطلاعاتی کاملاً سیاسی را از بین برده است» (Davies, ۲۰۰۴).

در عین حال، مهم‌ترین پیامدی که پنهان‌کاری مفرط، به ویژه در جوامع مردم‌سالار به وجود می‌آورد، زیر سؤال رفتن مشروعیت سیاسی ساختارها و سازمان‌های نظام سیاسی است که بر پنهان‌کاری اصرار می‌ورزند. شفاف‌سازی چاره این افت است. شفافیت به معنای پاسخ‌گویی به

درخواست در مورد اخبار مورد توجه جامعه است که به جامعه اجازه می‌دهد دولت مطبوع خود را در قبال اعمالش پاسخ‌گو نگاه دارد، حتی اگر دولت قادر نباشد در زمان واقعی به سؤال پاسخ دهد. این موضوع تنها مختص به سازمان‌های اطلاعاتی نیست و کارکرد آن را در کوچک‌ترین مسائل اجتماعی و دیگر موضوعات سیاسی می‌توان مشاهده کرد. برای مثال، حتی پنهان‌کاری در خصوص میزان قراردادهای منعقدشده یک مربی یا بازیکن فوتبال هم از این موضوع مستثنی نیست.

در عین حال، مفهومی که لازم است در آن دقت کافی به خرج داد، آن است که ناپستی موضوع و بار معنایی پنهان‌کاری در کارکردهای دولت را با مفهوم پنهان‌کاری در سازمان‌های اطلاعاتی یکسان دانست. حال، با توجه به مطالبات مردم‌سالارانه در قبال پنهان‌کاری، در بخش بعد به بررسی فرضیه رقیب که پنهان‌کاری را ابزاری در فعالیت اطلاعاتی می‌داند، می‌پردازیم.

### ج. پنهان‌کاری: ابزار فعالیت اطلاعاتی

در این بخش به بررسی پنهان‌کاری به عنوان ابزاری برای فعالیت اطلاعاتی می‌پردازیم. با این نگاه، پنهان‌کاری ابزاری است در جعبه ابزار سازمان‌های اطلاعاتی که نحوه استفاده از آن در چهارچوب معیارهای سازمان به مجریان باز می‌گردد. همچنین، در اینجا به تبیین منشاء برداشت ابزاری بودن پنهان‌کاری می‌پردازیم و پی می‌بریم که با گسترش جوامع مردم‌سالار و مطرح شدن نظارت بر ارکان نظام، از جمله سازمان‌های اطلاعاتی، تلاش شده است پنهان‌کاری به هویتی ابزارگونه برای اطلاعات تبدیل شود تا موضوع نظارت بر اطلاعات جنبه عملی به خود بگیرد. در این رویکرد، لفظ پنهان‌کاری بار معنایی مثبتی ندارد، چرا که به معنی جلوگیری از اطلاع جامعه مدنی از موضوعات جاری است.

در دهه‌های اخیر (بنا به شکل ساختار سیاسی و فرهنگی کشورها)، فعالیت اطلاعاتی از موضوعی مرموز و مخفی خارج شده (و یا مجبور است که خارج شود) و به شاخه‌ای از علوم اجتماعی که بخش عمده‌ای از وظایف آن پیش‌بینی و آینده‌پژوهی در طیف گسترده‌ای از موضوعات مرتبط با امنیت ملی است، تبدیل شده است. با بلوغ اطلاعات (حرکت از تبدیل شدن این حرفه به علم یا حداقل تلاش برای این انتقال)، خواه ناخواه از تمرکز و اتکای

این ابزار سیاسی به اقدامات کاملاً سری کاسته شده است. انقلاب منابع آشکار و تحول در فن‌آوری در این امر نقش مهمی برعهده داشته است (ر. ک. سالارکيا، ۱۳۹۰). در عین حال، این موضوع، به معنای از دست رفتن همه محرمانگی اطلاعات نیست. مردم‌سالاری که بنیان‌گرفته بر اساس شفافیت است، بدون پاسخ‌گویی زنده نخواهد ماند، اما این ویژگی اصلی دموکراسی، به معنای به ورطه خودکشی افتادن اطلاعات نیست.

برای حفاظت از منابع، شگردها و اخبار دارای طبقه‌بندی، میزانی از مخفی‌کاری و به عبارت دقیق‌تر، پنهان‌کاری ضروری است. در این بین، منابع و شگردها به حفاظت کامل نیاز دارند. خبرگان اطلاعاتی همگی متفق‌القولند که شگردهای فنی ویژه و هویت منابع، هم اشخاص و هم سازمان‌ها، در مقابل افشاشدن نیازمند حفاظت‌اند. در غیر این صورت، جان مأموران و منابع به خطر افتاده و ارتباطات به عنوان مهم‌ترین رمز موفقیت سازمان اطلاعاتی افشا می‌گردد که در این وضعیت، ادامه دسترسی به اخبار<sup>۱</sup> مهم به طور جدی به خطر می‌افتد. برای مثال، چنانچه رابطه و تبادل اطلاعاتی یک سازمان اطلاعاتی با فرد یا گروه و حزبی مشخص گردد، مسلماً جریان اطلاعات از این شریان به خطر خواهد افتاد. این خطر از یک منظر، از دست رفتن توانایی‌های اطلاعاتی منبع خواهد بود و از منظر دیگر، خطر ورود اطلاعات فریب توسط مطلعین مخالف ارتباط را به دنبال خواهد داشت. همچنین، از منظری دیگر، خطر بروز مخالفت‌های وسیع از درون جامعه مورد تبادل را خواهد داشت. هر کدام از این موارد می‌تواند منجر به از دست رفتن توانایی جمع‌آوری اطلاعات شود. این روند، در ادامه، حتی ممکن است به عاملی برای مرگ منابع انسانی، تغییر حکومت‌ها و افشای فن‌آوری‌های اطلاعاتی شود. این همه از مضرات از دست رفتن پنهان‌کاری در اطلاعات است. حتی تصور این وضعیت مشکل است که برای مثال، رابطه‌ای که سال‌ها صرف ایجاد آن شده است و پنهان‌کاری چتر حفاظتی آن است، افشا گردد و کل تلاش‌ها نابود گردد. تاریخ

---

۱. توجه داشته باشید که بین خیر و اطلاعات تفاوت وجود دارد. اطلاعات از نظر کیفیت و ارزش در مرحله‌ای بالاتر از خیر قرار دارد. آنچه خیر را به اطلاعات تبدیل می‌نماید، تحلیل‌گر اطلاعاتی (بررس) است که با دمیدن روح به کالبد بی‌جان خبر آن را تولید می‌نماید. برای درک بهتر موضوع به چرخه کلاسیک اطلاعات توجه بفرمایید.

اطلاعات مملو از چنین مواردی است.<sup>۱</sup> در کل، شفافیت همه‌جانبه در امور اطلاعاتی مزیت‌های پیش‌دستانه را از بانی آن سلب می‌نماید. در عین حال، این سؤال مهم همچنان باقی است که پنهان‌کاری تا چه حد و تا چه زمان؟ آیا اساساً زمانی فرا خواهد رسید که اطلاعاتی از این دست در اختیار افکار عمومی قرار گیرد؟

باید توجه داشت که پنهان‌کاری مبتنی بر حفاظت از منابع و روش‌ها باعث گردید برهان سطح لغزنده<sup>۲</sup> نیز در ارتباط با نگرانی‌های موجود در زمینه پنهان‌کاری عملیاتی مترتب و فراگیر شود. طبق این برهان، شفاف‌سازی مسائل اطلاعاتی غیر عملیاتی می‌تواند به شیوه‌ای خطرناک تبدیل شود و با تضعیف تدریجی پنهان‌کاری باعث فاش شدن مسائل اطلاعاتی عملیاتی گردد (Davies, ۲۰۰۴). به همین دلایل، در جوامع مردم‌سالار، سازوکار نظارت بر اطلاعات از طریق کارگروه‌های ویژه، به خصوص در نهادهای نظارتی پارلمانی در زمینه‌های زیر به انجام می‌رسد: (Born & Caparini, ۲۰۰۷, : ۳۹- ۴۰)

- بازبینی نوبه‌ای دستورالعمل‌ها و خط‌مشی‌های سرویس‌های اطلاعاتی در خصوص فعالیت‌های اطلاعاتی قانونی یا قابل قبول؛
- گزارش نوبه‌ای در خصوص یافته‌ها و هرگونه فعالیت اطلاعاتی که باعث ایجاد سؤالاتی جدی در مورد قانونی بودن یا به انجام رسیدن صحیح آنها شده است؛
- کمک به بررسی‌های قضایی در خصوص فعالیت‌هایی که سؤالاتی در مورد قانونی بودن آنها مطرح شده است؛
- مدیریت تحقیقات درباره فعالیت‌های اطلاعاتی سازمان‌های اطلاعاتی که به نظر می‌رسد برای تحقق وظایف آنها ضروری است.

---

۱. اطلاعات به عنوان بخشی از ابزار سیاست‌گذاری، با توجه به دسترسی‌های خود در موارد متعددی دست پنهان دولت‌ها در روابط سیاسی با دولت‌ها، سازمان‌ها و گروه‌های دولتی و غیردولتی و اشخاص به شمار می‌رود. رژیم اشغال‌گر قدس با توجه به مشکلات عدیده‌ای که در رابطه با دیگر کشورها دارد، به ویژه آن دسته از کشورها که افکار عمومی آن نسبت به ارتباط با این رژیم حساس هستند، ید طولایی دارد. کارکرد جامعه اطلاعاتی رژیم اشغال‌گر قدس در این موضوع را می‌توان بی‌همتا خواند. (Raviv & Melman, ۱۹۹۱).

البته، سازوکارهای ایجادشده برای ایجاد تعادل میان پنهان‌کاری و شفافیت سازمان‌های اطلاعاتی تلاش می‌کنند شرایطی را فراهم آورند تا پنهان‌کاری به عنوان ویژگی هستی‌شناختی اطلاعات را با توسل به روش‌های گوناگون، به گونه‌ای در قالب ویژگی ابزاری درآورده و کنترل کنند. «هیرش»، ایجاد تناسب میان نظارت و فعالیت سازمان اطلاعاتی در رهیافت گذر از ویژگی هستی‌شناختی به ویژگی ابزاری را در مقابل کمیسیون اطلاعات چنین شرح می‌دهد:

«نظارت باید الزامات حفاظت را رعایت کند. سازمان اطلاعاتی که در معرض دید عموم قرار بگیرد، کارایی خود را از دست می‌دهد. بنابراین، تضادی ایجاد می‌شود مابین نیاز به مخفی‌کاری در سازمان‌های اطلاعاتی و از طرف دیگر، نیاز ناظران بر این سازمان‌ها به دریافت اطلاعات. به این ترتیب، حق تصمیم‌گیری در امور اطلاعاتی یا حق ناشناخته‌ماندن منبع در مقابل حق شهروندان در گرفتن اطلاعات قرار می‌گیرد. حق شهروندی که می‌خواهد بداند آیا در حقوق اساسی او مداخله شده است یا خیر، مطرح می‌شود. نظارت بر سازمان‌های اطلاعاتی باید و می‌تواند در چهارچوبی انجام شود که قانون اساسی اجازه داده است» (اولف کوتاه، ۱۳۸۰: ۱۷۳).

برکوویتز و گودمن نیز با تأکید بر اینکه جامعه اطلاعاتی همواره درگیر پنهان‌کاری است، برآند که:

«پنهان‌کاری صرفاً باید وسیله‌ای برای انجام کار باشد و نه خصلت و ویژگی حاکم بر فرهنگ اطلاعات. این تمثیل را در نظر بگیرید: افسران پلیس سلاح‌های مرگبار حمل می‌کنند و می‌توانند متوسل به زور شوند. با این حال، تسلیحات مرگبار و استفاده از زور عناصر تقویت‌کننده حرفه پلیس نیستند. برعکس، به افسران پلیس از ابتدای آموزش یاد می‌دهند که از وجهه، اقتدار و نیز قدرت دستور دادن خود در شغلشان استفاده کنند و تنها در صورت ضرورت متوسل به زور به عنوان راه حل جایگزین شوند. به همین شکل، کارکنان اطلاعاتی نیز باید متخصص مدیریت کسب اطلاعات از منابع اعم از پنهان و آشکار باشند. به افسران هادی و تحلیل‌گران نیز باید آموزش داده شود که از پنهان‌کاری همان‌طور که افسر پلیس از سلاح‌های سازمانی خود استفاده می‌کند، تنها به عنوان ابزاری مفید به هنگام ضرورت استفاده کند.» (برکوویتز و گودمن، ۱۳۸۲: ۲۴۷-۲۴۶)



در کارگاه یک‌روزه‌ای که توسط مؤسسه رند و با حضور جمعی از صاحب‌نظران اطلاعاتی برای بررسی تئوری‌ها، مفاهیم و چالش‌های اطلاعاتی برگزار گردید، چنین جمع‌بندی شد:

«در اینکه پنهان کاری عنصر مهم اطلاعات است، اتفاق نظر کامل وجود دارد، زیرا از این طریق برتری نسبی برای کشور مجری کار اطلاعاتی فراهم آورده می‌شود. با وجود این، برخی این سؤال را مطرح کردند که آیا پنهان کاری عنصر ضروری در تعریف اطلاعات است یا فقط معیاری برای چگونگی اجرای مناسب آن توسط یک کشور می‌باشد. همه تردید داشتند که آیا عنصری کاربردی است یا یک اقدام اطلاعاتی است که نیازمند طبقه‌بندی می‌باشد.» (Tereverton & etal, ۲۰۰۶)

می‌بینیم که با توجه به شفافیت مورد نیاز جامعه، کارشناسان اطلاعاتی که از هستی‌شناختی بودن پنهان کاری در اطلاعات اندکی کوتاه آمده‌اند و تنها آن را عنصر مهم اطلاعات تلقی نموده‌اند، نسبت به ابزاری بودن صرف اطلاعات تردید دارند. در عین حال، شکی نیست که گام‌هایی اجرایی برای هرچه ابزاری‌تر کردن اطلاعات برداشته شده است. برخی از این گام‌ها چنان متناقض و ناشیانه برداشته شده که با استهزا و تمسخر روبه شده است. برای مثال، یکی از اولین اقدامات رئیس سیا، رابرت گیتس که به عنوان پانزدهمین رئیس سیا در نوامبر ۱۹۹۱ معرفی شد، ایجاد کارگروهی برای بررسی سیاست‌های پرهیز از پنهان کاری سیا بود که پاسخی باشد در برابر این انتقاد که پنهان کاری بیش از حد به اعتبار سازمان لطمه زده و روابط آن را با کنگره ضعیف کرده است. با وجود این، زمانی که این کارگروه برای آزادی بیش‌تر سیا پس از چهار هفته کار خود را به پایان رساند، گزارش آن فوراً طبقه‌بندی شد و باعث خنده و استهزای هرچه بیش‌تر گزارش‌گران و سردبیران سراسر کشور شد. پس از چند ماه تمسخر، سیا گزارش مربوطه را منتشر کرد (آیزندراس، ۱۳۸۳: ۱۶۵). در مثالی دیگر، زمانی که شرح وظایف شغلی یکی از نهادهای نظارتی دولتی هنگام طبقه‌بندی، به مهر سری ممهور می‌شود، حتی کارکنان خود این نهاد نظارتی که دسترسی آنان به اسناد پایین‌تر ارزیابی شده است (محرمانه و خیلی محرمانه) قادر نیستند از شرح وظایف اداره‌ای که در آن خدمت می‌کنند، مطلع شوند. در چنین رفتارهایی است که «وقتی همه‌چیز محرمانه شد، در آن صورت، هیچ چیز محرمانه نخواهد بود. وقتی مطالبی که ارزش پنهان نگه‌داشتن از دید عموم را ندارد، مهر محرمانه بخورد، رازداری داده‌های حساس هم بی‌ارزش می‌شود؛ هرچه مطالب محرمانه کمتر شود، مسأله محرمانگی در موضوعات واقعاً سری، جدی‌تر خواهد شد.» (De Valk, ۲۰۰۵: ۴۱).

## نتیجه گیری

به نظر می‌رسد در رقابت میان پنهان‌کاری و شفافیت در سازمان‌های اطلاعاتی، عملاً این پنهان‌کاری است که در اولویت قرار گرفته است (Chinen, ۲۰۰۹: ۱۴). پنهان‌کاری ضربان زندگی فعالیت اطلاعاتی است و چنانچه این عنصر ضروری از اطلاعات سلب شود، اطلاعات از حیز انتفاع ساقط خواهد شد. در عین حال، ممکن است شفافیت هزینه‌هایی بیش‌تر از آنچه به نظر می‌رسد داشته باشد، اما این بهایی است که بایستی برای ادامه روند مردم‌سالاری و برخورداری از حسن اعتماد اجتماعی پرداخت گردد. «اطلاعات به هر دو، مخفی‌کاری و نظارت محتاج است» (لاکوئر، ۱۳۸۱: ۴۷۷).

در طول قرن بیستم، نحوه برخورد کشورها با موضوع اطلاعات همانند نحوه برخورد با مسائل جنسی بوده است. به این شکل که با وجود هر دوی آنها و به تناسب مشکلات عدیده وابسته به آن مانند ایدز، به دلایل گوناگون رغبت چندانی در جامعه برای طرح آن وجود نداشته است. این وضعیت در برخی کشورها همچنان وجود دارد. به همین دلیل، در طول این قرن، همواره پنهان‌کاری، عنصر ذاتی و هستی‌شناختی اطلاعات بوده است. به نظر می‌رسد جوامع به دنبال آن هستند که پنهان‌کاری را از ویژگی هستی‌شناختی و عنصر لاینفک اطلاعاتی با جرح و تعدیل زمانی و مکانی به صفتی که میزان آن توسط صاحب صفت مهار می‌شود، به ویژگی ابزاری تبدیل نمایند.

پنج عاملی که امروزه باعث شفافیت در عرصه جهانی شده است شامل گسترش نظام‌های مردم‌سالار؛ افزایش رسانه‌های جهانی؛ گسترش سازمان‌های غیردولتی؛ گسترش رژیم‌های بین‌المللی که منوط به شفافیت اطلاعات است و افزایش توانایی‌های ارتباطی و انفجار اطلاعات و تسونومی اطلاعات منابع آشکار (Lord, ۲۰۰۷)، باعث شده است سازمان‌های اطلاعاتی برای ادامه حیات، هرچه بیش‌تر از انزوا و عزلت‌نشینی خارج شده و خود را با عناصر جدید جوامع قرن بیست‌ویکم تطبیق دهند. به همین دلایل است که سرویس‌های اطلاعاتی از آرژانتین و استرالیا گرفته تا آفریقای جنوبی و حتی انگلیس، امروزه وبسایت‌های ویژه خود را دارند (Weller, ۱۹۹۹) که در آن به معرفی خود می‌پردازند. وزارت اطلاعات جمهوری اسلامی ایران نیز اقدام به ایجاد وبسایت مختص به خود کرده است.

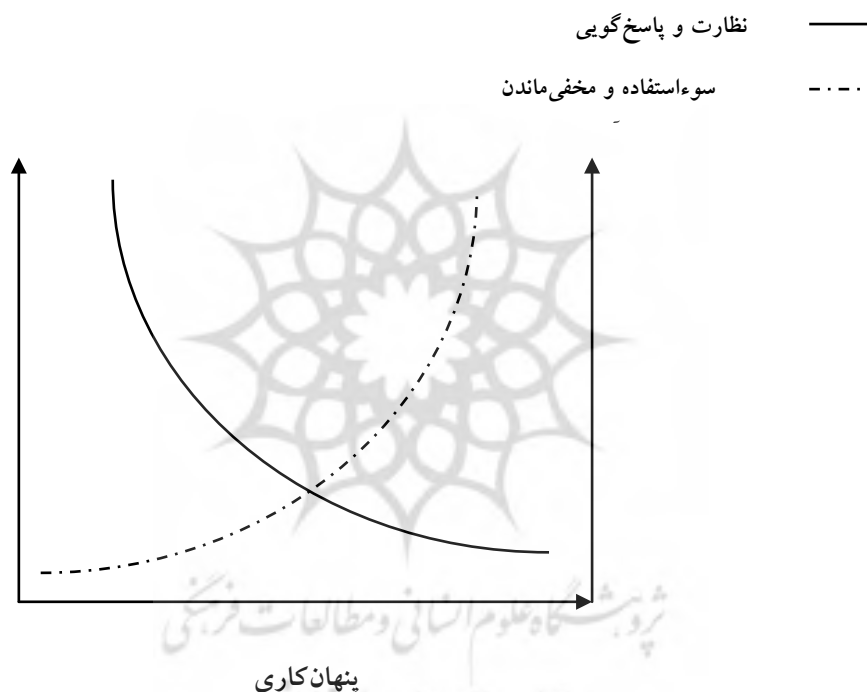
بنابراین، سوگیری حرکت قرن بیست و یکم به سوی کاهش میزان پنهان‌کاری سازمان‌های اطلاعاتی در جهتی است که این سازمان‌های تمام پنهان‌کار را در زیر چتر مردم‌سالاری جدید تعریف کند و شمشیر دولبه پنهان‌کاری را مهار نماید. البته، مهار و مدیریت آب بر اساس خواست مصرف‌کننده به منزله گرفته‌شدن خصلت سیال‌بودن آب نیست. سیال‌بودن آب در ذات آن است همان‌گونه که پنهان‌کاری عنصر ذاتی اطلاعات است. مهار پنهان‌کاری به منزله حذف عنصر مذکور از اطلاعات نیست. در غیر این صورت، اطلاعات وجود خارجی نخواهد داشت و نامی دیگر بر این ماهیت جدید بایستی گذاشت. همان‌گونه که با گذر از مرزهای تعریف‌شده، آب به یخ یا بخار مبدل می‌شود و دیگر کلمه آب به آن اطلاق نمی‌شود. گرچه برخی از اطلاعات را می‌توان به دور از پنهان‌کاری (جمع‌آوری آشکار) به دست آورد، نظیر فعالیتی که در برخی سازمان‌های غیرمحرمانه برای تولید اطلاعات به انجام می‌رسد، که نتیجه چنین محصولاتی خود دارای مهر طبقه‌بندی است. همچنین، نبایستی فراموش کرد که اخبار به دست آمده از همه منابع، برای کاهش عدم اطمینان تحلیل‌گران و تصمیم‌گیران امری ضروری است. به نظر می‌رسد امروزه بهتر است در وضعیت نظارت کارا بر اطلاعات، به جای لفظ پنهان‌کاری با بار معنایی منفی آن<sup>۱</sup>، از عنوان پنهان‌بودگی استفاده شود.

با توجه به آنچه پیش‌تر گفته شد، لازم است جوامع مردم‌سالار سازوکاری عملی را مهیا نمایند تا تناسب میان این دو تناقض‌نما، یعنی پنهان‌کاری و شفافیت تحت قوانین رعایت شود تا مزاج جامعه مردم‌سالار متناسب باقی بماند. این موضوع در کشورهای (نظیر کشورهای شرقی) که فرهنگ درون‌گرایی (پنهان‌کاری) نیز در آنها نهادینه شده و ریشه‌ای تاریخی دارد، اهمیتی دوچندان می‌یابد، زیرا خطر افراط و تفریط آنها را تهدید می‌نماید.<sup>۲</sup> همان‌گونه که در شکل زیر

۱. در رویکرد مردم‌سالارانه، پنهان‌کاری با برداشته‌هایی که بیان‌گر جلوگیری از دسترسی آزادانه مردم به حقوق خود می‌باشد، آغشته شده است. بنابراین، برای تطبیق این ویژگی ذاتی اطلاعات با شرایط زمینه‌ای بهتر است از واژه «پنهان‌بودگی» استفاده شود.

۲. ایران از جمله کشورهای شرقی است که درون‌گرایی، جایگاهی ویژه در فرهنگ و هنر آن دارد. این امر را به راحتی می‌توان در نوع معماری (فضاسازی درونی یک منطقه محصور مشخص)، موسیقی، ادبیات و مانند آنها ملاحظه کرد.

می‌بینیم، در برخورد دو منحنی نظارت و پاسخ‌گویی و سوءاستفاده و مخفی ماندن ناکارآمدی‌ها، نقطه بهینه‌ای وجود دارد که بنا به شرایط متفاوت جوامع تعریف می‌شود و این وظیفه ذاتی سیاست‌گذاران است که با درک صحیح از شرایط، وضعیت را تعریف کنند. در غیر این صورت، یا شفافیت و مردم‌سالاری آسیب خواهد دید و یا ابزار سیاست‌گذاری (اطلاعات) ناکارآمد خواهد شد (Doorey, ۲۰۰۷ & Johnston, ۲۰۰۵: ۱۱-۱۲).



جوامع با فرهنگ‌های خاص خود باید بیاموزند که بین شفاف‌سازی مورد نیاز افکار عمومی و پنهان‌کاری مورد نیاز برای ادامه حیات ساختارهای سیاسی و موضوع ما یعنی اطلاعات تعادل برقرار نمایند. بایستی مدیریت دولتی اطلاعات بر مبنای پنهان‌کاری شدید و عموماً خشک به برنامه قابل انعطاف و دارای توان اقناع افکار عمومی تبدیل شود. در این صورت، دولت به جای مخفی کردن همه چیز، اطلاعات زیادی را در اختیار افکار عمومی قرار می‌دهد،

اما حق انتخاب برای انتشار یا عدم انتشار اطلاعات را برای خود محفوظ می‌دارد. در عین حال، این به دست نمی‌آید مگر آنکه سیاست‌گذاران و تصمیم‌گیران سیاسی، از یک سو به مفاهیم مردم‌سالاری معتقد و از سوی دیگر، خارج از تعصب، به موضوعات و مفاهیم اطلاعاتی تسلط و چیرگی داشته باشند. «پنهان‌کاری نباید تبدیل به عادت دائمی شود» (Kimbal, ۲۰۰۱) و در عین حال، شفافیت نیز نباید تبدیل به ابزاری سیاسی گردد.



## منابع

- آستانا، ان‌سی (۱۳۸۸)؛ **مدیریت اطلاعات و امنیت**، ترجمه علی پیرحیاتی، تهران: دانشکده امام باقر(ع).
- ابوالحسنی، علی (۱۳۸۵)؛ **مبانی حفاظت از اسناد: نظام‌نامه و مقررات اجرایی دبیرخانه محرمانه**، تهران: مؤسسه مطالعات و پژوهش‌های بازرگانی (دفتر مرکزی حراست وزارت بازرگانی).
- اولف‌کوته، اودو (۱۳۸۰)؛ **بی‌ان‌دی: سازمان اطلاعات آلمان**، ترجمه معاونت پژوهشی دانشکده امام باقر(ع)، تهران: دانشکده امام باقر(ع).
- آیزندراس، کریچ (۱۳۸۳)؛ **نام‌های ملی: اطلاعات آمریکا پس از جنگ سرد**، ترجمه سید مجید نوری، تهران: دانشکده امام باقر(ع).
- برکوویتز و گودمن، بوریس دی. و آلن ای. (۱۳۸۲)؛ **بهترین حقایق اطلاعات در عصر اطلاع‌رسانی**، ترجمه معاونت پژوهشی دانشکده امام باقر(ع)، تهران: دانشکده امام باقر(ع).
- بلک، یان، موریس، بنی (۱۳۷۲)؛ **جنگ‌های نهانی اسرائیل**، ترجمه جمشید زنگنه، دفتر نشر و فرهنگ اسلامی.
- پیرآلم، ژان (۱۳۷۰)؛ **جاسوسی و ضد جاسوسی**، ترجمه: ابوالحسن سروقد مقدم، تهران: آستان قدس رضوی.
- ترنر، استنسفیلد (۱۳۸۷)؛ **پنهان‌کاری و دموکراسی**، ترجمه حسین ابوترابیان، تهران: اطلاعات، چ ششم
- ترنر، مایکل ای. (۱۳۸۸)؛ **علل شکست اطلاعات سری**، ترجمه قاسم بنی‌هاشمی، تهران: دانشکده اطلاعات.
- جانسون، لاج کی. (۱۳۹۰)؛ **اطلاعات راهبردی: عملیات پنهان در سیاست خارجی محرمانه**، ترجمه فرزین هدایت، تهران: مرکز آموزشی و پژوهشی شهید سپهبد صیاد شیرازی.
- سالارکیا، غلامرضا، پاییز (۱۳۹۰)؛ «انقلاب منابع آشکار در هزاره سوم: چالش هستی‌شناختی اطلاعات»، **فصلنامه مطالعات راهبردی**، شماره ۵۳.
- شولسکی، آبرام، (۱۳۸۱)؛ **نبرد بی‌صدا: درک دنیای اطلاعات**، ترجمه معاونت پژوهشی دانشکده امام باقر(ع)، تهران: دانشکده امام باقر(ع).
- کاتز، ساموئل، (۱۳۷۵)؛ **جاسوسان خط آتش**، ترجمه محسن اشرفی، تهران: اطلاعات
- لاکوئر، والتر، (۱۳۸۱)؛ **جهان اسرار**، ترجمه معاونت پژوهشی دانشکده امام باقر(ع)، تهران: دانشکده امام باقر(ع).
- لوونتال، مارک ام. (۱۳۸۷)؛ **فرآیند اطلاعات: از اسرار تا سیاست**، ترجمه: علیرضا غفاری، تهران: دانشکده امام باقر(ع).

میرمحمدی، مهدی، (۱۳۹۰)؛ سازمان‌های اطلاعاتی و سیاست خارجی: مطالعه موردی نقش سازمان سیا در سیاست خارجی آمریکا، مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران. وینر، تیم، جانستون، دیوید، لويس، نیل. ا (۱۳۷۶)؛ *خیانت*، ترجمه و انتشار دانشکده اطلاعات.

- Bruce, James B. (۲۰۰۸); «Making Analysis more Reliable: Why Epistemology Matters to intelligence», in *Analyzing Intelligence*, Gorge Washington University Press.
- Born & Caparini (ed.), Hans & , Marina (۲۰۰۷); *Democratic Control of Intelligence Services: Containing Rogue Elephants*, Ashgate
- Born, Hans, (۲۰۰۸); *Contemporary Challenges to the Democratic Oversight of Intelligence Services*, Geneva Centre for the Democratic Control of Armed Forces.
- Chinen, Mark A (۲۰۰۹); «Secrecy and Democratic Decisions», *Quinnipiac law Review*, Vol. ۲۷, available at: <http://ssrn.com/abstract=۱۳۰۲۰۶۷>
- Davies, Philip H.J. (۲۰۰۴); *The Use and Abuse of Intelligence: Spin, Open Government and the Politicisation of intelligence in Britain*, Brunel University, Brunel Center for Intelligence and Security Studies.
- De Valk, Gill (۲۰۰۵); *Dutch Intelligence: Towards a Qualitative Framework for Analysis*, Boom Juridische Uitgevers.
- Doorey, Timothy J. (۲۰۰۷); «Intelligence secrecy and Transparency: finding the Proper Balance from the War of Independence to the War on Terror», *Strategic Insight*, Vol. ۵, No. ۳.
- Herman, Michael, (۱۹۹۶); *Intelligence Power in Peace and War*, Cambridge: Cambridge University Press.
- Johnston, Rob (۲۰۰۵); *Analytic Culture in the US Intelligence Community: An Ethnographic Study of Intelligence*, Central Intelligence Agency
- Kimball, Warren F. (۲۰۰۱); «Openness and the CIA», *CSI*, Vol. ۴۴, No. ۵, available at <https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol44no5/html/v44i5a.ap.htm>.
- Lord, Kristin M. (۲۰۰۷); «National Intelligence in the Age of Transparency» in Johnson, loch K., *Strategic Intelligence*, Vol. ۱
- Moran, Christopher R., (June ۲۰۱۱); «The Pursuit of Intelligence History: Methods, Source, and Trajectories in the United Kingdom», *Studies in Intelligence*, Vol. ۵۵, No. ۲.
- ODNI (Office of the Director of National Intelligence) (۲۰۰۹); «The National Intelligence: A Consumer's Guide», from [http://www.dni.gov/reports/IC\\_Consumers\\_Guide\\_۲۰۰۹.pdf](http://www.dni.gov/reports/IC_Consumers_Guide_۲۰۰۹.pdf)
- Pateman, Roy (۲۰۰۳); *Residual Uncertainty*, University Press of America
- Posner, Richard A. (۲۰۰۶); *Uncertain Shield: The U.S. Intelligence System in the Throes of Reform*, Rowman & Littlefield Publishers.

- Raviv, Dan & Melman, Yossi (۱۹۹۱); *Every Spy a Prince: The Complete History of Israel's Intelligence Community*, Houghton Mifflin Co.
- Shapiro, Sholomo (۲۰۰۱); «The Media Strategies of Intelligence Services», *International of Intelligence and Counterintelligence*, Vol. ۱۴.
- Thompson, Dennis F. (۱۹۹۹) «Democratic Secrecy», ۱۱۴ Pol. SCI. Q.
- Treverton Gregory F. & et al. (۲۰۰۶); *Toward a Theory of Intelligence*, RAND.
- Treverton, Gregory F. (۲۰۰۵); *The Next Step in Reshaping Intelligence*, RAND Corporation available at: [http://www.rand.org/pubs/occasional\\_papers/۲۰۰۵/RAND\\_OP۱۵۲.pdf](http://www.rand.org/pubs/occasional_papers/۲۰۰۵/RAND_OP۱۵۲.pdf)
- Warner, Michael & McDonald, J. Kenneth, April (۲۰۰۵); «US Intelligence Community Reform Studies Since ۱۹۴۷», *Strategic Management Issues Office*, Center for the Study of Intelligence, Washington DC
- Weller, Geoffrey R. (۱۹۹۹); «Oversight of Australia's Intelligence Services», *International Journal of Intelligence and Counterintelligence*, Vol. ۱۲, No. ۴

