شماره 6

رهنمودهای حکومت‌داری خوب

ایجاد توازن بین باز بودن (علنی بودن) و محرمانه بودن اطلاعات در سکتور دفاعی: تجاربی از عملکردهای خوب بین‌المللی

Norwegian Ministry of Defence

Centre for Integrity in the Defence Sector

مرکز صداقت و درستکاری در سکتور دفاعی

مرکز صداقت و درستکاری در سکتور دفاعی به ترویج درستکاری، اقدامات ضد فساد و حکومتداری خوب در سکتور دفاعی می‌پردازد. این مرکز در همکاری با همکاران نرویژی و بین‌المللی در جستجوی ایجاد شایستگی، افزایش آگاهی و فراهم آوری ابزارهای عملی جهت کاهش خطرات فساد می‌باشد. مرکز صداقت و درستکاری در سکتور دفاعی در سال 2012 توسط وزارت دفاع ناروی تأسیس شد.

درباره نویسنده

فرانسیسکو کاردونا (Francisco Cardona) یک متخصص بین‌المللی در مرکز صداقت و درستکاری در سکتور دفاعی می‌باشد. کاردونا یک متخصص شناخته شده است که تمرکز وی طراحی و ارزیابی اصلاحات در خدمات ملکی و اداره عامه، قانون اداری و سیستم عدلی، پالیسی‌های ضد فساد و نهادسازی می‌باشد. تجربه وی از زادگاهش دراسپانیا، از دوره کاری وی در خدمات ملکی، شروع شده و سپس در سازمان‌های بین‌المللی همچون برنامه حمایت از بهبود حکومتداری و مدیریت (سیگما) در چارچوب سازمان همکاری و توسعه اقتصادی ادامه می‌یابد. وی 15 سال را به حیث تحلیلگر ارشد پالیسی در زمینه حکومتداری عامه در سیگما سپری نمود و در چهارچوب این برنامه به 25 کشور در حال گذار و در حال انکشاف در اروپای شرقی، آفریقا، آمریکای لاتین و منطقه کارائیب، مشوره ارائه داد. وی در رشته حقوق (پوهنتون والنسیا، 1976) تحصیل نموده و دارای چندین سند ماستری در اداره عامه می‌باشد.

پیشگفتار

هدف اصلی رهنمودهای حکومت‌داری خوب مرکز صداقت و درستکاری در سکتور دفاعی ارائه مسائل کلیدی مرتبط با "حکومت‌داری خوب" است. رهنمودها باید مختصر و بدون ساده‌سازی بیش از حد موارد باشد.

در ششمین رهنمود، هدف نویسنده زیر سوال بردن مفهوم "محرمیت" در سکتور دفاعی است. به همین منظور نویسنده می‌پرسد: "نقطه توازن بین آزادی دسترسی به اطلاعات و ضرورت اعمال برخی محدودیت‌ها بر آن دسترسی" در جوامع دموکراتیک که توسط "دولت باز" اداره می‌شود، کجاست؟ علاوه بر این، چه زمانی لازم است اطلاعات را به منظور محافظت از امنیت ملی محدود کنیم؟ به حقوق شهروندان برای حمایت از دولت توجه کنید.

این رهنمود توسط فرانسیسکو کاردونا، یکی از کارشناسان بین‌المللی ارشد مرکز صداقت و درستکاری در سکتور دفاعی، نوشته شده است. در اینجا می‌خواهم از او به خاطر سهم بسیار ارزشمندش به چنین موضوع مهمی در زمینه حکومت‌داری خوب تشکر کنم. موضوعی که در سال‌های اخیر در بحث‌های عمومی از اهمیت بالایی برخوردار بوده و احتمالاً در سال‌های آینده نیز ادامه خواهد یافت.

همچنین از سردبیر مرکز، بارد بریدراپ نودسن و آسه ماری فوسوم، هماهنگ‌کننده انتشارات، به خاطر تلاش‌هایشان تشکر می‌کنم. این مرکز امیدوار است که سهم‌گیری در موضوع حکومت‌داری خوب مورد استقبال مخاطبین زیادی، هم در سکتور عامه از جمله سکتور دفاعی و هم بیرون از آن، قرار بگیرد. ایجاد توازن بین باز بودن (علنی بودن) و محرمانه بودن اطلاعات در سکتور دفاعی جهت عملکرد درست جوامع دموکراتیک حیاتی است.

مرکز صداقت و درستکاری در سکتور دفاعی از دریافت هرگونه نظرات و پیشنهادات راجع به این رهنمود خوشحال خواهد شد.

اوسلو، 24 اپریل 2018

پیر کریستنسن
رئیس

فهرست

مقدمه

این رهنمود عملکردهای خوب بین‌المللی که توسط اتحادیه اروپا و کشورهای سازمان همکاری و توسعه اقتصادی اتخاذ شده را بطور مختصر ارائه می دهد. عملکردهایی که مقصدشان حفظ محرمیت اطلاعات عمومی در عرصه دفاعی و امنیت ملی، ضمن وصول اطمینان از حقوق جامعه برای دسترسی به اطلاعاتی که در اختیار نهادهای عمومی است، می باشد. هدف این رهنمود پیشنهاد پالیسی‌هایی است که دولت باز و دسترسی به اطلاعات را ارتقاء می‌دهد و توانایی شهروندان را برای قضاوت آگاهانه راجع به عملکرد حکومت بهبود می‌بخشد. در عین حال، مرزها و محدودیت‌های لازم برای محافظت صحیح از اسرار دولتی که در امنیت ملی، دفاعی و استخباراتی و همچنین مبارزه با فساد و جرایم حساس می‌باشد، را تعیین می‌کند.

شفافیت و عمومی‌سازی به عنوان بهترین راه‌حل جهت پیشگیری از بروز فساد، سوءمدیریت و حکومت‌داری ضعیف در نظر گرفته می‌شود. دموکراسی‌ها در شرایط پنهان‌کاری (محرمیت) نمی‌توانند به درستی عمل کنند، چراکه پنهان‌کاری بیش از حد به راحتی می‌تواند شهروندان را از پروسه سیاسی بیرون کرده و رژیم سیاسی را به غیر دموکراتیک کند. این بدان معنی است که روند اعمال قدرت ممکن است از کنترل خارج شود و منجر به عدم پاسخگویی دموکراتیک شود. با این حال، برای حفظ عملکرد صحیح دموکراسی در یک حکومت کارآمد ممکن است دسترسی مردم به اطلاعات نیز محدود شود. بنابراین، خواه اطلاعات عمومی افشاء شود یا محدودیت‌های خاصی برای افشای آن اعمال شود باید به همان اندازه منافع عامه را تأمین کند.

چارچوب مفهومی: امنیت ملی به عنوان توجیهی برای محرمانه بودن اطلاعات

فرضیه مفهومی اساسی این است که دولت باز و آزادی دسترسی به اطلاعات از یک سو و محدودیت این آزادی از سوی دیگر منافع عامه را تامین می‌کند. این یک اصل پذیرفته‌شده بین‌المللی است که حکومت‌ها باید "حق دانستن" را ترویج دهند در حالی که محدودیت‌های معقولی را به منظور حفاظت از اطلاعات محرمانه خاص تعیین کنند. این محدودیت‌ها جهت اطمینان از کارآیی دولت در برخی عرصه‌ها، به ویژه در عرصه‌های دفاعی و امنیت ملی لازم است.

مشکل اصلی مشروعیت زمان و چگونگی محدودیت دسترسی شهروندان به اطلاعات است. اطمینان از دسترسی عامه به این اطلاعات هدف بلندپروازانه (دموکراسی) کشورهای موفق دموکراتیک است، در حالی که مرزهای قانونی خاصی برای محدود کردن این دسترسی تعیین شده است. چگونگی ایجاد توازن مناسب بین این دو رویکرد تا حد زیادی به تاریخ کشور، ارزش‌های اجتماعی و سایر عوامل فرهنگی بستگی دارد. به همین دلیل تعیین اینکه آیا استندردهای بین‌المللی برای کمک به برقراری توازن مناسب وجود دارد یا خیر دشوار است (Transparency International UK, 2014). در واقع، با وجود مباحث و تلاش‌های علمی و فکری فراوان در سال‌های اخیر برای ایجاد برخی اصول کلی، چنین استندردهای بین‌المللی عملاً وجود ندارد.[1]

در صورت نادیده گرفتن و عدم کنترل، دامنه محرمیت به راحتی گسترش یافته و بزرگتر می‌شود. برخی از نهادهای دولتی که در زمینه‌های مدیریت امنیت ملی، دفاع، تحقیقات جنایی، استخباراتی یا مبارزه با تروریسم فعالیت می‌کنند، علاقه‌مند به حفظ محرمیت در تمام فعالیت‌های خود هستند، حتی اگر این امر منجر به جلوگیری از حق دانستن شهروندان راجع به فعالیت‌های حکومت شود. علاوه بر هزینه‌های زیاد برای حفظ مکانیزم محرمیت، استفاده بیش از حد و گسترده از محرمیت اعتماد عمومی به نهادهای حکومتی را تضعیف می‌کند و در نهایت منجر به تضعیف مشروعیت دموکراتیک می‌شود. پنهان‌کاری و محرمیت بیش از حد منجر به اشتباهات و تخلفات بیشتری نسبت به شفافیت و تدقیق عمومی می‌شود، زیرا عدم شفافیت، تدقیق عمومی و اصلاح عملکرد ضعیف را دشوارتر می‌کند. در نتیجه، در دراز مدت، پنهان‌کاری و محرمیت بیش از حد می‌تواند تهدیدی بزرگتر از باز بودن (علنی بودن) برای امنیت ملی باشد.

به عنوان مثال، به گفته برخی از مقامات دولتی از جمله مقامات ایالات متحده، محرمیت و پنهان کاری بیش از حد "به یک مانع غیرقابل توجیه برای تبادل اطلاعات در داخل و بیرون حکومت تبدیل شده است که به پالیسی‌های عامه آسیب می‌رساند" (Aftergood, 2008, page 400) . این مسئله به مشکل طبقه‌بندی بیش از حد اطلاعات محرمانه اشاره می‌کند، یعنی سرویس‌های نگهدارنده

1 See The Tshwane Principles (2013): https://www.opensocietyfoundations.org/fact-sheets/tshwane-principles-national-security-and-right-information-overview-15-points

اطلاعات تمایل دارند به طور قابل توجهی بیش از آنچه در واقع لازم است به طبقه‌بندی اطلاعات محرمانه بپردازند.

هدف اصلی هر سیستم طبقه‌بندی جلوگیری از افشای اطلاعاتی است که ممکن است امنیت ملی را تهدید کند، اما ابهامی که پیرامون مفاهیم و اصطلاحاتی مانند "امنیت ملی" و "تهدیدات امنیتی" وجود دارد، شرایطی را برای استفاده بیش از حد از ابزارهای محرمیت ایجاد می‌کند. مشکل تمایز بین اطلاعات واقعی و ذهنی (انتزاعی) ایجاد معیارهای مشخص برای طبقه‌بندی صحیح اطلاعات را دشوار می‌کند.

طبقه‌بندی صحیح اطلاعات محرمانه (تعیین سطوح محرمانه بودن هر یک از اطلاعات) به خودی خود مفهومی کاملاً پیچیده است، اما از نظر مفهومی ممکن است توافق کنیم که یک طبقه بندی "مناسب" طبقه بندی است که توجیهات معقولی داشته و تا حد ممکن با ارزش‌های دموکراتیک، باز بودن (علنی بودن)، شفافیت و دسترسی آزاد به اطلاعات مطابقت داشته باشد. به عبارت دیگر، یک محدودیت معقول در شفافیت به این واقعیت‌ها اشاره دارد الف) استثنایی باشد، و ب) از منافع مهم امنیت ملی محافظت کند. در نتیجه، در عرصه دفاعی و امنیت ملی اطلاعاتی وجود دارد که پنهان‌کاری آنها برای امنیت ملی حیاتی نیست و می‌تواند - به طور کامل یا جزئی - افشاء شود.

رویکرد سنتی رایج در بعضی از کشورهای دموکراتیک نشان می‌دهد که شفافیت (علنی بودن) صرفاً نمایانگر خواسته یک شهروند است و محرمیت اطلاعات به خاطر امنیت ملی در دفاع از منافع عامه است. به عنوان مثال، آقای ژان مارک ساوئه، معاون شورای مشورتی دولت فرانسه، در 5 جولای 2011 در یک سخنرانی در مجلس شورای ملی فرانسه، پارلمان فرانسه، گفت: " راه پیش رو این است که مرزی بین محرمیت مشروع برای حفاظت از منافع عامه و شفافیتی که شهروندان خواستار آن هستند، ایجاد کنیم" (ساوو، 2011 ، صفحه 6). این عبارت بر این فرض استوار است که حفظ محرمیت از منافع عامه محافظت می‌کند، در حالی که شفافیت منافع عامه را تأمین نمی‌کند، بلکه صرفاً خواسته‌ای است که توسط کنجکاوی شهروندان و ژورنالیستان انجام می‌شود. این یک فرض بسیار سوال برانگیز است. تجربه نشان داده است که ارتقاء شفافیت یکی از بهترین راه‌ها برای محافظت از منافع عامه است، زیرا این امر به پاسخگویی (مسئولیت‌پذیری) مقامات دولتی در برابر شهروندان و سایر میکانیسم‌های کنترول دموکراتیک کمک می‌کند. بنابراین، شفافیت، به جای محرمیت می‌تواند به عنوان وسیله‌ای برای پر کردن "شکاف طبیعی بین دولت و جامعه" تلقی شود (Fenster, 2010, page 619).

بر اساس اجماع بین‌المللی موجود، شفافیت باید در پالیسی و فعالیت‌های مقامات دولتی به عنوان یک قاعده کلی در نظر گرفته شود، در حالی که محرمیت یک قاعده مستثنی است. علاوه بر این، چنین استثنائاتی باید توجیه شود: تنها در صورت مشروعیت قابل توجیه هستند و تنها در صورتی مشروعیت دارند که ثابت شود این استثنائات برای محافظت از منافع واقعی امنیت ملی ضروری است.

ضرورت تمایز بین محرمیت مشروع و نامشروع مستلزم مقداری کنترول توسط مقاماتی است که به طور مستقل عمل کرده و جدا از مقاماتی فعالیت می‌کنند که به طبقه‌بندی اطلاعات محرمانه می‌پردازند. چنین مکانیزم‌های مستقل کنترول را دادگاه‌ها یا نهادهای عمومی تخصصی می‌توانند اعمال کنند. این مکانیزم‌ها تعیین می‌کند که آیا منافع امنیت ملی به عنوان توجیهی برای طبقه‌بندی اطلاعات محرمانه به اندازه کافی مهم است یا خیر. بدون مکانیزم‌های کنترول بیرونی، تصمیم‌گیری در مورد طبقه‌بندی اطلاعات کاملاً اختیاری و به احتمال زیاد خودسرانه می‌شود. با این حال، همانطور که قرار ذیل خواهیم دید، از نظر تاریخی دادگاه‌ها نقشی را ایفا کرده‌اند - و هنوز هم متعهد به انجام آن هستند - که بسیار متفاوت از عدم افشا سازی و عدم شفافیت اطلاعات است.

همانطور که در بالا ذکر شد، شفافیت کامل مطلوب

نیست و احتمالاً امکان‌پذیر هم نیست. علاوه بر این، دولت همیشه در موارد خاصی که نامشخص یا مبهم است، فعالیت می‌کند. همانطوریکه توسط فینستر اشاره شد (2010 ، ص 623)، غالباً بین محرمیت و شفافیت محدوده‌ای وجود دارد، یعنی محرمیت لزوما مغایر با شفافیت نیست. در عمل، محرمیت و شفافیت کاملاً یک واقعیت متضاد نیستند، زیرا هم محرمیت و هم شفافیت مستلزم پایه‌های اساسی متفاوتی هستند و از نظر ساختار با یکدیگر تفاوت دارند، (Riese, 2014, page 14).

شفافیت بیشتر لزوماً به معنای محرمیت کمتر نیست، اما بهبود کیفیت می تواند از محرمیت محافظت کند. به عبارت دیگر، شفافیت بیشتر بدین معناست که فقط نیازهای واقعی محرمیت محافظت می‌شود. در این زمینه، توجه به این نکته مهم است که نهادینه‌سازی پالیسی‌های شفافیت در بیشتر کشورها مسئله جدیدی است، در حالیکه نهادینه سازی پالیسی‌های محرمیت از سنت‌های تثبیت شده دیرینه ناشی می‌شود. ارزش‌ها و علایق هر یک از این سنت‌ها هنوز ناهمگن و به نوعی متناقض است. چالش اینست که نهادینه‌سازی حق دانستن و حمایت از نیازهای واقعی محرمانه بودن - چه در ساختارهای سازمانی و چه در عملکرد حکومت به صورت تدریجی هماهنگ شود. هماهنگی بین این دو پالیسی باید به طور ایده آل منجر به یک پالیسی واحد سازمانی سازگارتر جهت دسترسی به اطلاعات در حکومت‌های ملی، مطابق با نیازهای امنیت ملی شود.

با این حال، مفهوم "امنیت ملی" کاملا مبهم است، زیرا می‌تواند معانی مختلفی در بسترهای مختلف ملی داشته باشد که منجر به پیچیده‌تر شدن مسئله می‌شود. در بررسی بسیاری از کشورهای اروپایی که توسط جکوبسن (2013) انجام شد، امنیت ملی در یک درجه یا درجه دیگری روابط بین‌الملل و همچنین تهدیدات امنیت داخلی را در بر می‌گیرد،. به عبارت دیگر، لزوما یک مرز مشخص وجود ندارد.

برای تعیین اینکه آیا پنهان‌کاری حکومت مشروع است یا نه، افترووود (2009، صفحه 403-402) سه دسته عملی محرمیت را پیشنهاد می‌کند، ضمن تایید اینکه مشکل دائمی پالیسی عامه جداسازی پنهان‌کاری مشروع و غیرمشروع است - طوریکه اولی را حفظ و دومی را افشا می‌کند:

1. محرمیتی **که واقعاً به امنیت ملی مربوط می‌شود:** حفاظت از اطلاعاتی که ممکن است تهدید خاص قابل شناسایی برای امنیت یک ملت با به خطر انداختن قابلیت‌های دفاعی یا روابط خارجی آن باشد. حفظ چنین اطلاعاتی مورد مناقشه نیست، بخاطر اینکه همین مسئله منطق اصلی سیستم‌های اطلاعات محرمانه است. منافع عامه زمانی به بهترین وجه تامین می‌شود که چنین اطلاعاتی محرم بماند.

2. محرمیت **بوروکراتیک:** تمایل بوروکرات‌ها به حفاظت از اطلاعات، چه به دلیل راحتی و چه به ظن اینکه افشای اطلاعات ممکن است خطرناکتر از محرمانه بودن آن باشد. این گرایش بوروکراتیک معمولاً منجر به طبقه بندی بیش از حد اطلاعات می‌شود و در نتیجه مقدار زیادی اطلاعات طبقه‌بندی‌شده غیرضروری ایجاد می‌شود. این امر همچنین هزینه‌های هنگفتی را برای حفظ محرمیت اطلاعات به دنبال دارد و اغلب باعث بوجود آمدن حس اهمیت در خود و عدم تمایل به افشای نحوه عملکرد یک نهاد خاص حکومتی می‌شود.

3. محرمیت یا **پنهان‌کاری سیاسی:** تمایل طبقه‌بندی اطلاعات برای تأمین منافع سیاسی. این شکل از پنهان‌کاری بحث برانگیزترین و نامطلوب ترین است زیرا از مشروعیت پذیرفته‌شده منافع واقعی امنیت ملی به منظور پیشبرد آجندای منافع شخصی و یا فرار از جنجال سیاسی یا جلوگیری از مواجهه با مردم برای حسابدهی استفاده می‌شود. در موارد شدید، پنهان‌کاری سیاسی نقض قوانین، نقض حقوق بشر، فساد یا سوء مدیریت را پنهان می‌کند و همچنین تهدیدی برای سلامت، صداقت و درستکاری پروسه سیاسی است.

نقش کلی ضعیف قوه قضائیه در کنترول سیستم‌های طبقه‌بندی‌شده (محرمانه)

همانطور که قبلاً اشاره شد، دادگاه‌ها به طور سنتی و در حال حاضر در واکنش به عملکرد اداراتی که به طبقه‌بندی اطلاعات محرمانه می‌پردازند، "امتیاز اجرایی اسرار دولتی"، متمایز هستند. نقش قضایی متمایز کمک کرده تا این اندیشه جا بگیرد که حساسیت امنیت ملی اجازه نمی‌دهد اطلاعات حتی در دادگاه فاش شود(Setty، 2012). به عنوان مثال، پرونده برجسته جنگ سرد (ایالات متحده و رینولدز).[2]

تمایل دادگاه‌ها برای همراهی با قوه مجریه پس از حملات تروریستی 11 سپتامبر در ایالات متحده افزایش یافته است. ادعاهای حکومت برای محافظت از امنیت ملی به طور مداوم در دادگاه بر اصولی مانند حسابدهی، شفافیت و دولت باز غلبه دارد. پرونده‌های متعددی در ایالات متحده، بریتانیا، فرانسه و سایر کشورهای دموکراتیک جهان نقش محدود قوه قضائیه در بررسی تصمیمات اجرایی امنیتی را منعکس می‌کند، چه برسد به کشورهای که در سطح پایین تر دموکراسی قرار دارند. این رویکرد متأسفانه می‌تواند حمایت از حقوق اساسی، حاکمیت قانون و منافع واقعی امنیتی را تضعیف کند.

برای طبقه‌بندی اطلاعات محرمانه توسط مقامات اجرایی به منظور جلوگیری از بازنگری قضایی مورد استناد قرار می گیرد، یا حداقل مثمریت این بازنگری را کمتر می کند. استثنائات مربوط به علنی بودن اطلاعات بر اساس ادعاهای مبتنی بر سه شرط فوق معمولاً توسط دادگاه ها پذیرفته می‌شود، حتی اگر - گاهی اوقات - دادگاه ها به طور مبهم اعلام کنند که این امتیاز فقط باید به موارد واقعی امنیت ملی محدود شود. این موضع رایج عموماً آشکار می‌کند که "قوه قضاییه مفهوم کنترل و موازنه [در تفکیک قوا] را نادیده گرفته، از مسئولیت قوه قضائیه شانه خالی کرده و به ساختار مورد نیاز برای شاکیان، جهت ادعای جبران خسارت در برابر تهاجم بیش از حد دولت، بی اعتنایی می کند (Setty 2012، ص 1573).

فوکس در اثر مشهور خود در مورد نقش دادگاه‌ها Fuchs (سال 2006، ص 168) خاطرنشان می‌کند که "با توجه به اهمیت ارزشی که حق دسترسی به اطلاعات حکومتی دارد، این حق فقط زمانی قربانی می‌شود که نیاز مشروع به پنهان‌کاری وجود داشته باشد. پارلمان و مردم به خودی خود در موقعیتی نیستند که پنهان‌کاری بیش از حد را مورد پرسش قرار دهند. بررسی مستقل بخشی از مسئولیت قوه قضائیه برای اطمینان از مطابقت اقدامات حکومت با الزامات قانونی است." فقط دادگاه‌ها به اندازه کافی مستقل هستند تا پنهان‌کاری بیش از حد را به چالش بکشند، اما ظاهراً، فوکس خاطرنشان می‌کند که آنها از انجام این عمل خودداری کرده‌اند.

تقریباً در همه کشورهای اروپایی که توسط یاکوبسن (2013) مورد بررسی قرار گرفته است، دادگاه‌ها اختیار بررسی اطلاعات محرمانه‌ای که حکومت ها تلاش دارند به بهانه امنیت ملی پنهان کنند، را دارند. اما در برخی از کشورها اجازه بررسی اطلاعات محرمانه محدود به دادگاه‌های خاص یا قضات دارای مجوز ویژه می‌باشد. در آلمان تنها محکمه اداری فدرال اجازه بررسی اطلاعات طبقه‌بندی‌شده را دارد. در اسپانیا، اگر چه "قانون اسرار رسمی" به قضات اجازه نمی‌دهد چنین اطلاعاتی را ببینند و این حق را برای کنگره و مجلس سنا محدود کرده است، ستره محکمه تصمیم گرفته است که فقط و فقط او قدرت بررسی اطلاعات محرمانه طبقه‌بندی‌شده توسط حکومت را دارد. فرانسه تنها کشوری است که در آن دادگاه‌ها حق بررسی مستقیم راجع به اطلاعات محرمانه را ندارند، (Sartre و Ferlet ، 2010). قانون سال 1988 برای محدود کردن این ممنوعیت، کمیسیون مستقل دفاع ملی CSDN را ایجاد کرده است که به درخواست قاضی می‌تواند به اطلاعات محرمانه دسترسی داشته باشد - جهت ارزیابی اینکه آیا افشای اطلاعات محرمانه منطقی است یا خیر.[3] از نظر اتحادیه اروپا، بیشتر مراجع قضایی در کشورهای اروپایی عمدتاً به این نتیجه می‌رسند که افشای اطلاعات می‌تواند برای منافع امنیت ملی مضر باشد، (Jacobsen 2013).

2 https://supreme.justia.com/cases/federal/us/345/1/case.html

3 http://www.defense.gouv.fr/sga/le-sga-en-action/droit-et-defense/secret-defense/secret-defense

معیارها و سطوح طبقه‌بندی اطلاعات (تعیین سطوح محرمانه بودن هر یک از اطلاعات)

سطوح طبقه‌بندی اطلاعات به گونه‌ای معیاری شده است که همین سیستم طبقه‌بندی‌شده را می‌توان در بسیاری از کشورهای سازمان همکاری و توسعه اقتصادی یافت. در میان کشورهای سازمان همکاری و توسعه اقتصادی، نیوزلند نمونه خوبی از نحوه برخورد با اطلاعات محرمانه دولتی (اسرار دولتی) است. در نیوزلند، اطلاعات رسمی مطابق با معیارها بر اساس تعریف دقیق "ضرورت حفاظت از اطلاعات رسمی" محافظت می‌شود: اطلاعات باید تا حدی حفظ شود که به نفع عموم باشد و محرمانگی حفظ شود. در تعیین سطوح محرمانه بودن چنین اطلاعاتی سعی می‌شود آسیبی که ممکن است در نتیجه افشای غیرمجاز اطلاعات وارد شود و همچنین اقدامات اتخاذ شده برای حفاظت از آن در نظر گرفته شود.[4] طبق رهنمودهای نیوزلند، طبقه‌بندی به خودی خود به این معنا نیست که اطلاعات رسمی باید محفوظ بماند. بلکه اطلاعات باید از نظر حساسیت با توجه به معیارهای تعیین شده در قانون به طور عینی ارزیابی شود.[5] سیستم طبقه‌بندی امنیتی استرالیا از این جهت جالب است که رهنمودهای روشنی برای طبقه‌بندی اطلاعات محرمانه و افشای آن ارائه می‌دهد.[6]

سطوح طبقه‌بندی اطلاعات محرمانه در نیوزلند عملکردهای رایج بین‌المللی را به منظور حفظ منافع عامه تعقیب می‌کند، که به شرح ذیل است:

- **مرتبط با امنیت ملی:** افشای اطلاعات باعث به خطر افتادن سیستم دفاعی و امنیتی و همچنین روابط بین‌المللی کشور یا حکومت‌های دوست خواهد شد.
- **اطلاعات مرتبط با پالیسی‌های حکومت و/یا خصوصی افراد:** افشای اطلاعات ممکن است عملکرد حکومت را به خطر بیندازد یا به افراد آسیب برساند.

اطلاعات امنیت ملی در سطوح زیر با استفاده از این معیارها محافظت می‌شود:

1. **محرم اکید:** افشای آن منافع ملی را به شدت به خطر می‌اندازد:
   - مستقیماً ثبات داخلی نیوزلند یا کشورهای دوست را تهدید کند
   - مستقیماً منجر به از دست دادن جان مردم شود
   - باعث آسیب جدی به امنیت قوای مسلح نیوزلند یا متحدان آن شود
   - عملکرد عملیاتی نیروهای مسلح نیوزلند یا یک کشور دوست را به طور جدی مختل کند
   - آسیب جدی به موثریت مستمر عملیات‌های امنیتی و استخباراتی با ارزش برساند
   - روابط با سایر حکومت‌ها را به طور جدی مختل کند
   - صدمات جدی بلندمدت به زیربناهای مهم ملی وارد کند
2. **محرم:** افشای آن می‌تواند به طور جدی به منافع ملی آسیب برساند:
   - منجر به افزایش تنش بین‌المللی شود
   - روابط با حکومت‌های دوست را به طور جدی مختل کند
   - آسیب جدی به امنیت قوای نیوزلند یا قوای کشورهای دوست برساند

4 New Zealand's Official Information Act of 1982.
5 New Zealand's Guidelines for Protection of Official Information. See https://protectivesecurity.govt.nz/home/information-security-management-protocol/new-zealand-government-security-classification-system/
6 Australia (2014): Information Security Management Guidelines. Australian Government Classification System. At https://www.protectivesecurity.gov.au/informationsecurity/Documents/AustralianGovernmentclassificationsystem.pdf

- صدمات جدی به موثریت قوای نیوزلند یا قوای کشورهای دوست برساند
- آسیب جدی به موثریت عملیات‌های ارزشمند امنیتی یا استخباراتی برساند
- ثبات داخلی نیوزلند یا کشورهای دوست را تهدید کند
- زیربناهای مهم ملی را تعطیل یا به طور اساسی مختل کند.

3. **محرمانه:** افشای آن می‌تواند به طور قابل توجهی به منافع ملی آسیب برساند:

- صدمات قابل توجهی به روابط دیپلماتیک وارد کند - باعث اعتراضات رسمی یا تحریم‌های دیگر شود
- آسیب رساندن به موثریت عملیات قوای مسلح نیوزلند
- به قوای مسلح نیوزلند یا قوای دوست آسیب برساند
- به موثریت عملیات ارزشمند امنیتی یا استخباراتی آسیب برساند
- به ثبات داخلی نیوزلند یا کشورهای دوست آسیب برساند
- باعث از بین رفتن زیربناهای‌های ملی کشور شود

4. **دسترسی محدود:** افشای آن می‌تواند بر منافع ملی تأثیر منفی بگذارد:

- بر روابط دیپلماتیک تأثیر منفی می‌گذارد
- مانع موثریت عملیاتی قوای مسلح نیوزلند یا قوای مسلح دوست شود
- مانع امنیت قوای مسلح نیوزلند یا قوای کشورهای دوست شود
- بر ثبات داخلی نیوزلند یا کشورهای دوست تأثیر منفی بگذارد
- بر رفاه اقتصادی نیوزلند یا کشورهای دوست تأثیر منفی بگذارد

پالیسی حکومت و حریم خصوصی افراد در سطوح زیر و با استفاده از این استانداردها محافظت می‌شود:

5. **حساس و محدود:** افشای آن ممکن است به منافع حکومت آسیب برساند یا شهروندان را در معرض خطر قرار دهد:

- به خطر انداختن امنیت هر فرد
- به اقتصاد نیوزلند آسیب جدی وارد کند
- مانع مذاکرات حکومت شود

6. **مبتنی بر محرمانه بودن:** کافشای آنها می‌تواند به قانون و نظم آسیب برساند، مانع فعالیت‌های تجارتی حکومت شود، بر حریم خصوصی شهروندان تأثیر منفی بگذارد:

- جلوگیری از رعایت قانون
- بر حریم خصوصی شهروندان تأثیر منفی بگذارد
- به اطلاعات تجارتی شهروندان آسیب برساند
- روی تعهدات مربوط به محرمانه بودن تأثیر منفی بگذارد
- آسیب به اقداماتی که برای حفاظت از سلامت یا ایمنی مردم می‌باشد
- آسیب به منافع اقتصادی نیوزلند
- آسیب به اقداماتی که از خسارت مادی به جامعه جلوگیری می‌کند یا آن را کاهش می‌دهد
- نقض کنوانسیون‌های قانون اساسی
- مانع از رفتار موثر مردم در امور
- نقض امتیازات مسلکی قانونی
- مانع فعالیت های تجارتی حکومت

افشاء یا استفاده از اطلاعات به منظور کسب سود یا سود ناعادلانه

همانطور که قبلاً اشاره شد، علائم و معیارهای مشابه برای طبقه‌بندی اطلاعات محرمانه ممکن است در بسیاری از کشورهای سازمان همکاری و توسعه اقتصادی وجود داشته باشد. قوانین طبقه‌بندی اطلاعات حتی در ترکیه در دسترس عموم نیست، سطوح خاصی از طبقه‌بندی اطلاعات محرمانه وجود دارد (Jacobsen 2013). سوئد تنها کشوری بود که به نظرسنجی تحلیل شده توسط Jacobsen (2013) پاسخ داد که در آن قانون سطوح طبقه بندی اطلاعات را مشخص نکرده است، زیرا در سوئد طبقه بندی وظیفه ای کاملاً اداری دارد.

سایر جنبه‌های مربوط به طبقه بندی اطلاعات محرمانه (به عنوان مثال طرزالعمل‌های طبقه بندی، الزامات طبقه بندی، مقامات مسئول طبقه بندی، الزام به بیان دلایل طبقه بندی، حسابدهی در مورد طبقه بندی نادرست، نهادهای نظارتی و غیره) در کشورهای اروپایی بسیار متفاوت است (رجوع کنید به Jacobsen 2013 و شفافیت بین‌المللی انگلستان 2014).

معیارهای لغو طبقه‌بندی اطلاعات محرمانه

در کشورهای اروپایی، لغو طبقه‌بندی اطلاعات محرمانه از طریق سه معیار اصلی شکل می‌گیرد: محدودیت زمانی، رویداد تحریک کننده یا دوره بررسی اجباری. هدف اصلی از چنین معیارهایی جلوگیری از طبقه‌بندی دائمی اطلاعات محرمانه است. با این حال، به ندرت می‌توان کشورهایی را یافت که در قوانین یا شیوه‌های اداری خود هیچگونه معیاری برای لغو طبقه‌بندی اطلاعات محرمانه ارائه نکرده باشند. طبق محاسبات انجام شده توسط Jacobsen (2013)، محدوده زمانی متوسط برای طبقه بندی اطلاعات محرمانه در بین کشورهای اروپایی 30 سال است، با محدودیت‌های زمانی خاص از 10 سال در هلند تا 100 سال در رومانی و به طور نامحدود در اسپانیا و ترکیه. به هر حال، هلند در اروپا استثناء است.

دوره معمول برای بررسی اجباری اطلاعات طبقه بندی شده 5 سال است. در سویدن، هیچ دوره بررسی اجباری از پیش تعیین شده‌ای وجود ندارد، اما هر زمان که درخواست افشای اطلاعات داده شود، هر یک از اطلاعات محرمانه باید مورد بررسی قرار گیرند. خارج ساختن اطلاعات محرمانه از طبقه‌بندی به صورت اتوماتیک در کشورهای مختلف متفاوت است (رویداد محرک)، اما عامل اصلی در اکثر آنها تصمیم اختیاری حکومت برای خارج ساختن اطلاعات مختلف محرمانه از طبقه‌بندی است. چنین تصمیمی می‌تواند بر اساس اقدامات قانونی انجام شده توسط یک شهروند یا سازمان مدنی تحت قانون دسترسی به اطلاعات اتخاذ شود.

آزمایش تحت کنترول قرار دادن محرمیت اطلاعات: آزمایش آسیب و آزمایش توازن منافع عامه

با توجه به مطالب منتشر شده در سایت Right-2INFO.org، که مربوط به یک سازمان غیر حکومتی است و قوانین و عملکردهای خوب را ترویج می‌دهد، آزمایش آسیب و آزمایش منافع عامه از ضرورت محدود سازی متناسب و ضروری برای دسترسی به اطلاعات ناشی شده است.[7] نهاد OECD-SIGMA (2010) یک رویکرد مفهومی مفصل و گسترده به ایده‌هایی که این آزمایش‌ها بر اساس آن ایجاد شده را ارائه می‌دهد، رویکردی که اساساً برمبنای تمایز بین محدودیت‌های مطلق و نسبی دسترسی به اطلاعات است. مورد اول عمدتا شامل موارد مربوط به دفاع و امنیت ملی است.

آزمایش آسیب

با توجه به آزمایش آسیب، مقامات دولتی باید نشان دهند که افشای اطلاعات مشخص ممکن است منافع حفاظت شده را تهدید و به آنها آسیب برساند. بنابراین، افشای چنین اطلاعاتی نباید رخ دهد. آزمایش آسیب دولت را ملزم می‌کند که خطر آسیب اساسی و آشکار به منافع مشروع معین را توجیه کند. به این معنا که دولت موظف است ثابت کند که محدودیت مربوط به منافع مشروع خاصی است و افشای آن ممکن است به آن منافع خاص آسیب جدی برساند و این آسیب باید خاص، ملموس، قریب الوقوع و به اندازه کافی مستقیم باشد، یعنی آسیب بر اسای حدس و گمان یا سوال برانگیز نباشد.

آزمایش توازن منافع عامه

آزمایش توازن منافع عامه به نسبی بودن (غیر مطلق) بودن اشاره دارد. این آزمایش نیازمند عملکرد متوازن است، به این معنی که آسیب افشاگری در قبال منافع عامه ای که از طریق افشاگری تامین می شود، باید سنجیده شود. شرایطی که در آن منافع عامه روشن و مفصل ممکن است بر نیاز به پنهان‌کاری / محرمیت غلبه کند – چنین خط مشی باید توسط قوانین ملی مشخص می‌شود. بر اساس بسیاری از مودل‌های ملی مورد استفاده در طبقه بندی اطلاعات محرمانه - از جمله مودل‌های قاره آمریکا و آفریقا- از جمله اطلاعات مربوط به نقض حقوق بشر یا جنایات علیه بشریت، منافع عامه بر سایر منافع برتری می‌یابد. آزمایش متوازن‌سازی مستلزم آن است که یک مقام دولتی یا یک نهاد نظارتی میزان آسیبی را که با افشای اطلاعات ممکن است به منافع حفاظت شده خاص وارد شود را در مقایسه با منافع عامه که با چنین افشاگری به دست می‌آید، ارزیابی کند.

منافع عامه در کشورهای مختلف تعاریف متفاوتی دارد که اغلب نیاز به ارزیابی جداگانه برای هر مورد دارد. به طور کلی، منافع عامه که طرفدار افشای اطلاعات است معمولاً شامل موضوعات مربوط به بحث عمومی، مشارکت عمومی در بحث سیاسی، حسابدهی به تخصیص و هزینه‌های وجوه عامه و مسائل مرتبط به امنیت عامه است. مسائل مربوط به امنیت عامه و محیط زیست، تهدیدات جدی برای سلامتی و اطلاعات مربوط به نقض فاحش حقوق بشر معمولاً مواردی هستند که اولویت افشای اطلاعات بخاطر منافع عامه را توجیه می‌کنند.

برخی از کشورها رهنمودهایی را برای طرزالعمل‌های اداری خدمات ملکی منتشر کرده‌اند. به عنوان مثال، در ایالت نیو ساوت ولز، استرالیا، کارکنان خدمات ملکی هنگام تصمیم گیری برای نشر اطلاعات باید آزمایش توازن منافع عامه را اعمال کنند. این بدان معناست که آنها این موضوع را ارزیابی می‌کنند که آیا منافع عامه با افشای اطلاعات تامین می‌شود یا با عدم افشای آن. با توجه به این رهنمودها آزمایش توازن منافع عامه شامل سه مرحله است.[8]

1. شناسایی منافع عامه در افشای اطلاعات .
2. شناسایی منافع عامه در عدم افشای اطلاعات.
3. تعیین اهمیت نسبی منافع عامه به نفع و مخالف افشاگری و تعیین توازن بین آن منافع.

علیرغم موضع روشن قوانین استرالیا برای افشای

7 http://www.right2info.org/exceptions-to-access/harm-and-public-interest-test

8 http://www.ipc.nsw.gov.au/fact-sheet-what-public-interest-test

اطلاعات، قوانین ولایتی در مورد دسترسی به اطلاعات موقعیت‌های متعددی را ایجاد می کند که در آن فرض بر این است که عدم افشای اطلاعات و پنهان‌کاری بهتر از افشای آن است. برجسته‌ترین آنها اطلاعاتی است که بر قوانین محرمیت ارجعیت دارند - از 26 فعالیت به طور خاص نام برده شده است. این امر از یک گرایش عمومی که بر بسیاری از کشورهای سازمان همکاری و توسعه اقتصادی تأثیر می‌گذارد، پیروی می‌کند، جاییکه قوانین آزادی اطلاعات درعمل در مورد قوانین سنتی مربوط به اسرار دولتی بی ربط است. اسرار دولتی دائماً بیرون از محدوده قوانین مربوط به آزادی دسترسی به اطلاعات است. علاوه بر این، اکثر کشورها تمایل زیادی برای هماهنگی بین قوانین سنتی تنظیم کننده امنیت دولت با قوانین جدید در زمینه آزادی دسترسی به اطلاعات عمومی ندارند.

دواقعیت این است که بسیاری از قوانین مربوط به آزادی اطلاعات تقریبا بر محرمیت اطلاعات مربوط به امنیت ملی تاثیر نمی‌گذارد، به این معنی که قانونگذاری و مراجعه به دادگاه‌ها تاکنون به عنوان ابزارهایی برای کاهش روند جهانی استفاده بیش از حد از محرمیت و پنهان‌کاری در فعالیت‌های نهادهای امنیتی و استخباراتی موثر نبوده است. چنین نهادهایی، علیرغم گرایش گسترده بین‌المللی به سوی شفافیت عمومی بیشتر و خواسته‌های جامعه مدنی برای "حق دانستن"، با شیوه سنتی و غالباً مبهم خود در برخورد با اطلاعات محرمانه اساسا تحت تاثیرقوانین آزادی اطلاعات قرار نگرفته‌اند.

همه اینها به این واقعیت اشاره می‌کند که تصویب قوانین کلی که در برقراری توازن بین محرمیت و باز بودن (علنی بودن) موثر باشد هم از نظر مفهومی و هم از نظر عملی چالش برانگیز است. یکی از دلایل این امر این است که نهادها یا ادارات دولتی که اغلب به طبقه‌بندی اطلاعات محرمانه می‌پردازند، معمولاً اهداف و انگیزه‌های کاملاً متفاوتی در کار و عملکرد خود دارند. این امر فرهنگ‌های مختلف اداری مربوط به امنیت را تقویت می‌کند. به عنوان مثال، نهادهای نظامی عمدتا بر تکنالوژی سلاح و پلان‌های عملیاتی تمرکز می‌کنند، سازمان‌های استخباراتی بر حفاظت از منابع و روش‌های عملیاتی تمرکز می‌کنند، دیپلمات‌ها نگران پیامدهای بین‌المللی حفظ اطلاعات یا افشای اطلاعات (محرمیت یا عدم محرمیت) دیپلماتیک هستند و پلیس مشتاق محافظت از پلان‌های اطلاع‌رسانی و عملیاتی است. علاوه بر این، واضح است که در اداراتی مانند موارد ذکر شده مردم ترجیح می‌دهند برای جلوگیری از مشکلات غیر ضروری که اغلب منجر به طبقه‌بندی بیش از حد اطلاعات محرمانه می شود، به شکل ایمن تری عمل کنند (Aftergood, 2009).

در نتیجه ، ناظران و متخصصان آگاه تصور می‌کنند که حتی اگر ضروری است تا طبقه‌بندی اطلاعات محرمانه توسط اداره مربوطه انجام شود، نهاد لغو کننده طبقه‌بندی اطلاعات محرمانه باید بیرون از آن اداره باشد. این بهترین راه برای خنثی‌سازی تمایل اداره‌ای است که منافع خود را بر منافع دیگران ترجیح می‌دهد و بهترین راه برای پاکسازی آن از افراط در طبقه‌بندی اطلاعات است (Aftergood, 2009 page 412). بعضی تلاش‌های موفقیت آمیز برای انجام این کار در ایالات متحده انجام شده است، به عنوان مثال، توسط هیئت درخواست *طبقه‌بندی امنیتی بین‌الادارای*[9] (ISCAP) و مرور *پالیسی طبقه‌بندی اساسی* (FCPR).[10] در فرانسه، CSDN مثال دیگری ارائه می‌دهد (به بالا مراجعه کنید). تجربه ایالات متحده ، همانطور که در Aftergood (2009) تشریح شد، نشان می‌دهد که "اگر یک سازمان نتواند با موفقیت به یک مقام ارشد یا هیئت نمایندگی‌های دیگر توضیح دهد و آنها را متقاعد کند که چرا طبقه‌بندی اطلاعات محرمانه برای امنیت ملی مورد نیاز است". بنابراین دلیلی بر ادامه طبقه‌بندی اطلاعات وجود ندارد.

9 https://www.archives.gov/declassification/iscap

10 https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/ODNI%20FY2017%20FCGR.pdf :See also the 1994 pioneering review in the Energy Department at: https://www.osti.gov/opennet/forms.jsp?formurl=od/fcprsum.html

نتیجه‌گیری

1. قانون تنظیم محرمانه بودن اطلاعات در عرصه‌های امنیتی و دفاعی ضروری است و باید تا آنجا که ممکن است دقیق باشد. چنین قانونی باید معیارهای لازم را برای طبقه‌بندی اطلاعات محرمانه و همچنین لغو آن تعیین کند، با توجه به اینکه این قانون معمولاً ماهیت کلی دارد و در نتیجه معیارها نیز کلی خواهند بود. قانون تنظیم محرمانه بودن که در بسیاری از کشورها بر قانون دسترسی آزاد به اطلاعات مقدم است باید با قانون مربوط به دسترسی آزاد به اطلاعات هماهنگی ایجاد کند تا از ناهماهنگی در نظم حقوقی ملی جلوگیری شود.

2. در کنار یک چارچوب حقوقی مناسب، اطمینان از مدیریت آگاهانه و ماهرانه در سطح اداری برای اعمال معیارهای طبقه‌بندی اطلاعات حقوقی به شیوه ای منطقی و محتاطانه برای به حداکثر رساندن ارزشهای دموکراتیک و اصل شفافیت عمومی ضروری است. درک آگاهانه نیاز به توازن در ملاحظات مختلف باید بخشی از فرهنگ سازمانی باشد. روسای ادارات مربوطه باید برای دستیابی به یک رویکرد متوازن بین محرمانه بودن مشروع و شفافیت مشروع تلاش کنند.

3. کاهش طبقه‌بندی غیرموجه و بیش از حد اطلاعات محرمانه و همچنین ایجاد توازن بین حق دانستن مردم و ضرورت‌های امنیت ملی- و سایر دلایل مشروع محرمیت - کار دشواری است. تبدیل فرهنگ پنهان کاری به فرهنگ شفافیت در عرصه دفاعی احتمالاً در آینده نزدیک در اکثر کشورهای اتحادیه اروپا و کشورهای سازمان همکاری و توسعه اقتصادی بعید است.[11]

4. انتظار می‌رود که کارمندان و سایرین که در سکتور امنیتی و دفاعی کار می‌کنند وفادار بوده و طرزالعمل‌های تعیین‌شده را رعایت کنند. این ویژگی‌ها در واقع ضروری هستند، اما هنوز هم می‌توان، و لازم است، تا یک اندازه نوآوری و ایده های جدید را تشویق کنیم، حتی اگر امکان تغییر ناچیز به نظر برسد. با این وجود، لازم است نگاهی انتقادی به چگونگی دستیابی به توازن مطلوب بین محرمیت مشروع، از یک سو، و دسترسی مشروع به اطلاعات، از سوی دیگر، داشته باشیم.

5. پرسنل مسئول اجرای قوانین محرمیت یا پالیسی‌های محرمیت نیاز به آموزش‌های تخصصی دارند تا بتوانند به الزامات دموکراتیک برای باز بودن (علنی بودن) اطلاعات و شفافیت مورد نیاز حکومت پاسخ دهند. آیا در پرتو قانون چه اطلاعاتی باید از چشم عموم پنهان بماند. باز بودن (علنی بودن) بی‌رویه جایگزینی برای محرمیت بی‌رویه نیست. کیفیت کار و شایستگی پرسنل امنیتی و دفاعی بسیار مهم است، زیرا این امر پیامدهای مستقیم روی یک جامعه دموکراتیک و همچنین روی روابط بین نهادهای امنیتی و جامعه مدنی دارد.

6. یک نهاد مستقل، برای مثال یک کمیسیون بین‌الاداری لغو طبقه‌بندی اطلاعات محرمانه که خارج از حوزه نفوذ نهادهای مهم محرمانه مانند ارتش، استخبارات و پلیس فعالیت می‌کند، باید به طور دوره‌ای قدرت بازبینی و لغو طبقه‌بندی اطلاعات محرمانه‌ای که ادارات خواهان پنهان کردن آن هستند، را داشته باشد. به طور کلی، ثابت شده است که دادگاه‌ها درقبال امتیازات اجرایی اسرار دولتی متمایز هستند و دلایل محدودی برای تغییر در این عرصه وجود دارد.

11 Even if Romania seems to have managed to do so (Matei, 2007).

7. به نظر می‌رسد عملکردهای خوبی که در حال ظهور هستند در مقایسه با عملکردهای سنتی طبقه‌بندی اطلاعات محرمانه اختیارات سلیقه‌ای را کاهش داده‌اند. تصمیم راجع به طبقه بندی و لغو طبقه بندی اطلاعات محرمانه نباید توسط یک فرد گرفته شود، بلکه توسط یک کمیته یا کمیسیون مستقل، که قادر به قضاوت بی طرفانه راجع به ضرورت طبقه‌بندی یا لغو طبقه‌بندی به شکل کامل یا جزئی باشد، گرفته شود. چنین واحد تخصصی باید با معیارهای قانونی تعیین‌شده جهت تشخیص آسیب و انجام آزمایش‌های متوازن هدایت شود. تعداد اعضای این کمیته یا کمیسیون مستقل باید محدود باشد، به عنوان مثال، 5 تا 7 عضو و همچنین می‌تواند شامل کارشناسان امنیتی از قوه مجریه، پارلمان، نماینده‌گان مردم، مدافعین حقوق بشر و قوه قضاییه باشد.

فهرست منابع

Aftergood, Steven (2009):"*Reducing Government Secrecy: Finding What Works*," in Yale Law & Policy Review

Vol. 27, No. 2 (Spring, 2009), pp. 399-416. Available at: https://www.jstor.org/stable/40239716?seq=1#page_scan_tab_contents

Fenster, Mark (2010): *Seeing the State: Transparency as Metaphor*, in Administrative Law Review, pages 617-672, available at http://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=1571&context=facultypub

Fuchs, Meredith (2006): *Judging Secrets: The Role Courts Should Play in Preventing Unnecessary Secrecy*, in Administrative Law Review, Volume 58, Number 1, Winter 2006, pages 131-176.

Jacobsen, Amanda L. (2013): *National Security and the Right to Information in Europe*. Available at: http://www.right2info.org/resources/publications/national-security-page/national-security-expert-papers/jacobsen_nat-sec-and-rti-in-europe

Matei, Florina Cristiana (2007): *Reconciling Intelligence Effectiveness and Transparency: The Case of Romania*, in Strategic Insights, Volume VI, Issue 3 (May 2007). Available at: https://calhoun.nps.edu/bitstream/handle/10945/11297/mateiMay07.pdf?sequence=1

OECD (2010), "*The Right to Open Public Administrations in Europe: Emerging Legal Standards*",

SIGMA Papers, No. 46, OECD Publishing, Paris. At: http://dx.doi.org/10.1787/5km4g-0zfqt27-en

Riese, Dorothée (2014): *Secrecy and Transparency*, paper resented at the ECPR Conference in Glasgow , September 3-6, 2014. Available at: https://ecpr.eu/Filestore/PaperProposal/2cedead9-5191-42de-ae36-7d320a28a304.pdf

Sartre, Patrice & Ferlet, Philippe (2010): *Le secret de défense en France* in Revue Études 2010/2, Tome 412, février, pages 165-175. At : https://www.cairn.info/revue-etudes-2010-2-page-165.htm

Sauvé, Jean-Marc (2011): *Culture du secret contre transparence sans limite : quel équilibre pour garantir l'intérêt général ? Transparence, valeurs de l'action publique et intérêt général*, discours à l'Assemblée Nationale le mardi 5 juillet 2011 au colloque organisé par Transparence Internationale France. Disponible à : http://www.conseil-etat.fr/content/download/2597/7819/version/1/file/discours-transparence-international.pdf

Setty, Sudha (2012): *The Rise of National Security Secrets*, in Connecticut Law Review, volume 44, number 5, July 2012, pages 1563-1582.

Transparency International UK (2014): Classified Information: A Review of 15 Countries. Available at: http://ti-defence.org/wp-content/uploads/2016/03/140911-Classified-Information.pdf

مجموعه رهنمودهای حکومت‌داری خوب


رهنمود های
حکومت داری
خوب
شماره 4
دسترسی به معلومات
و شفافیت عمومی
Centre for Integrity
in the Defence Sector


رهنمود های
حکومت داری
خوب
شماره 5
مدیریت ریسک فساد
و جعل در دارایی‌های
دولتی در سکتور دفاعی
Norwegian Ministry
of Defence
Centre for Integrity
in the Defence Sector

رهنمودهای حکومت‌داری خوب مجموعه‌ای از نوشتارهای کوتاه است که هر کدام یک عنوان مشخص و مهم مرتبط با حکومت‌داری خوب در سکتور دفاعی را مورد بحث قرار می‌دهد. افرادی که علاقمند به کسب آگاهی بیشتر راجع به یک یا چندین عنوان مستقیما مرتبط با حکومت‌داری خوب در سکتور دفاعی – و یا به صورت عموم در سکتورعامه می‌باشند می‌توانند این نوشتارها را مطالعه نمایند. این نوشتارها همچنین می‌تواند برای مقاصد آموزشی مورد استفاده قرار گیرد.

منتشر شده توسط مرکز درستکاری در سکتور دفاعی
طراحی: www.melkeveien.no
چاپ: سازمان خدمات و امنیت دولتی نروژ
می 2018

ترجمه نسخه اصلی انگلیسی به دری توسط سازمان پیمان اتلانتیک شمالی (ناتو) انجام شده است

CENTRE FOR INTEGRITY IN THE DEFENCE SECTOR
www.cids.no