یادداشت راهبردی

رهیافت‌های مدیریت جامعه اطلاعاتی

مهدی میرمحمدی *

مقدمه

سازماندهی و مدیریت فعالیت اطلاعاتی در دوره مدرن، با دو مسئله بنیادین مواجه بوده است. نخست، چگونگی توزیع صلاحیت‌ها و اختیارات فعالیت اطلاعاتی در میان نهادهای نظامی و غیرنظامی و مسئله دوم، چگونگی مدیریت تضاد میان فعالیت‌های پنهان‌پژوهانه نهادهای اطلاعاتی با مجموعه‌ای از ارزش‌ها و هنجارها شامل اصول و محدودیت‌های شرعی، اخلاقی، مردم‌سالارانه و قانونی است.

از زمان ظهور فعالیت اطلاعاتی نظام‌مند و مدرن در ایران که می‌توان آن را با ظهور ساواک مقارن دانست، مدیران سیاسی و اطلاعاتی ایرانی نیز به تدریج هر دو مسئله را تجربه کردند. تا پیش از انقلاب اسلامی، سران رژیم پهلوی قادر به درک درست این مسائل و اهمیت مدیریت آن نبودند و همین ناتوانی منجر به شکل‌گیری تمایل فزاینده برای فعالیت اطلاعاتی نه تنها در ساواک، بلکه علاوه بر آن در «رکن دو ارتش» و شهربانی شد. این تمایل فزاینده، همراه با تشدید رقابت بین‌سازمانی و افزایش آسیب‌پذیری‌ها و تهدیدات علیه رژیم پهلوی، ناگهان در دهه ۵۰ به

* دانش‌آموخته دکتری روابط بین‌الملل دانشگاه تهران

افزایش فعالیت نهادهای اطلاعاتی نظامی و غیرنظامی در جامعه انجامید. این شرایط سه پیامد در محیط امنیت ملی برای رژیم پهلوی به دنبال داشت: نخست، موازی‌کاری و ناهماهنگی میان سازمان‌های اطلاعاتی بود. دوم، افزایش خفقان اجتماعی و درپی آن نفرت از نهادهای اطلاعاتی در نزد افکارعمومی؛ و سوم، ایجاد فشارهای بین‌المللی به دلیل شکنجه و نقض اصول انسانی در بازداشت‌گاه‌ها که توسط عناصر آزادشده از بند رژیم و شبکه دانشجویان خارج از کشور بازنمایی می‌شد. رژیم پهلوی برای مدیریت پیامد نخست، «کمیته مشترک ضدخرابکاری» را تأسیس کرد تا بتواند تکثر در فعالیت‌های اطلاعاتی داخلی را مدیریت کند، اما دیرهنگام و بی‌اثر بودن این اقدام، در کنار ناتوانی رژیم در فهم پیامدهای اجتماعی داخلی و بین‌المللی اقدامات اطلاعاتی مدیریت‌نشده، مشروعیت رژیم را نزد مردم و نخبگان داخلی و همچنین جامعه بین‌المللی به شدت زیر سؤال برد. در واقع تشدید فعالیت اطلاعاتی در دهه ۴۰ و دهه ۵۰ که انتظار می‌رفت با ضربه‌زدن به گروه‌های مسلح سازمان‌یافته، ضریب امنیت را افزایش دهند، به نوبه خود تبدیل به یک نقطه ضعف و عامل نفرت از رژیم پهلوی نزد افکارعمومی داخلی و خارجی شد.

در ادبیات مطالعات اطلاعاتی به این وضعیت «نقش اطلاعات در ناامنی ملی» اطلاق می‌شود و منظور این است که اگر فعالیت اطلاعاتی در چارچوب کنترل‌های قانونی، نهادی و اخلاقی مدیریت نشود، به جای آنکه به افزایش امنیت بیانجامد، به فرسایش آن منجر می‌شود. لزوم مدیریت پیامدهای منفی فعالیت اطلاعاتی، طی دو دهه گذشته منجر به ظهور تلاش‌های نظری برای ارائه راه‌حل‌هایی جهت مدیریت دو مسئله ابتدایی این نوشتار شده است که در ادامه به طور خلاصه به آنها اشاره می‌شود.

رهیافت‌های سه‌گانه مدیریت تکثر

برای مدیریت موازی‌کاری و تکثر در فعالیت اطلاعاتی دو رهیافت نظری ظهور کرده است. رهیافت نخست «تقسیم کار تخصصی» یا «تمرکزگرایی تخصصی» در فعالیت اطلاعاتی است. در این رهیافت، نظام‌های سیاسی صلاحیت‌ها و اختیارات «سازمان‌های اطلاعاتی» خود را بر اساس معیارهای زیر تفکیک می‌کنند تا از موازی‌کاری و ناهماهنگی و پیامدهای ناخواسته آن جلوگیری شود. این معیارها عبارتند از:

- تقسیم کار بر اساس حوزه جغرافیایی که منجر به شکل‌گیری دو سازمان تخصصی مجزا برای «ضداطلاعات» و «اطلاعات خارجی» می‌شود. سرویس ضداطلاعاتی صلاحیت و اختیار اقدامات اطلاعاتی در درون مرزها را دارد و سرویس اطلاعات خارجی مسئول جمع‌آوری و اقدام اطلاعاتی در خارج از مرزها است. برای نمونه «سرویس مخفی اطلاعات» موسوم به «MI6» و «سرویس امنیتی» موسوم به «MI5» که به ترتیب

سازمان اطلاعات خارجی و سازمان ضداطلاعاتی انگلستان هستند، طبق این معیار سازماندهی شده‌اند. تقسیم کار میان سازمان اطلاعات مرکزی آمریکا، موسوم به «سیا» و دفتر تحقیقات فدرال آمریکا، موسوم به «اف‌بی‌آی» نیز بر این مبنا می‌باشد.

- تقسیم‌کار بر اساس حوزه‌ی موضوعی که طبق آن سازمان‌های اطلاعاتی نظامی و غیرنظامی از یکدیگر تفکیک می‌شوند. سازمان‌های اطلاعاتی نظامی در موضوعات مرتبط با نظامیان و فرایندهای فرماندهی نظامی صلاحیت دارند و حوزه‌های موضوعی مدنی نیز در صلاحیت سرویس‌های اطلاعاتی غیرنظامی قرار می‌گیرد.
- تقسیم کار بر اساس روش‌جمع‌آوری که منجر به تفکیک و تمایز سازمان‌های اطلاعات فنی از سرویس‌های اطلاعاتی مبتنی بر منابع انسانی می‌شود. برای نمونه ستاد ارتباطات دولتی در انگلستان یا سازمان امنیت ملی در آمریکا، نهادهای اطلاعاتی تخصصی در حوزه جمع آوری فنی هستند.

البته در عمل می‌توان ترکیبی از این معیارها را برای تقسیم کار تخصصی در نظر گرفت. کشورهایی که چند سازمان اطلاعاتی تخصصی دارند، معمولاً یک نهاد ملی بالادستی برای سیاست‌گذاری یکپارچه، نظارت بر عملکرد و پاسخگوکردن سازمان‌های اطلاعاتی در برابر قانون، تأسیس می‌کنند. «دفتر اطلاعات ملی» در آمریکا یک نمونه عینی از چنین نهادهایی است که وظیفه نظارت، بودجه‌ریزی و سیاست‌گذاری ملی اطلاعاتی در آمریکا را برعهده دارد.

رهیافت دوم برای مدیریت تکثر و موازی‌کاری، «تمرکز ساختاری و یکپارچگی» در فعالیت اطلاعاتی است که در اصطلاح به آن «تجمیع اطلاعات زیر یک سقف» نیز گفته می‌شود. براین اساس، برخی از نظام‌های سیاسی تمامی فعالیت‌های اطلاعاتی شامل اطلاعات خارجی، ضداطلاعات، جمع‌آوری فنی و اقدام پنهان را در یک سازمان مستقل و یکپارچه ملی تجمیع می‌کنند. در این حالت، معمولاً کشور دارای یک سرویس اطلاعاتی غیرنظامی یکپارچه در کنار سازمان‌های اطلاعاتی و ضداطلاعاتی نظامی است که صلاحیت‌ها و اختیارات آنها با معیار «حوزه موضوعی» از یکدیگر تفکیک شده است. سرویس اطلاعاتی غیرنظامی به طور همزمان مسئول جمع‌آوری خارجی، ضداطلاعات، تحلیل اطلاعاتی و اقدام پنهان است و ضمن پشتیبانی از کشورداری مدنی، وظیفه پشتیبانی از نهادهای نظامی را نیز برعهده دارد. برای مثال «وزارت اطلاعات جمهوری اسلامی ایران» یک نمونه عینی از این رویکرد است. البته در قرن بیستم، نمونه‌هایی از سرویس اطلاعاتی یکپارچه ملی با ماهیت شبه‌نظامی نیز وجود داشت که «کمیته امنیت دولتی» شوروی موسوم به «کا.گ.ب.» یکی از آنها است.

رهیافت سوم در خصوص مدیریت تکثر، «موازی‌کاری مدیریت‌شده» است. گاهی به دلیل ازدیاد و تشدید تهدیدات ضداطلاعاتی و اطلاعاتی، نظام‌های سیاسی برای حفظ امنیت خود مجبور به بسیج اطلاعاتی و استفاده از نهادهای مختلف با وظایف هم‌پوشان می‌شوند تا یک موقعیت اظطراری را مدیریت کنند. در این حالت، رهبران نظام سیاسی با اراده خود و با هدف عبور از شرایط دشوار امنیتی، اجازه دخالت نهادهای نظامی و غیرنظامی اطلاعاتی در موضوعات یکسان را صادر می‌کنند تا قادر باشند تهدیدات فزاینده را کنترل کنند. البته این رهیافت مشروط به دو معیار است؛ نخست «مدیریت‌کردن» موازی‌کاری است که معنای آن وجود قوانین یا دستورات بالادستی برای فعالیت اطلاعاتی موازی در یک موضوع خاص توسط دو یا چند نهاد است و دوم آنکه این وضعیت نباید تبدیل به رویه دائمی شود و پس از عبور از شرایط اضطرار باید پایان یابد.

نظارت بر اطلاعات و مسئله تعارض فعالیت اطلاعاتی و ارزش‌ها

دومین مسئله در مدیریت نهادهای اطلاعاتی، چگونگی کنترل تعارض میان پنهان‌پژوهی و پنهان‌کاری با اصول قانونی، شرعی و انسانی است. در ادبیات اطلاعاتی«نظارت بر اطلاعات» به عنوان سازوکاری جهانی برای تضمین قانونمندی و حتی کارآیی سازمان اطلاعاتی معرفی شده است. براین اساس گفته می‌شود که نظام‌های سیاسی برای تضمین کارایی سازمان‌های اطلاعاتی و همچنین اطمینان از رعایت ارزش‌ها و هنجارهای مورد نظرشان در فرایند کاراطلاعاتی باید چهار نوع نظارت را بر دستگاه‌های اطلاعاتی اعمال کنند که به شرح زیرند:

- **نظارت اجرایی:** که منظور از آن نظارت بر عملکرد سرویس اطلاعاتی توسط مقام ارشد اجرایی کشور است. برای نمونه در نظام جمهوری اسلامی ایران، رئیس محترم جمهور وظیفه نظارت اجرایی بر سازمان‌های اطلاعاتی غیرنظامی کشور را برعهده دارند که آن را از طریق وزیر اطلاعات به عنوان نماینده قانونی رئیس‌جمهور منتخب مردم در سازمان اطلاعاتی، اعمال می‌نمایند. مقام معظم رهبری نیز از طریق ستاد کل نیروهای مسلح وظیفه نظارت اجرایی بر نهادهای اطلاعاتی و ضداطلاعاتی نظامی را اعمال می‌نمایند.
- نظارت قضایی: که منظور از آن نظارت بر رعایت چارچوب‌های قانونی در اعمال قدرت اطلاعاتی بر شهروندان توسط مقامات قضایی است. البته نظارت قضایی، عمدتاً یک امر پیشینی است. به این معنا که هر گونه اقدام اطلاعاتی مداخله‌جویانه باید قبل از آغاز مجوز قضایی لازم را اخذ کند. در حالت پسینی نیز، پس از آنکه یک سرویس اطلاعاتی فردی را به یک اتهام خاص دستگیر می‌کند، تصمیم‌گیری نهایی برای مجازات بر عهده دستگاه قضایی مستقل است.

- **نظارت پارلمانی:** که منظور از آن پاسخگوبودن مقامات اجرایی اطلاعاتی هر کشور در برابر نمایندگان منتخب مردم است. هدف از نظارت پارلمانی، از یک طرف جلوگیری از سیاست‌زدگی اطلاعات و سوءاستفاده از قدرت اطلاعاتی توسط دستگاه‌های اجرایی است و از طرف دیگر تضمین پاسخگوبودن دستگاه‌های اطلاعاتی به ویژه در نظام‌های مردم‌سالار است.
- **نظارت درونی:** که معنای آن نظارت درونی سازمان اطلاعاتی بر پرسنل و کارگزاران اطلاعاتی است تا تضمین‌کننده رعایت اصول و ارزش‌های حرفه‌ای، فکری و قانونی در فرایند کار اطلاعاتی باشد. برای نمونه فلسفه وجودی بخش‌های حفاظتی و بازرسی در ساختار نهادهای اطلاعاتی، در چارچوب نظارت درونی است.

نتیجه‌گیری

اولین نکته در بخش پایانی نوشتار، تأکید بر این واقعیت است که هیچ‌کدام از رهیافت‌های فوق، خیر مطلق یا شرّ مطلق نیستند. هر رهیافتی واجد برخی مزیت‌ها و برخی نقاط ضعف است. نکته دوم آن است که معمولاً انتخاب میان چند رهیافت، یک تصمیم سیاستی است که توسط رهبران ارشد نظام‌های سیاسی اتخاذ می‌شود و مدیران و کارشناسان اطلاعاتی باید بدانند که تأثیرگذاری بر این سطح از سیاست‌گذاری اطلاعاتی، مستلزم توانمندی آنان در شکل‌دادن به گفتمان ملی در باب اطلاعات در واحدهای تصمیم‌گیری است. در هر حال، دو معیار جایگاه حیاتی در انتخاب درست دارند. معیار اول «قدرت اطلاعاتی» است. اصل اول در سازماندهی دستگاه‌های اطلاعاتی باید تناسب آن با خلق قدرت اطلاعاتی باشد. سازماندهی اطلاعات باید به گونه‌ای باشد که فارغ از سلایق و جهت‌گیری‌های سیاسی و حزبی، به کسب، حفظ و افزایش «قدرت اطلاعاتی» بیانجامد. معیار دوم نیز تناسب سازماندهی با ماهیت نظام سیاسی و خواسته‌های نهادینه در افکار عمومی است. سازمان‌های اطلاعاتی هر کشور باید برآمده و سازگار با ارزش‌های سیاسی کشور باشند. برخی از ساختارها تنها در نظام‌های سیاسی اقتدارگرا مناسب‌اند و به خلق قدرت اطلاعاتی و امنیت می‌انجامند. همان ساختارها اما ممکن است در یک جامعه مردم‌سالار نه تنها «قدرت اطلاعاتی» را کاهش دهند، بلکه فراتر از آن به تضعیف بنیان‌های مشروعیت نظام سیاسی منجر شوند. مدیران اطلاعاتی در هر کشوری باید متوجه این نکته باشند که سازماندهی اطلاعات یا هر نوع نهادسازی اطلاعاتی در نظام‌سیاسی متبوعشان باید متناسب با ارزش‌ها و ضدارزش‌هایی باشد که نظام سیاسی برمبنای آن بنیان‌گذاری شده است