مطالعات حقوق تطبیقی
دورهٔ ۵، شمارهٔ ۲،
پاییز و زمستان ۱۳۹۳
صفحات ۵۳۵ تا ۵۵۷

افشای اطلاعات طبقه‌بندی‌شده از سوی پایگاه ویکی‌لیکس؛ تقابلی نوین میان حق دسترسی به اطلاعات و امنیت ملی

عباسعلی کدخدایی *

دانشیار گروه حقوق عمومی دانشکدهٔ حقوق و علوم سیاسی دانشگاه تهران

هیوا حاجی‌ملا

دانش‌آموختهٔ کارشناسی ارشد حقوق بین‌الملل دانشکدهٔ حقوق و علوم سیاسی دانشگاه تهران

(تاریخ دریافت:۱۳۹۲/۳/۲۰- تاریخ پذیرش:۱۳۹۳/۴/۱۳)

چکیده

افشای اطلاعات طبقه‌بندی‌شدهٔ مرتبط با نفع عموم، به یکی از چالش‌های عمدهٔ حقوقی در چند سال اخیر تبدیل شده است. در دهه‌های گذشته تقابل میان حق مردم به دریافت اطلاعات و «اصل حاکمیت و رضایت قبلی» در قالب رسانه‌های سنتی (پخش مستقیم ماهواره‌ای) به نفع «اصل جریان آزاد اطلاعات» حل شد و محدودیت امنیت ملی جایگزین تقابل شد. اما امروزه پایگاه ویکی‌لیکس با دسترسی به اطلاعات طبقه‌بندی‌شدهٔ دولت‌ها و انتشار آن‌ها، تقابل نوینی از حق دسترسی به اطلاعات دولتی و امنیت ملی دولت‌ها را به نمایش گذاشته است. ازاین‌رو در پژوهش پیش‌روی برآنیم تا ضمن بررسی این تقابل، دربارهٔ راه‌های حقوقی تعامل و همزیستی افشای اطلاعات طبقه‌بندی شده و امنیت ملی در قالب حق دسترسی به اطلاعات و اسناد دولتی به کاوش بپردازیم.

واژگان کلیدی

اطلاعات طبقه‌بندی‌شده، اطلاعات مرتبط با نقض حقوق بشر، امنیت ملی، حق دسترسی به اطلاعات، ویکی‌لیکس.

---

* نویسنده مسئول فاکس ۰۲۱-۶۶۴۰۹۵۹۵ aliyary1385@gmail.com
Hajimolla_Hiwa@yahoo.com

مقدمه

نشر اسناد طبقه‌بندی‌شدهٔ دولتی از سوی یک پایگاه اینترنتی از جمله رویدادهای نادر دوران ما است که در قرن بیستم تصور آن سخت بود. بااین‌حال بیش از پنج سال است که پایگاه اینترنتی ویکی‌لیکس تمام شهرتش را مدیون انتشار این اسناد و تصاویر طبقه‌بندی‌شده است. این پایگاه با افشای اطلاعات طبقه‌بندی شدهٔ دولت‌ها، با اینکه یکی از اصول اساسی تأمین امنیت ملی دولت‌ها یعنی حفظ محرمانگی اطلاعات را نقض کرده، اما اطلاعات ارزشمندی از فساد رهبران و نقض حقوق بشر و بشردوستانه از سوی دولت‌های مدعی رعایت حقوق بشر را در اختیار جامعهٔ بین‌المللی قرار داده است. ویکی‌لیکس در سال ۲۰۰۷م با انتشار اسنادی از دولت کنیا، اقدامات خود را شروع کرد. از مهم‌ترین آن‌ها می‌توان به اسنادی در خصوص فساد رهبران کنیایی، به‌ویژه دانیل ارپ موی، اشاره کرد (Benkler, 2011, p. 316). در سال ۲۰۰۹م نیز اسنادی در زمینهٔ کشتارهای فراقضایی و ناپدیدسازی در کنیا را منتشر ساخت و تا مدت‌ها بیشتر فعالیت‌های خود را بر این کشور متمرکز ساخت. اما بعد از سال ۲۰۰۹م فعالیت پایگاه گسترش یافت، به‌طوری که امروزه چالش‌برانگیزترین اسناد انتشاریافته که ویکی‌لیکس بیشترین شهرت خود را مدیون آن‌هاست، اسناد دولتی امریکا است که عمده‌ترین اسناد منتشرشدهٔ پایگاه را به خود اختصاص داده است.

به دنبال انتشار اسناد طبقه‌بندی شده، تعدادی از دولت‌ها آن را مداخله در امور داخلی خود قلمداد کرده، خواستار توقف فعالیت پایگاه شدند. اما از آنجا که بیشتر اسناد انتشاری متعلق به ایالات متحدهٔ امریکا بود، این کشور بی‌درنگ اقدامات پایگاه را محکوم و انتشار این اسناد را «تهدید علیه امنیت ملی امریکا» قلمداد کرد (Kyle, 2012, p. 424). در همین راستا بسیاری از نمایندگان کنگرهٔ امریکا خواهان شناسایی این پایگاه به عنوان یک سازمان تروریستی شدند (Benkler., op. cit., p. 331). اما ویکی‌لیکس اقدامات خود را در راستای اعمال مادهٔ ۱۹ اعلامیهٔ جهانی حقوق بشر می‌داند که به‌موجب آن هر فردی حق دارد به درست‌ترین اخبار و اطلاعات داخلی و خارجی فارغ از شکل و چگونگی تحقق آن دسترسی داشته باشد. ازآنجا که اطلاعات موردنظر این ماده به‌عنوان بخشی از آزادی بیان قلمداد شده، حقی است بشری که همهٔ افراد حق دسترسی به چنین اطلاعاتی را فراتر از مرزها در قالب هر نوع رسانه‌ای دارند. بر همین اساس این نوع اطلاعات همگانی است که می‌توان آن را در قالب «جریان آزاد اطلاعات» قرار داد. اما اطلاعاتی که پایگاه در زمینهٔ انتشار آن‌ها فعالیت می‌کند، «اطلاعات نگهداری‌شده در

نهادهای دولتی» است. دسترسی به اطلاعات و اسناد دولتی، حقی است برخاسته از مسئولیت دولت که متضمن تعهد دولت در ارائهٔ اطلاعات و حق مردم در دریافت آن‌هاست. بنابراین، جستجو و انتشار این اطلاعات حقی ویژه را می‌طلبد که متعلق به روزنامه‌نگاران است؛ چراکه در هر کشوری آن‌ها به دلیل نقش عمده‌ای که در راستای منافع جمعی و به‌عنوان دیدبان دارند، از «حق جستجوی اطلاعات دولتی» برخوردارند.

اما حق دسترسی به اطلاعات و اسناد دولتی نیز مانند سایر حقوق و آزادی‌های فردی با محدودیت امنیت ملی همراه است. به این منظور بیشتر دولت‌ها سیستم طبقه‌بندی اطلاعات را پذیرفته‌اند، تا به این وسیله میان نیاز دولت به حفظ محرمانگی و حق مردم به دریافت اطلاعات دولتی، تعادل ایجاد شود. اما ازآنجا که مفهوم امنیت ملی مبهم است و دولت‌ها بر اساس تفسیر خود اطلاعات را طبقه‌بندی می‌کنند، این سیستم ضرورتاً شهروندان و جامعهٔ بین‌المللی را از دسترسی به اطلاعات دولتی در بسیاری از موضوعات مهم محروم می‌کند (Barandes, 2007, p.381). به این منظور در بیشتر کشورهای دارای قوانین دسترسی به اسناد و اطلاعات دولتی، فرض «افشای حداکثری اطلاعات»، از افشای اطلاعات مرتبط با نفع عموم و همراه با حسن‌نیت افراد حمایت می‌کند. پایگاه ویکی‌لیکس با نادیده گرفتن نیاز دولت‌ها به حفظ محرمانگی اطلاعات و انتشار آن‌ها، توانسته است اطلاعات مرتبط با نفع عموم را افشا کند و حق مردم به دریافت اطلاعات و اسناد دولتی را جامهٔ عمل بپوشاند.

اگرچه در دهه‌های ۸۰ و ۹۰ میلادی جدال میان طرف‌داران «حق مردم به دریافت اطلاعات»، یعنی کشورهای غربی، و حامیان «اصل حاکمیت و رضایت قبلی»، یعنی روسیه و کشورهای جهان سوم، در قالب رسانه‌های سنتی (پخش مستقیم ماهواره‌ای) به نفع «اصل جریان آزاد اطلاعات» حل شد و محدودیت امنیت ملی جایگزین تقابل شد، امروزه تقابلی نوین را در عرصهٔ رسانه‌های نو شاهد هستیم.

ازاین‌رو پژوهش حاضر با فرض روزنامه‌نگار قلمداد کردن پایگاه ویکی‌لیکس، بر آن است تا ضمن پرداختن به حق دسترسی به اطلاعات دولتی، چگونگی برخورد آن با امنیت ملی را بررسی کند. در ادامه تلاش خواهد شد به واکاوی راه‌های حقوقی تعامل و همزیستی افشای اطلاعات طبقه‌بندی شده و امنیت ملی در قالب حق دسترسی به اطلاعات و اسناد دولتی پرداخته شود تا از این طریق بتوان تقابل جریان آزاد اطلاعات دولتی و امنیت ملی دولت‌ها را در فضای بدون مرز اینترنت حل کرد.

دسترسی به اطلاعات دولتی در اینترنت؛ کشاکشی میان حق و تهدید امنیت ملی

۱. حق دسترسی به اطلاعات دولتی

در مقررات بین‌المللی حقوق بشر، اطلاعات به دو دستهٔ «اطلاعات عموماً در دسترس» (Generally Accessible) و «اطلاعات نگهداری‌شده از سوی نهادهای دولتی» (Information Held by Government) تقسیم می‌شود[۱]. بر مبنای این تفکیک، حق دسترسی به اطلاعات نیز به دو دستهٔ کلی «حق دسترسی به اطلاعات دولتی» و «حق دسترسی به اطلاعات همگانی» قابل تقسیم است.

حق دسترسی به اطلاعات دولتی در مقایسه با اطلاعات همگانی عمر چندانی ندارد. این حق به معنای «توانایی افراد در دسترسی به اطلاعاتی است که در اختیار دولت است» (نمک‌دوست تهرانی، ۱۳۸۳، ص۶۴). «حق به دانستن»، « حق بر اطلاعات» و «آزادی اطلاعات» از دیگر مفاهیمی است که برای اشاره به این حق استفاده می‌شود. قلمرو شمول حق دسترسی به اطلاعات دولتی تا حد زیادی متغیر است و هر دولتی با توجه به ساختار حکومتی خود آن را تنظیم می‌کند (انصاری، ۱۳۸۷، ص۶۷).

۱.۱. ابعاد حق دسترسی به اطلاعات دولتی

۱.۱.۱. دسترسی به اطلاعات شخصی. حق دسترسی در این بعد به معنای توانایی افراد در دسترسی به اطلاعاتی است که دولت دربارهٔ آن‌ها جمع‌آوری کرده است. هر فرد باید قادر به تشخیص نهادها یا ارگان‌هایی که اطلاعات شخصی او را نگهداری می‌کنند، باشد. دسترسی فرد به اطلاعات دولتی در این بعد، او را قادر می‌سازد تا در مقابل سوءاستفاده احتمالی دولت از خود دفاع کند. همچنین بسیاری از حقوق افراد که در معاهدات حقوق بشری مقرر شده است، به‌طور مستقیم با حق دسترسی به اطلاعات

---

۱. چنین تفکیکی را می‌توان در تفاسیر عمومی کمیتهٔ حقوق بشر از مادهٔ ۱۹ میثاق مشاهده کرد؛ برای مثال ر.ک.

Human Right Committe.,*General comment, No. 34, op. cit.*, para. 18

همچنین می‌توان به قضایایی که دیوان اروپایی حقوق بشر مادهٔ ۱۰ کنوانسیون اروپایی حقوق بشر را تفسیر کرد و در آن‌ها میان این دو دسته اطلاعات تفکیک قائل شد، اشاره کرد؛ برای مثال نک:

Case of Gaskin v. The United Kingdom,7 July 1989 , para. 31, or Case of Leander v. Sweden, 26 March 1981 , para. 26.

نگهداری‌شده از سوی نهادهای دولتی ارتباط دارد و اگر افراد توانایی دسترسی به این اطلاعات را نداشته باشند، از عهدهٔ استیفای کامل حقوق خود برنمی‌آیند؛ برای مثال می‌توان به حق بر حریم خصوصی اشاره کرد.

یکی از مهم‌ترین مفاهیمی که در تعریف حریم خصوصی به آن استناد می‌شود، کنترل بر «اطلاعات شخصی» است. بسیاری از این اطلاعات از سوی نهادهای دولتی نگهداری می‌شوند و افراد در صورت نیاز به اطلاعات، می‌توانند آن را درخواست کنند. دیوان اروپایی حقوق بشر در آرای زیادی به مادهٔ ۸ کنوانسیون اروپایی حقوق بشر در خصوص حق دسترسی افراد به اطلاعات استناد کرده است[۲] که برای مثال می‌توان به قضیهٔ روتارو و رومانی اشاره نمود. در این قضیه، خواهان خواستار استفاده از یک فایل حاوی اطلاعات شخصی بود که از سوی سرویس اطلاعاتی رومانی نگهداری می‌شد و دولت رومانی با رد درخواست او اجازهٔ این کار را به وی نداد. بنابراین با اقامهٔ دعوا در دیوان، دادگاه رای داد که رد درخواست ارائهٔ اطلاعات مربوط به زندگی شخصی، نقض مادهٔ ۸ کنوانسیون شمرده می‌شود. (ECtHR, 4 May 2000, para 46) . به‌این‌ترتیب دیوان با تفکیک نوع تعهد دولت، حق دسترسی به اطلاعات شخصی را نه به‌عنوان نقض مادهٔ ۱۰ در خصوص آزادی بیان، بلکه به‌عنوان نقض مادهٔ ۸ کنوانسیون لحاظ کرد. کمیتهٔ حقوق بشر نیز برای حمایت مؤثر از حریم خصوصی در نظریهٔ عمومی خود از مادهٔ ۱۷ اعلام کرد: «هر فردی باید قادر به تشخیص نهادهای دولتی یا خصوصی که بر اطلاعات شخصی او کنترل دارند، باشد. اگر فایل‌های شخصی او دربردارندهٔ اطلاعات نادرست یا برخلاف قانون باشد، فرد باید قادر به درخواست اصلاح یا حذف آن اطلاعات باشد» (H. R. Committee, 1988, para. 10).

۲.۱.۱. دسترسی به اطلاعات عمومی. در این بعد، حق دسترسی به اطلاعات در دو سطح داخلی و بین‌الملل قابل بررسی است.

آشناترین و معمول‌ترین سطح حق دسترسی به اطلاعات، حق دسترسی به اطلاعات در سطح داخلی یک جامعه به‌عنوان یک «حق شهروندی» است. حقوق بین‌الملل با به‌رسمیت شناختن اصل حاکمیت دولت‌ها، دولت‌های دیگر را از مداخله در امور داخلی آن‌ها برحذر داشته، سرنوشت داخلی یک جامعه را به‌دست افراد آن جامعه می‌سپرد؛ برای نمونه می‌توان به مادهٔ ۲۵ میثاق بین‌المللی حقوق مدنی سیاسی اشاره کرد که حق

---

۲. متن مادهٔ ۸ کنوانسیون اروپایی حقوق بشر چنین است: «هر کسی حق بر رعایت زندگی خصوصی و خانوادگی، منزل و ارتباطاتش را دارد».

شهروندان به مشارکت در امور سیاسی را به‌رسمیت می‌شناسد، « اما امروزه دمکراسی معنایی فراتر از برگزاری صرف انتخابات و برخورداری از حق رای یافته است؛ به بیان دقیق‌تر، جامعهٔ نوین بر پایهٔ رضایت شهروندان آگاه و مشارکت آگاهانهٔ آنان در فرایندهای سیاسی بنا شده است» (نمک‌دوست تهرانی، ۱۳۸۳، ص۶). بنابراین درصورتی شهروندان قادر خواهند بود حقوق دمکراتیک خود را اعمال کنند که از طریق سازوکارهای پیش‌بینی شده در قوانین آزادی اطلاعات، به اسناد مربوط دسترسی داشته باشند. این دسترسی مقدمه‌ای خواهد بود برای پاسخ‌گویی دولت در مقابل شهروندان؛ شهروندانی که صاحبان اصلی قدرت‌اند.

دسترسی به اطلاعات دولتی در سطح بین‌الملل به‌عنوان یک «حق بشری» یکی از حوزه‌های نسبتاً جدید این حق به‌شمار می‌رود که در آن نه‌تنها شهروندان، بلکه همهٔ افراد فارغ از ملیت، ذی‌حق شمرده می‌شوند. هرچند ریشه‌های اصلی این حق به دههٔ ۸۰ میلادی برمی‌گردد، اما تحولات حقوق بین‌الملل و به‌ویژه حقوق بشر در دههٔ اخیر باعث شناسایی گستردهٔ این حق در سطح بین‌المللی شده است که در دو حوزه نمود یافته است؛ یکی «حق دسترسی به اطلاعات زیست‌محیطی» و دیگری «حق بر دانستن حقیقت». موضوع حق بر دانستن حقیقت، بیشتر دسترسی به اسناد و اطلاعات مرتبط با نقض حقوق بشر و حقوق بشردوستانه است. حق یادشده زمانی نقض می‌شود که به دنبال نقض یک سری از حقوق بشر، مقامات دولتی از ارائهٔ اطلاعات مربوط به زمینه‌های نقض خودداری کنند (Naqvi, 2006, 249) .

۲.۱. جریان آزاد اطلاعات دولتی از طریق اینترنت

همان‌طور که ملاحظه شد، دسترسی به اطلاعات شخصی از حقوق فردی شمرده می‌شود و هر شخصی به‌واسطهٔ داشتن حق بر حریم خصوصی و دادرسی عادلانه می‌تواند خواستار دسترسی به این اطلاعات باشد. اما دسترسی به اطلاعات عمومی، اسنادی را شامل می‌شود که بدون درخواست دسترسی به آن‌ها، دولت متعهد به ارائهٔ آن‌ها از طریق رسانه‌های جمعی است. اما حق شهروندان به دریافت اطلاعات دولتی، در بیشتر زمینه‌ها با نقض تعهد از جانب دولت روبه‌رو بوده است؛ چراکه آنان اغلب اطلاعاتی را ارائه می‌دهند که در راستای تأیید مشروعیتشان باشد.

اینترنت با پتانسیل‌ها و مزایای منحصربه‌فرد خود توانست این خلأ را پر کرده، حق مردم به دریافت اطلاعات را به‌عنوان ناظر فعالیت‌های دولت عملی سازد؛ به‌طوری‌که

امروزه هر فردی که به اسناد مربوط به ناکارآمدی، نقض قانون و نقض حقوق و آزادی‌های فردی از سوی دولت دسترسی دارد، می‌تواند با قرار دادن آن‌ها در محیط اینترنت، حق مردم به دریافت اطلاعات دولتی را تحقق بخشد.

۲.۲. انتشار اطلاعات مرتبط با امنیت ملی؛ جلوه‌گاه تقابل

اطلاعات مرتبط با امنیت ملی، اطلاعاتی هستند که یا به‌واسطهٔ ماهیت خود اطلاعات یا نهادهای درگیر و یا زمان تولید آن‌ها از حساسیت امنیتی برخوردارند و نباید عموم مردم به آن دسترسی داشته باشند. دولت‌ها در قوانین داخلی خود از «طبقه‌بندی اطلاعات» برای محدودسازی دسترسی افراد به اطلاعات مرتبط با امنیت ملی استفاده می‌کنند. محدودیت‌های متفاوتی در اننتشار اطلاعات بر اساس سطح طبقه‌بندی ایجاد می‌شود؛ برای مثال اطلاعاتی که به‌عنوان «فوق سری» طبقه‌بندی شده‌اند، حمایت‌های محرمانه بیشتری را از اطلاعاتی که صرفاً به عنوان اطلاعات «سری» طبقه‌بندی می‌شوند، نیاز دارد (Kovarovic, 2011, p. 275).

قرار دادن اطلاعات دولتی در اینترنت و انتشار آن‌ها در راستای حق مردم به دریافت اطلاعات، خود اتفاق خجسته‌ای است، اما قابلیت‌های اینترنت این توانایی را برای افراد ایجاد کرده است که بدون توجه به نوع اطلاعات دولتی، اطلاعات طبقه‌بندی شده را نیز در محیط اینترنت قرار دهند؛ به‌طوری که امروزه پرده‌برداری از اسرار دولتی از طریق اینترنت به یک موضوع چالش‌برانگیز حقوقی تبدیل شده است. در یک سو، منتقدان دولت و ناراضیان از وضعیت حقوق بشر با استفاده از اینترنت و نیز اطمینان از گمنامی، این توانایی را به‌دست آورده‌اند که پیام خود را بدون مداخلهٔ دولت منتشر، و از اینترنت به‌عنوان سلاحی علیه فساد دولت‌ها استفاده کنند.از دیگر سو، انتشار اطلاعات دولتی بدون توجه به نوع اطلاعات، اصول محرمانگی اطلاعات امنیتی دولت را به‌عنوان یکی از مؤلفه‌های اصلی تأمین امنیت ملی با چالش روبه‌رو می‌سازد و به این طریق امنیت ملی کشورها با تهدید مواجه می‌شود (Opper, 2011, p. 237) .

بررسی حق بر افشای اسناد طبقه‌بندی شدهٔ امریکا از سوی پایگاه ویکی‌لیکس در توازن با امنیت ملی

۱. معرفی پایگاه ویکی‌لیکس

ویکی‌لیکس (Wikileaks) نام یک پایگاه اینترنتی است که به‌وسیلهٔ یک گروه ناشناس از مهندسان کامپیوتر و فعالان سیاسی که مدعی مبارزه با فساد و رژیم‌های ستمگر در سراسر دنیا هستند، در سال ۲۰۰۶م در کشور سوئد پایه‌گذاری شد. ویکی‌لیکس اهداف اصلی خود را شفاف‌سازی عملکرد دولت‌ها، مبارزه با فساد حکومتی و ارتقای دموکراسی از این راه عنوان کرده است، و فعالیت‌های خود را در راستای اعمال مادهٔ ۱۹ اعلامیهٔ جهانی حقوق بشر می‌داند. این پایگاه ادعا می‌کند با افشای این اطلاعات، فساد کمتر، حکومت‌ها بهتر، و دمکراسی قوی‌تر می‌شود.

پایگاه در طول فعالیت کوتاه خود، بیش از چند صد هزار سند منتشر نموده است که به کشورهای زیادی مربوط می‌شوند؛ به‌طوری که نام بیشتر کشورها در فهرست اسناد ویکی‌لیکس به‌چشم می‌خورد. اما امروزه چالش‌برانگیزترین اسناد انتشاریافته که ویکی‌لیکس بیشترین شهرت خود را مدیون انتشار آن‌هاست، اسناد دولتی امریکا می‌باشد. پایگاه ویکی‌لیکس با انتشار این اسناد، جلوه‌گاه اصلی تقابل میان نیاز دولت به حفظ محرمانگی و حق مردم به دریافت اطلاعات را نشان داد. با توجه به این اسناد در این قسمت سعی خواهد شد به این پرسش پاسخ داده شود که به چه شکل می‌توان تقابل میان منافع دولت در حفظ محرمانگی اطلاعات و حق مردم در آگاه شدن از کارکرد دولت را حل کرد.

۲. مشروعیت طبقه‌بندی اطلاعات؛ تفسیری از بند ۳ مادهٔ ۱۹ میثاق

۱.۲. طبقه‌بندی نادرست اطلاعات و حق بر افشای آن‌ها

مادهٔ ۱۹ میثاق، اختیار ایجاد محدودیت بر مبنای امنیت ملی را به دولت‌ها داده و در بند ۳ مقرر داشته است که این محدودیت باید به‌موجب قانون تصریح شود. کمیتهٔ حقوق بشر نیز در تفسیر این بند مقرر می‌دارد: «محدودیت‌ها باید دارای شرایط زیر باشند: ۱) در قانون داخلی مقرر شده باشد.۲) آن‌ها باید فقط به دلایلی که در مادهٔ ۱۹ مقرر شده‌اند؛ تحمیل شوند» (H. R. Committee., General Comment no. 10, 1983. Para. 4).

بر همین اساس قوانین آزادی اطلاعات در بیشتر کشورها، «اطلاعات طبقه‌بندی شده» را به‌عنوان یک استثنا در راستای حمایت از منافع امنیت ملی پذیرفته‌اند؛ برای مثال می‌توان به قانون «انتشار و دسترسی آزاد به اطلاعات» جمهوری اسلامی ایران اشاره کرد که در مادهٔ ۱۳ اسناد و اطلاعات طبقه‌بندی شده را جزء استثنائات دسترسی به اطلاعات قرار داده است. قانون آزادی اطلاعات امریکا نیز به‌صراحت انتشار اطلاعات طبقه‌بندی شده را در صورت درخواست آن رد کرده است.

همان‌طور که ملاحظه می‌شود، هدف اصلی از ایجاد محدودیت بر مبنای امنیت ملی و اختیار دولت‌ها در طبقه‌بندی اطلاعات مرتبط با آن، از دسترس خارج کردن اسنادی است که دسترسی عامهٔ مردم به آن‌ها امنیت ملی را با تهدید روبه‌رو می‌سازد. این‌گونه اسناد شامل فیلم‌ها، دفاتر، پرونده‌ها، تصاویر، نقشه‌ها، نمودارها، نوارهای ضبط‌صوت و هرگونه اشیایی است که هدف اصلی از طبقه‌بندی آن‌ها، جلوگیری از آسیب مستقیم به امنیت ملی یا دیگر منافع حیاتی دولت مربوطه باشد (H. R. Council, 2012, para. 108). بنابراین، طبقه‌بندی اطلاعات برای حمایت از منافع غیرمرتبط با امنیت ملی مشروعیت ندارد (Stone, 2006, p. 93). همان‌طور که اصل ۱۲ مجموعهٔ اصول ژوهانسبورگ مقرر می‌دارد که ایجاد محدودیت در دسترسی به اطلاعات دولتی باید به منظور حفظ مصلحت مشروع امنیت ملی صورت گیرد؛ برای نمونه، اطلاعات نباید برای پنهان‌سازی نقض قانون، ناکارامدی، خطاکاری دولت، و یا پیشگیری از رسوایی شخص، سازمان یا مؤسسه طبقه‌بندی شوند(Papandrea, 2007, p. 242). اما امروزه طبقه‌بندی اطلاعات به سلاحی در دست دولت تبدیل شده است تا به‌وسیلهٔ آن اطلاعاتی را که مردم حق دریافت آن را دارند، برای پنهان کردن خطاکاری‌های حزبی و بی‌ارتباط با منافع مشروع امنیت ملی طبقه‌بندی کند[۳]. از طرفی دیگر، همواره امکان اشتباه در طبقه‌بندی اطلاعات وجود دارد.

بنابراین به‌موجب مجموعهٔ اصول ژوهانسبورگ، صرف طبقه‌بندی اسناد را نمی‌توان مانعی در حق دسترسی روزنامه‌نگاران به این اطلاعات محسوب کرد؛ چراکه هدف اصلی

---

۳. در این زمینه می‌توان به گزارش کمیته‌ای در امریکا اشاره کرد. این کمیته در مطالعاتی که بر روی اسرار دولتی دههٔ ۱۹۹۰ دولت امریکا انجام داده بود، در گزارش سال ۱۹۹۷م خود اعلام کرد که «سیستم طبقه‌بندی اغلب به‌منظور اهدافی غیرمرتبط با امنیت ملی به‌کار می‌رود، و فقط ۱۰ درصد اطلاعات دولتی، به‌منظور حفاظت از اسرار مشروع امنیت ملی طبقه‌بندی شده‌اند» (Kitrosser, 2012, pp. 427-428).

تدوین‌کنندگان مادهٔ ۱۹ میثاق، حمایت از امنیت ملی کشورهاست، نه اطلاعات طبقه‌بندی شدهٔ آن‌ها. نمونه‌هایی از اسناد افشاشده از سوی پایگاه ویکی‌لیکس را می‌توان در این دسته قرار داد؛ برای مثال اسناد مرتبط با فساد مقامات کنیایی که دربردارندهٔ هیچ‌گونه نفع مشروع امنیت ملی نبوده، صرفاً برای سرپوش نهادن بر خطاکاری رهبران کنیایی طبقه‌بندی شده بود (Yochai, 2011, p. 316).

۲.۲. اطلاعات درست طبقه‌بندی شده و بررسی امکان افشای آن‌ها

طبقه‌بندی اطلاعات مربوط به امنیت ملی زمانی به‌درستی انجام شده است که افشای آن‌ها خطرهایی برای امنیت ملی در پی داشته باشد (Papandrea, 2012, p. 98)؛ صرف نظر از اینکه این اسناد حاوی اطلاعاتی باشند که مشروعیت طبقه‌بندی آن‌ها مورد سؤال باشد، و صرف نظر از منفعت عمومی در این اطلاعات. بنابراین در این مرحله است که مسئله پیچیده می‌شود؛ چراکه این اسناد حاوی اطلاعاتی است که به‌درستی طبقه‌بندی شده‌اند و حفظ محرمانگی آن‌ها برای جلوگیری از تهدید امنیت ملی ضروری است و درعین‌حال دارای نفع عموم می‌باشند. از مهم‌ترین اسنادی که در این دسته قرار می‌گیرند، می‌توان به اطلاعات دیپلماتیک، جاسوسی و نظامی اشاره کرد. برای حفاظت از چنین اطلاعاتی، بیشتر کشورها افشای چنین اسنادی را جرم‌انگاری کرده، بالاترین مجازات‌ها را برای آن در نظر گرفته‌اند.

حال این پرسش مطرح می‌شود که آیا با توجه به ماهیت امنیتی این اطلاعات و درستی طبقه‌بندی آن‌ها، امکان افشای چنین اطلاعاتی وجود دارد یا خیر؟

ماهیت اطلاعات دیپلماتیک و جاسوسی چنان است که افشای آن‌ها موجب اختلال در کار سرویس‌های اطلاعاتی و دیپلماتیک می‌شود. کار دیپلماسی نیازمند آن است که مبادلهٔ اطلاعات میان مقامات بالای دیپلماتیک، آرام و بدون مداخلهٔ افراد بیرونی جریان یابد. اهمیت حمایت از کار مجموعه‌های دیپلماتیک در چندین قضیه از سوی دیوان اروپایی حقوق بشر به‌رسمیت شناخته شده است (ECtHR, 2006, Para. 52)؛ تاجایی که از نظر قاضی ویلدهابر در قضیهٔ استول و دولت سوئیس، همهٔ کشورها گزارش‌های دیپلماتیک خود را به‌صورت محرمانه طبقه‌بندی می‌کنند (Ibid, Para. 23). کنوانسیون ۱۹۶۱م وین نیز در خصوص روابط دیپلماتیک، محرمانگی همهٔ ارتباطات دیپلماتیک را در مواد ۲۴ تا ۲۷ خود به عنوان یک اصل عرفی حقوق بین‌الملل پذیرفته است (Ibid,2007, Grand Chamber, Para. 79).

دیوان اروپایی حقوق بشر در قضیهٔ گاردین و آبزرور، در خصوص انتشار اطلاعات طبقه‌بندی شدهٔ سرویس‌های اطلاعاتی انگلیس، دو دورهٔ زمانی پیش و پس از جولای ۱۹۸۷ را از هم تفکیک کرد. در دورهٔ اول انتشار، محتوای اطلاعات برای مردم ناشناخته بود و تنها پس از انتشار از سوی دو روزنامهٔ انگلیسی آبزرور و گاردین بود که مردم از این اطلاعات آگاه شدند. اما پس از انتشار کتاب مأمور اطلاعاتی در امریکا، ازآنجا که به تعبیر دادگاه « ماهیت محرمانهٔ اطلاعات از بین رفته بود» (ECtHR, 1991, para. 66)، قرار منع صادره از سوی دادگاه انگلیسی را برخلاف بند ۲ مادهٔ ۱۰ کنوانسیون اروپایی حقوق بشر اعلام کرد. بنابراین از نظر دادگاه تا زمانی که اطلاعات ماهیت محرمانه داشته باشند، حق بر انتشار این اطلاعات وجود ندارد. بنابراین تنها دولت است که تشخیص می‌دهد چه زمانی اطلاعات برای مردم افشا شود.

اما از دیدگاه کمیتهٔ حقوق بشر، وقتی دولت‌ها محدودیت‌هایی را در دسترسی به اطلاعات وضع می‌کنند، محدودیت‌ها نباید به‌گونه‌ای باشد که اصل حق را از اعتبار بیندازد (H. R. Committee, 2011, Para. 21)؛ یعنی اصل و قاعده را باید به‌صورت موسع، و استثنا را به‌صورت مضیق تفسیر نمود. بنابراین محدودیت بر مبنای امنیت ملی همواره باید در سایهٔ اصل حق مردم به دریافت اطلاعات دولتی تفسیر شود.

هرچند که تعرض‌ناپذیری اسناد دیپلماتیک در حقوق بین‌الملل، اهمیت محرمانگی در این قلمرو را نشان می‌دهد، اما افشای اسناد دیپلماتیک را نمی‌توان تحت پوشش مقررات تعرض‌ناپذیری آرشیوها و اسناد موجود در کنوانسیون وین قرار داد؛ چراکه این مقررات برای حمایت از آرشیوها و اسناد دولت فرستنده در مقابله با مداخلهٔ دولت دریافت‌کننده یا نهادهای تحت صلاحیت آن کشور می‌باشد.

بنابراین باوجود ضرورت حفظ کارکرد مؤثر مأموران دیپلماتیک و جریان آزادانهٔ اطلاعات میان آن‌ها، محرمانگی اطلاعات دیپلماتیک و جاسوسی را نباید به هر قیمتی حمایت کرد و همواره نقش ضروری روزنامه‌نگاران در انتقال اطلاعات مرتبط با نفع عموم را باید در نظر داشت (ECtHR, 2007,Para. 128)؛ چنان‌که دیوان اروپایی حقوق بشر در چندین قضیه صرف استناد دولت به طبقه‌بندی اطلاعات دیپلماتیک و اهمیت آن‌ها برای امنیت ملی را پایان کار ندانسته، ارزیابی و ایجاد تعادل در آن‌ها را به قضاوت نشسته است. برای مثال در قضیهٔ استول، دادگاه مقرر داشت که باوجود اهمیت و حساسیت اطلاعات موجود، مردم نیز نفع مشروعی در دریافت اطلاعات در خصوص نحوهٔ برخورد ماموران دولتی با چنین مسائل حساسی دارند (See also: ECtHR, (2008), Guja

.(v. Moldova Para. 64.or Observer and Guardian v. United Kingdom, para. 57 بنابراین نهادهای اطلاعاتی و امنیتی به دلیل نقش ویژه و بسیار مهمی که در جامعه ایفا می‌کنند، باید همانند دیگر نهادهای عمومی در معرض حسابرسی دموکراتیک قرار گیرند.

نتیجه آنکه همواره ممکن است نیاز به حفاظت از اطلاعات درست طبقه‌بندی شده، به‌وسیلهٔ یک نفع عمومی در افشا کنار گذاشته شود (Papandrea, 2012, p. 97)؛ همچنان‌که بند ۲ مادهٔ ۳ کنوانسیون ۲۰۰۹ شورای اروپا در خصوص دسترسی به اسناد دولتی، پس از ذکر محدودیت‌های دسترسی به اطلاعات دولتی، مقرر می‌دارد که در صورت وجود «یک نفع عمومی برتر»، یعنی برتر از منافع پیش‌بینی‌شده در این سند (که امنیت ملی یکی از آن‌ها ذکر شده است)، می‌توان اطلاعات یادشده در آن‌ها را افشا کرد.

۳.۲. بررسی آثار ناشی از افشا؛ آشتی دادن نیاز دولت به حفظ محرمانگی و حق مردم به دریافت اطلاعات دولتی

افشای اطلاعات درست طبقه‌بندی شده را نمی‌توان به عنوان یک حق به‌رسمیت شناخت؛ بنابراین همواره ارزیابی منافع و مضرات ناشی از افشا لازم است. به بیان دیگر همیشه باید محاسبه‌ای بی‌طرفانه دربارهٔ هزینه_ فایدهٔ افشا صورت پذیرد. فقط در صورتی می‌توان افشای اسناد طبقه‌بندی شده از سوی یک روزنامه‌نگار را قابل توجیه دانست که منافع ناشی از افشا بر خطرهای ناشی از تهدید امنیت ملی برتری یابد.

۱.۳.۲. نفع عمومی (Public Interest) ناشی از افشا. باید دید که معیارهای نفع عمومی چیست که توجیه‌کنندهٔ افشای اطلاعات نظامی، دیپلماتیک و جاسوسی در راستای حق مردم به دریافت اطلاعات باشد و آیا افشای اسناد دیپلماتیک و جاسوسی پایگاه توانسته است به این معیارها برسد؟

با توجه به اینکه مبنای اصلی حق دسترسی به اطلاعات دولتی، شفافیت و نظارت افراد بر عملکرد دولت می‌باشد، هر سندی که دربردارندهٔ اطلاعاتی باشد که پاسخ‌گویی دولت را در پی داشته باشد و یا برای ایفای حقوق جمعی آن‌ها ضرورت داشته باشد، می‌توان واجد «نفع عموم» دانست؛ همچنان‌که « اعمال غیرقانونی» ,ECtHR, 1991) (Para. 18 و « تخلف» (ECtHR, 2008, Para.70) از جمله معیارهایی است که دیوان اروپایی حقوق بشر در قضایای آبزرور و گاردین علیه انگلستان و همچنین گوجا علیه مولداوی برای تشخیص نفع عموم، آن را به‌کار برده است.

اسناد افشاشدهٔ امریکا حقایق زیادی را در خصوص فساد، اغماض نسبت به نقض حقوق بشر و سرکوب در کشورهای هم‌پیمان امریکا نشان می‌دهد. در زیر به مهم‌ترین منافع ناشی از افشای این اسناد در دو سطح داخلی و بین‌المللی اشاره می‌شود.

مسئولیت دولت امریکا در خصوص اعمال غیرقانونی خود در برابر شهروندان امریکایی و اطلاع از هزینه‌های نظامی امریکا در افغانستان و عراق، و میزان تلفات غیرنظامیان در طول جنگ عراق از مؤلفه‌های نظارت شهروندان بر دولت است. اسناد منتشرشده به‌جز دولت امریکا، اطلاعات زیادی را در خصوص دولت‌های دیگر و فساد و خطاکاری رهبران آن‌ها دربر دارد. یکی از مهم‌ترین مصادیق آن، افشای فساد دولتمردان تونس بود که به باور بسیاری از پژوهشگران نقش مستقیمی در خیزش عمومی مردم تونس و حرکت آنان در راستای حق تعیین سرنوشت خود داشته است (Fenster, 2012, pp. 804-805).

افزون‌بر مسئولیت در برابر شهروندان، دولت امریکا در برخی شرایط در برابر جامعهٔ بین‌المللی نیز مسئولیت دارد که لازمهٔ آن نظارت بر اعمال دولت است. با انتشار اولین سند در نوامبر ۲۰۰۷ در خصوص شیوهٔ ادارهٔ زندان گوانتانامو، روشن شد که برخلاف ادعای دولتمردان امریکایی مبنی بر نقض نشدن حقوق بشر در زندان گوانتانامو و باوجود تکذیب مکرر مقامات امریکایی، برخی زندانیان این زندان از دید کمیتهٔ بین‌المللی صلیب سرخ پنهان نگه‌داشته شده و شکنجه می‌شوند. پایگاه در آوریل ۲۰۱۰ فیلم محرمانهٔ ۱۷ دقیقه‌ای معروف به «قتل تصادفی» (Collateral Murder) را منتشر کرد. این فیلم محرمانه متعلق به ارتش امریکاست، و به‌وسیلهٔ دوربین نشانه‌گیری بالگرد آپاچی ضبط شده است و کشتار بی‌علت بیش از ده غیرنظامی ازجمله دو خبرنگار را در حومهٔ بغداد در سال ۲۰۰۷م نشان می‌دهد (Ibid, p. 762).

۲.۳.۲. آسیب‌های ناشی از افشا. به‌دنبال افشای اسناد نظامی امریکا در عراق و افغانستان، مأموران ارشد نظامی امریکا ادعا کردند که عملیات نظامی آن‌ها تحت تأثیر اسناد انتشاری قرار گرفته است. در حوزهٔ فعالیت‌های جاسوسی امریکا نیز وزارت امور خارجهٔ امریکا ادعا می‌کند که ارتباطات داخلی میان سرویس‌های اطلاعاتی، کارایی مؤثر خود را از دست داده است و منابع خارجی، اطلاعات را از ترس فاش شدن هویتشان در اختیار مأموران دیپلماتیک امریکایی قرار نمی‌دهند (Ibid, pp. 791-793).

۳.۳.۲. موازنهٔ منافع و آسیب‌ها. همان‌طور که ملاحظه شد، اسناد افشاشده افزون‌بر

نفع عمومی برای مردم امریکا، منافعی نیز برای مردم دیگر کشورها داشته است. بنابراین پرسشی که مطرح می‌شود این است که منافع عمومی کدام کشور را باید در مقابل آسیب‌های ناشی از افشا ارزیابی کرد[۴]؟

در پاسخ به این پرسش می‌توان گفت ازآنجا که اسناد افشاشده متعلق به دولت امریکا بوده و حق دسترسی به اسناد دولتی امریکا متعلق به شهروندان آن کشور است، زمانی افشای اطلاعات درست طبقه‌بندی شده در راستای حق مردم به دریافت اطلاعات قابل توجیه است که منافع ناشی از افشا برای شهروندان آن کشور بر خطرهای تهدید امنیت ملی غلبه یابد. هرچند که سرعت دریافت و انتشار اطلاعات و حجم گستردهٔ اسناد افشاشده از سوی پایگاه، ارزیابی آثار افشا و بررسی منافع و مضرات ناشی از آن را دشوار ساخته است، اما در اینجا می‌توان استدلال کرد که آسیب به امنیت ملی در اثر افشای اسناد نظامی، دیپلماتیک و جاسوسی، بر منافع ناشی از آن برای شهروندان امریکا برتری دارد. نتیجه آنکه، پایگاه ویکی‌لیکس حق بر افشای چنین اطلاعاتی را نداشته است.

۴.۳.۲. افشای اطلاعات طبقه‌بندی شدهٔ مرتبط با نقض شدید حقوق بشر؛ بی‌نیاز از موازنه. به‌موجب میثاق بین‌المللی حقوق مدنی- سیاسی، تعدادی از حقوق مهم‌تر از بقیه‌اند که تحت هیچ شرایطی قابل تعلیق نیستند؛ حق بر حیات و منع شکنجه مصادیقی از این حقوق غیرقابل تعلیق به‌شمار می‌روند. افزون‌براین، در بند ۲ مادهٔ ۴ میثاق که نمی‌توان امنیت ملی را مبنای تعلیق آن‌ها قرار داد، نقض شدید، گسترده یا سیستماتیک سایر حقوق بشری را نیز نمی‌توان بر این اساس توجیه کرد (McCarthy, 1998, p.375)؛ چنان‌که دیوان بین‌المللی دادگستری در نظریهٔ مشورتی خود در قضیهٔ دیوار حائل در سال ۲۰۰۴م چنین رای داد: «از آنجا که ساختن دیوار و مسیر انتخاب‌شده، موجب نقض شدید شماری از حقوق فلسطینیان در سرزمین‌های اشغالی می‌شود، تخلفات ناشی شده از آن مسیر را نمی‌توان به‌موجب امنیت ملی توجیه کرد» (ICJ Reports, 2004, Para.137).

---

۴. پاسخ به این پرسش از آن جهت مهم است که تعدادی از اسناد افشاشده درعین‌حال که به امنیت ملی امریکا آسیب می‌زنند، نفع عمومی را نیز برای مردم دیگر کشورها دربر داشته‌اند؛ برای مثال می‌توان به افشای هویت جاسوسان امریکا در کشورهای دیگر اشاره کرد که با وجود اینکه هیچ نفعی برای مردم امریکا ندارد، اما کشورهای دیگر با شناسایی جاسوسان و مجازات آن‌ها می‌توانند در جهت حمایت از امنیت ملی خود اقدام کنند.

بنابراین در این شرایط ما نمی‌توانیم منفعت امنیت ملی را در تقابل با این حقوق به تعادل برسانیم. حال پرسش این است که آیا می‌توان «حق دسترسی به اطلاعات دولتی مربوط به نقض شدید حقوق بشر» را از جملهٔ این حقوق غیرقابل تعلیق قلمداد کرد که محدودیت امنیت ملی را توانایی مقابله با آن نیست؟

در پاسخ به این پرسش باید گفت که یکی از دلایل اصلی غیرقابل تعلیق بودن حقوق مقرر در بند ۲ مادهٔ ۴ میثاق، ماهیت آن‌ها می‌باشد که به‌صورتی اساسی با کرامت انسان مربوط است و نقض آن به‌منزلهٔ نادیده گرفتن کرامت بشر است. با دسترسی به اطلاعات مرتبط با نقض این حقوق و افشای آن‌ها، جامعهٔ بین‌المللی قادر خواهد بود با شناسایی متخلف، اقدامات لازم را برای جلوگیری از وقوع دوبارهٔ آن‌ها انجام دهد. بنابراین قلمرو گستردهٔ این حق و ارتباط نزدیک آن با دیگر حقوق غیرقابل تعلیق مثل حق بر شکنجه نشدن، به این معناست که این حق نیز می‌بایست غیرقابل تعلیق باشد.

اصل ۱۹ مجموعهٔ اصول ژوهانسبورگ مقرر می‌دارد که هر گونه محدودیت (از جمله امنیت ملی) حق دسترسی به اطلاعات نباید دارای چنان ماهیتی باشد که اهداف حقوق بشردوستانه را خنثی کند. به‌موجب مادهٔ ۱ کنوانسیون‌های چهارگانهٔ ژنو، طرف‌های معاهده نه‌تنها باید کنوانسیون‌ها را اجرا کنند، بلکه باید تضمین دهند که همهٔ طرف‌های معاهده، آن‌ها را رعایت می‌کنند. این تعهدات برای نمونه شامل اقدامات متفاوتی برای حمایت از جمعیت‌های غیرنظامی و به‌ویژه حملات بدون تفکیک می‌شود. روشن است که هر طرف معاهده به اطلاعاتی نیازمند است که قانع شود طرف دیگر معاهده کنوانسیون را رعایت می‌کند (Coliver, 1999, pp.54-55).

از طرفی دیگر اجرای عدالت و به‌ویژه مجازات افراد ناقض کرامت بشری تا حد زیادی وابسته به اطلاعاتی است که طبقه‌بندی شده و از دسترس خارج شده‌اند. دیوان بین‌المللی کیفری یوگسلاوی سابق در اکتبر سال ۱۹۹۷ در خصوص اطلاعات دولتی موردنیاز سازمان ملل برای تعقیب جرائم جنگی، رای داد که دولت کرواسی نمی‌تواند از ارائهٔ اطلاعاتی که دادستانی دیوان در پرونده‌ای علیه یک ژنرال کروات بوسنیایی قرار احضار صادر کرده بود، به دلایل امنیت ملی خودداری کند (Ibid., pp. 44-45).

نتیجه آنکه افشای اطلاعات طبقه‌بندی شدهٔ مرتبط با نقض شدید حقوق بشر را نمی‌توان در تقابل با منفعت مشروع امنیت ملی به توازن رساند؛ هرچند این اسناد از

جمله اسنادی باشد که به‌درستی طبقه‌بندی شده است. اسناد افشاشدهٔ شکنجه در زندان‌های گوانتانامو، زندان‌های مخفی امریکا و دسترسی نداشتن کمیتهٔ بین‌المللی صلیب سرخ به آن‌ها و حملات بی‌تناسب نیروهای امریکایی در جنگ، کشتارهای فراقضایی در کنیا از جمله مصادیقی است که دولت‌های کنیا و امریکا با نقض تعهد خود در برابر جامعهٔ بین‌المللی و طبقه‌بندی این اسناد، حق مردم به اطلاع از این جرائم را نادیده گرفته‌اند.

۳. تعهدات ناشی از افشای اطلاعات طبقه‌بندی شده

به موجب بند ۳ مادهٔ ۱۹ میثاق مدنی_ سیاسی، اِعمال حق آزادی بیان با «تعهدات و مسئولیت‌هایی» همراه است که شامل روزنامه‌نگاران نیز می‌شود. آن‌ها نمی‌توانند از تعهدشان نسبت به اطاعت از قوانین کیفری کشورها رها باشند و لازم است در انتشار و طریقهٔ دسترسی به اطلاعات با حسن‌نیت عمل کنند. بنابراین آن‌ها باید اصول روزنامه‌نگاری را رعایت کرده، در انتشار اطلاعات قصد آسیب زدن به امنیت ملی دولت را نداشته باشند.

۱.۳. نداشتن قصد آسیب به امنیت ملی دولت

مرتبط‌ترین قانونی که به‌موجب آن دولت امریکا می‌تواند جولیان آسانژ یا دیگر افراد فعال در پایگاه ویکی‌لیکس را تحت پیگرد قرار دهد، استناد به قانون جاسوسی ۱۹۱۷م است که در طی جنگ جهانی اول با هدف جلوگیری از جاسوسی و حمایت از اسرار نظامی، تصویب شده است[۵]. در اینجا دو چالش ماهیتی در تعقیب آسانژ و یا دیگر گردانندگان پایگاه به‌موجب قانون جاسوسی وجود

۵. بخش ۷۹۸ این قانون با عنوان «افشای اطلاعات طبقه‌بندی شده» مقرر می‌دارد: «(a) هرکسی که عالماً و عامداً، انتقال دهد و یا به شکل دیگری در دسترس قرار دهد، نشر دهد و یا از هر طریقی استفاده کند به‌منظور صدمه به امنیت یا منافع ایالات متحده یا برای منافع هر دولت خارجی اطلاعات طبقه‌بندی شده‌ای را: ۱) در ارتباط با ماهیت، آماده‌سازی و یا استفاده از هر نوع کد، رمز یا سیستم پنهانی ایالات متحده؛ ۲) در ارتباط با طراحی، ساخت، استفاده، نگهداری یا اصلاح هر وسیله، ابزار استفاده شده یا برنامه‌ریزی شده برای استفاده ایالات متحده برای اهداف پنهانی یا ارتباطات جاسوسی؛ ۳) در ارتباط با ارتباطات فعالیت‌های جاسوسی ایالات متحده؛ باید به جریمهٔ نقدی یا حبس کمتر از ۱۰ سال و یا هر دو محکوم شود».

دارد[۶]. اولین چالش، حمایت‌های گسترده از آزادی بیان و آزادی مطبوعات بر اساس اصلاحیهٔ اول قانون اساسی امریکاست؛ تاجایی که در قضیهٔ پنتاگون، پی‌پر، قاضی بلک، اظهار داشت که «در آشکارسازی طرز کار حکومت که منجر به جنگ ویتنام شده است، روزنامه‌ها دقیقاً همان کاری را انجام دادند که بانیان آن انتظار داشتند» (Lacey, 2011, p.212). بنابراین کسانی که اطلاعات را منتشر می‌کنند، داخل حوزهٔ مسئولیتی نمی‌شوند.

دومین مشکل اثبات عنصر معنوی است. یعنی باید ثابت شود که آسانژ با انتشار اطلاعات طبقه‌بندی شده، قصد آسیب زدن به امنیت ملی امریکا را داشته است. اثبات این موضوع سخت است، چراکه قصد اظهارشده از سوی پایگاه این است که صرفاً به‌عنوان یک مجرای رسانه‌ای فعالیت می‌کند و شهروندان را از فعالیت‌های دولت‌ها در دنیا آگاه می‌سازد (Ibid., pp.216- 217). ، و درعمل انتشار این نوع اطلاعات از همهٔ کشورها، این قصد را تأیید می‌کند. از طرف دیگر، انتشار اسناد مرتبط با نقض حقوق بشر، فعالیت گردانندگان پایگاه را به‌عنوان یک مدافع حقوق بشر به‌موجب اعلامیهٔ مدافعان حقوق بشر توجیه کرده است؛ بنابراین « آن‌ها باید قادر باشند، نقش ضروری خود را در نشان دادن حقیقت و مسئول شناختن متخلفان حقوق بشر، بدون ترس از مجازات کیفری ایفا کنند» (Council of Europe, 2007, Para. 4).

---

۶. افزون‌بر چالش‌های ماهیتی، عمده‌ترین مشکل پیش‌روی امریکا در تعقیب آسانژ، فرایندهای استرداد او می‌باشد. به‌دنبال فرار آسانژ به انگلستان، دیوان عالی بریتانیا روز ۳۰ می۲۰۱۲ رای به استرداد او به سوئد برای رسیدگی به اتهام تجاوز به عنف داد، اما آسانژ ادعا می‌کند که اتهام تجاوز توطئه است و انگیزهٔ اصلی سوئد استرداد او برای محاکمه به امریکاست. بنابراین آسانژ در ۱۹ ژوئن ۲۰۱۲ به سفارت اکوادور پناهنده شد. دولت اکوادور نیز در ۱۶ آگوست ۲۰۱۲ به او پناهندگی سیاسی اعطا کرد. ازآنجا که آسانژ با شکستن وثیقهٔ حقوقی انگلستان به سفارت اکوادور پناه برده است، حتی با فرض قبول پناهندگی دیپلماتیک در حقوق بین‌الملل، نمی‌توان پناهندگی او را قبول کرد. بنابراین همچنان در حوزهٔ صلاحیتی انگلستان قرار دارد. با استرداد آسانژ به سوئد، در رابطهٔ میان امریکا و سوئد موافقت‌نامهٔ استرداد ۱۹۶۱م میان دو کشور حاکم خواهد بود. مادهٔ ۵ موافقت‌نامه، «جرم سیاسی» را از جرائم قابل استرداد مستثنا کرده است. جرم سیاسی، جرمی است که مستقیماً علیه امنیت یک دولت یا ملت باشد؛ جرائمی همچون خیانت، شورش، یا جاسوسی در این دسته قرار می‌گیرند. به‌موجب حقوق بین‌الملل، مرتکبان جرائم سیاسی را نمی‌توان استرداد کرد. برای کسب اطلاعات بیشتر در خصوص چالش‌های حقوقی استرداد آسانژ، نک: Thebes, 2011.

۲.۳. شیوهٔ دسترسی به اطلاعات دولتی

دولت امریکا در خصوص اقدامات پایگاه ادعا می‌کند که چنین اقداماتی «درخواست از کارمندان دولتی برای تخلف از قانون و درز اطلاعات طبقه‌بندی شده است»؛ بنابراین نمی‌تواند از حمایت‌های مقرر برای روزنامه‌نگاران بهره‌مند باشد.

۱.۲.۳. ویکی‌لیکس، دریافت‌کنندهٔ صرف اطلاعات. تا زمانی که پایگاه دریافت‌کنندهٔ صرف اطلاعات باشد، نمی‌توان آن را برای درز اطلاعات طبقه‌بندی شدهٔ دولت‌ها مسئول شناخت. همچنان‌که در قضیهٔ استول در دیوان اروپایی حقوق بشر، دولت استدلال کرد که دسترسی شاکی به اسناد طبقه‌بندی شده در اثر نقض محرمانگی اسرار رسمی بوده است؛ بنابراین دسترسی او به اسناد غیرقانونی شمرده شده است. اما دادگاه ضمن رد استدلال دولت، مقرر داشت که شاکی، شخص مسئول برای درز اسناد نبوده و این وظیفهٔ دولت‌هاست که کارمندان خود را چنان سازماندهی کرده، تعلیم دهند تا اسناد به بیرون از سازمان درز نکند (ECtHR, 2007, paras.142-143). بنابراین افشای اطلاعات از سوی پایگاه به‌عنوان یک رسانه را نمی‌توان با افشاگری‌های اخیر ادوارد اسنودن مقایسه کرد[۷]. هرچند که شنود مکالمات خصوصی از سوی سازمان اطلاعات مرکزی امریکا، خلاف صریح قانون اساسی و تعهدات حقوق بشری آن دولت است، اما اسنودن به‌عنوان کارمند، متعهد به حفظ اسرار آن سازمان است. باوجوداین، امروزه تعدادی از دولت‌ها قوانینی را به‌تصویب رسانده‌اند که به موجب آن کارمندان دولت نیز می‌توانند به افشاگری بپردازند. بر اساس این قوانین که به «Whistle-blowing» شهرت یافته است، یک کارمند دولتی با اعتقاد به یک نفع عمومی برتر از نفع اداره‌ای که در آن خدمت می‌کند، می‌تواند اطلاعات مرتبط با فساد و اعمال غیرقانونی اداره را به قصد آگاه‌سازی جامعه و متوقف ساختن وضع غلط موجود، انتشار دهد (Banisar, 2006, p. 5).

دیوان عالی امریکا نیز در حکم خود در سال ۲۰۰۱م، در قضیهٔ بارتینکی و واپر، حمایت خود را از دریافت اطلاعات از «یک منبع که آن را به‌صورت غیرقانونی به دست آورده بود» اعلام کرد. در این قضیه، مجری رادیو یک نوار صوتی در خصوص قطع

---

۷. ادوارد جوزف اسنودن (Edward Joseph Snowden) متولد ۱۹۸۴ میلادی، افشاگر کنونی و کارمند سابق سازمان اطلاعات مرکزی امریکا و پیمانکار سابق آژانس امنیت ملیبود است. اسنودن در ژوئن ۲۰۱۳ اطلاعات طبقه‌بندی شده‌ای از برنامه‌های فوق سری ان اس ای را برای انتشار به گاردین و واشینگتن پست داد.

غیرقانونی مکالمات تلفنی از یک منبع ناشناس دریافت کرد. او بعد از دریافت نـوار، آن را از رادیو پخش کرد. دادگاه رأی داد که پخش آن قانونی اسـت؛ حتـی اگـر بتـوان منبـع ناشناس را برای دسترسی غیرمجاز بـه نـوار تحـت پیگـرد قـرار داد (Stone, Geoffrey, 2011, p.116). بنابراین هرچند هویت افرادی که اسناد طبقه‌بندی شده را بـه پایگـاه درز داده‌اند ناشناس باقی مانده، تا زمانی که پایگاه دریافـت‌کننـدۀ صـرف اطلاعـات و اسـناد طبقه‌بندی‌شده باشد، عمل آن غیرقانونی نیست.

۲.۲.۳. ایجاد صندوق مجازی و گمنامی منبـع. ولـی آیـا نمـی‌تـوان ایجـاد صـندوق مجازی و دریافت اطلاعات از سوی پایگاه را نوعی عمـل غیرقـانونی تلقـی کـرد؟ چراکـه ایجاد صندوق و ارائۀ بالاترین سیستم امنیت گمنامی، به تشویق افـراد بـرای درز اسـناد طبقه‌بندی شده به پایگاه منجر می‌شود؛ به همین دلیل می‌توان آن را نوعی مشارکت در درز اطلاعات به‌شمار آورد.

چنین استدلالی قابل انتقـاد اسـت، چراکـه گمنـامی منبـع یکـی از اصـول اساسـی روزنامه‌نگاری سنتی شمرده می‌شود؛ چنان‌که شورای وزیران اروپـا در توصـیه‌نامـه‌ای در خصوص حق روزنامه‌نگاران بر افشا نکردن منابع اطلاعاتی خود، آن را به‌عنـوان «حـداقل استانداردهای حـق روزنامـه‌نگـاری» توصـیف کـرد (Council of Europe, 2000, Para. 1). گزارشگر سازمان ملل دربارۀ آزادی بیان نیـز در گـزارش ویـژه خـود اظهـار داشـت کـه حمایت از منبع، دارای اهمیتی اساسـی بـرای روزنامـه‌نگـاران اسـت کـه بـدون چنـین حمایتی، موانع زیادی در حق روزنامه‌نگاران در جستجو و دریافت اطلاعات ایجاد خواهـد شد (Banisar, 2007, pp.12-13). بر همین اساس کمیتۀ حقوق بشـر در نظریـۀ تفسـیری خود اعلام می‌دارد که دولت‌ها باید مزیت‌هـای ویـژۀ روزنامـه‌نگـاری را کـه شـامل افشـا نکردن منبع اطلاعاتی نیز می‌شود، بـه‌رسـمیت بشناسـند (H. R. Committee., *General comment no. 34*, para.45).

دیوان اروپایی حقوق بشر نیز در قضـیۀ انگلسـتان و گـودوین، قـرار صـادره از سـوی دادگاهی در انگلستان برای افشای هویت منبع اطلاعـاتی را کـه بـه‌دسـت روزنامـه‌نگـار رسیده بود، در تداخل با مادۀ ۱۰ کنوانسیون اروپایی حقوق بشر اعلام کرد و مقرر داشت که «حمایت از منبع یکی از شرایط اصـلی آزادی روزنامـه‌نگـاری اسـت... بـدون چنـین حمایتی، ممکن است منابع از همکاری با روزنامـه‌هـا در انتقـال اطلاعـات بـه مـردم در ارتباط با موضوعات مرتبط با نفع عموم خودداری کنند. درنتیجه نقش ضـروری روزنامـه به‌عنوان یک مراقب و دیدبان، ممکن است نادیده گرفته شده و توانایی روزنامه‌هـا بـرای

ارائه اطلاعات درست و قابل اعتماد تحت تـاثیر قـرار گیـرد» (ECtHR, 1996, Para. 39). بنابراین پایگاه با ایجاد سیستم گمنامی، درواقع در راستای اِعمال حق خود به‌عنوان یـک روزنامه‌نگار و تعهد در مقابل منبع، مبنی بر افشا نکردن هویت او اقدام کرده است.

نتیجه

پایگاه ویکی‌لیکس بـا اسـتفاده از پتانسـیل‌هـا و مزیـت‌هـای اینترنـت و دادن اطمینـان گمنامی به کاربران خود توانسـت بـه انبـوهی از اطلاعـات طبقـه‌بنـدی شـدهٔ دولـت‌هـا دسترسی پیدا کند و با افشای آن‌ها جلـوهٔ جدیـدی از تقابـل میـان حـق دسترسـی بـه اطلاعات و امنیت ملی را به نمایش بگذارد. اما با حرکت حقوق بین‌الملل سنتی به سوی حقوق بین‌الملل انسان‌محور، امروزه دولت‌ها به صرف استناد به امنیت ملی نمی‌تواننـد از تعهدات بین‌المللی خود شانه خالی کنند، چراکه امنیـت ملـی بـا هـر منفعـت احتمـالی برابری نمی‌کند. اسناد افشاشده از سوی پایگاه ویکی‌لیکس و به‌ویژه اسـناد طبقـه‌بنـدی شدهٔ دولت امریکا نشان داد که دولت‌ها گاهی این اطلاعات را به مقاصدی غیرمـرتبط بـا امنیت ملی طبقه‌بندی کرده‌اند. بنابراین لازم است تا به شکلی معقـول و منطقـی میـان نیاز دولت به حفظ محرمانگی و حق مردم به دریافت اطلاعات دولتی توازن ایجاد شود.

یکی از اصول اساسی حاکم بر حق دسترسی به اطلاعات دولتـی، حمایـت از افشـای همراه با حسن‌نیت افرادی است که به اطلاعات مرتبط با نفع عموم دسترسی دارنـد. امـا افشای اسنادی را که به‌درستی طبقه‌بندی شده‌اند، نمی‌توان به‌عنوان یک حق به‌رسمیت شناخت. بنابراین همواره باید ارزیابی منصفانه از آثار ناشی از افشا صـورت گیـرد. امـا در سطح بین‌الملل دسترسی به اطلاعات مرتبط با نقض فاحش حقوق بشر بی‌نیاز از موازنـهٔ آثار است و باید حق بر افشای چنین اسنادی را به‌رسمیت شناخت، هرچنـد دربرگیرنـدهٔ اطلاعاتی مرتبط با امنیت ملی باشند.

اعمال حقوق و آزادی‌های فردی با تعهدات و مسئولیت‌هـایی همـراه اسـت؛ بنـابراین افشای اطلاعات طبقه‌بندی شدهٔ دولت‌ها باید در سایهٔ اطاعت از قوانین کیفری دولـت‌هـا و با استفاده از روش‌های قانونی صورت گیرد. ویکی‌لیکس نیز به‌عنوان یک پایگاه خبری، لازم است اصول روزنامه‌نگاری را در دسترسی به اطلاعات و انتشار آن‌ها رعایت کند.

به‌عنوان یک راهکار می‌تـوان گفـت رسـیدن بـه تـوافقی بـین‌المللـی و انعقـاد یـک کنوانسیون در زمینهٔ افشای همراه با حسن‌نیت اسناد طبقه‌بندی شـده در راسـتای حـق مردم به دریافت اطلاعات دولتی سخت است؛ چراکه هر کشوری بسته به منافع و مصالح

ملی خود تعریف متفاوتی از اسناد طبقه‌بندی شده دارد، اما در حقوق بین‌الملل انسان‌محور، موضوعاتی برای توافق وجود دارد که ورای منافع ملی متفاوت دولت‌ها، می‌توان زمینهٔ انعقاد کنوانسیونی بین‌المللی را در افشای اطلاعات مرتبط با آن، به‌عنوان حقوقی مطلق و غیرقابل تعلیق به‌رسمیت شناخت. افشای اطلاعات مربوط به نقض شدید حقوق بشر یکی از آن مصادیق است.

همان‌طور که اشاره شد، امروزه در بیش از ۳۰ کشور جهان قوانینی با عنوان «Whistle-Blowing» به‌تصویب رسیده که نویدبخش ابزاری مؤثر و کارآمد در راستای مبارزه با فساد، نقض حقوق بشر و اعمال غیرقانونی دولت شده است.

منابع و مآخذ

۱. انصاری، باقر (۱۳۸۷)، ***آزادی اطلاعات***، تهران، دادگستر.

۲. نمک‌دوست تهرانی، حسن (۱۳۸۳)، ***آزادی اطلاعات و حق دسترسی: بنیان دمکراسی***، مجلس و پژوهش، تهران، ش۴۲، ص ۱۰۸-۶۳.

▪ کتاب‌ها و مقاله‌ها

3. Banisar, D., (2007), **Silencing Sources: An International Survey of Protections and Threats to Journalists Sources**, Privacy International Global Survey Series, 8 November.
4. ----------, (2006), **whistleblowing international standards and developments**, first conference about corruption and transparency, Mecxico 23-25 March.
5. Barandes, Laura, (2007), **A Helping Hand: Addressing New Implications of The Espionage Act on Freedom of The Press**, Cardozo Law Review, vol. 29, pp. 371-403.
6. Benkler, Yochai., (2011), **A Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate**, Harvard Civil Rights-Civil Liberties Law Review, vol. 46, pp. 311-397.
7. Coliver, Sandra, (1999), **Commentary to The Johannesburg Principles on National Security, Freedom of Expression and Access to Information**, in:Sandra Coliver, et al., Secrecy and Liberty: National Security, Freedom of Expression and Access to Information, The Hague,Martinus Nijhoff Publishers, pp. 12-80.
8. Fenster, Mark, (2012), **Disclosure's Effects: WikiLeaks and Transparency**, Lowa Law Review, vol. 97, pp. 753-807.
9. Kyle, Lewis., (2012),**Wikifreak-out: The Legality of Prior Restraints on WikiLeaks' Publication of Government Documents**, Journal of Law & Policy, vol. 38, pp. 417-440.

10. Kitrosser, Heidi, (2012), **Free Speech Aboard the Leaky Ship of State: Calibrating First Amendment Protections for Leakers of Classified Information**, Journal of National Security Law & Policy, vol. 6:2, pp. 409-446.
11. Kovarovic, Kate, (2011), **When the Nation Springs a [Wiki]Leak: The "National Security" Attack on Free Speech**, Touro International Law Review, vol. 14, no. 2, pp. 273-333.
12. Lacey, Heather, (2011), **Government Secrets, National Security and Freedom of the Press: The Ability of the United States to Prosecute Julian Assange**, Miami National Security & Armed Conflict Law Review, pp. 202-226.
13. McCarthy, Anna, (1998), **The International Human Rights and States of Exception**, The Hague: Martinus Nijhoff Publishers.
14. Naqvi, Yasmin, (2006), **The right to the truth in international law: fact or fiction?** International Review of RedCross, vol. 88, no. 862, pp. 245-273.
15. Opper, Melissa, (2011), **WikiLeaks: Balancing First Amendment Rights with National Security**,Loyola of Los Angeles Entertainment Law Review, vol. 31, no. 239, pp. 237-267.
16. Papandrea, Mary, (2007), **Lapdogs, Watchdogs, and Scapegoats: the Press and National Security Information**, Indiana Law Journal, vol. 83, pp. 233-305.
17. ----------, (2012), **Balancing and the Unauthorized Disclosure of National Security Information,** Iowa Law Review Bulletin, vol. 97, pp. 94-114.
18. Stone, Geoffrey, (2006), **Prosecuting the Press for Publishing Classified Information**, FIU Law Review, vol. 2, pp. 93- 96.
19. Stone, Geoffrey, (2011), **WikiLeaks, the Proposed SHIELD Act, and the First Amendment**,Journal of National Security Law & Policy, vol. 5, pp. 105-118.
20. Thebes, Molly, (2011), **The Prospect of Extraditing Julian Assange**, North Carolina Journal of International Law and Commercial Regulation, vol. 37, pp. 889-915.

▪ آرای قضایی

21. European Court of Human Rights (ECtHR), (2000), **Rotaru v. Romania,**Judgment, 4 May.
22. ECtHR., (1991), **Observer and Guardian v. United Kingdom**, Judgment, 26 November.
23. ECtHR, (2008), **Guja v. Moldova**, Judgment, 12 February.
24. ECtHR, (1996), **Goodwin v. The United Kingdom,** judgment, 27 March.
25. ICJ Reports, (2004), **Case Concerning Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory.**

▪ اسناد و گزارش‌ها

26. H. R. Committee, (2011), **General Comment No. 34**, 21 July.
27. H. R. Committee, (1988), **General comment, no. 16**, 8 April, para. 10.
28. H. R. Committee, (1983), **General Comment no. 10**, 29 June.

29. UN. H. R. Council., **Report of 4 June 2012**, A/HRC/20/17.
30. Council of Europe, (2007), **Fair Trial Issues in Criminal Cases Concerning Espionage or Divulging State Secrets,** Resolution, 19 April.
31. Council of Europe, (2000), **The Right of Journalists Not To Disclose Their Sources of Information**, Recommendation, 8 March.