واکنش حقوق بین‌الملل به وب‌پنهان: چرایی و چگونگی

(مقاله علمی-پژوهشی)

فریناز فیضی*

امیرحسین رنجبریان**

تاریخ دریافت: ۱۴۰۱/۰۵/۰۸ تاریخ پذیرش: ۱۴۰۱/۰۹/۰۵

چکیده

همانند قرن هفدهم میلادی که بشر با اختراع میکروسکوپ دریافت که دنیای پیرامون فراتر از چیزی است که در معرض حواس وی قرار دارد، نظام‌های حقوق ملی و بین‌المللی در هزاره سوم، در مواجهه با بخش ناپیدای اینترنت (وب پنهان) که پدیده‌ای ناملموس و ناشناخته اما واجد اهمیت و عظمت و پنهان در حجاب گمنامی است، سرگردان مانده و نتوانسته‌اند واکنش خاص، مناسب و فراگیری داشته باشند. در این مقاله، قبل از هر چیز ضرورت توجه و واکنش حقوق بین‌الملل به وب‌پنهان بررسی شده است. سپس با مراجعه به منابع بین‌المللی و واکاوی دیدگاه‌های مطرح، واکنش ناکافی حقوق بین‌الملل نسبت به وب‌پنهان، نقد و ظرفیت‌های موجود در حقوق بین‌الملل از قبیل اسناد غیرالزام‌آور، حقوق نرم و همکاری‌های بین‌المللی بررسی شده است. در انتها نحوهٔ کاربرد این ظرفیت‌ها در مسیر دستیابی به چارچوب‌های حقوقی واقع‌گرایانه وب‌پنهان و مهم‌ترین ملاحظاتی که باید مورد توجه قرار گیرد، مطالعه شده است.

کلید واژگان:

اسناد بین‌المللی، حقوق سایبر، حقوق نرم، وب‌پنهان.

* دانشجوی دکتری حقوق بین‌الملل، دانشکده حقوق و علوم سیاسی، دانشگاه تهران(نویسنده مسئول).
farinaz.fz@yahoo.com

** دانشیار، دانشکده حقوق و علوم سیاسی، دانشگاه تهران
aranjbar@ut.ac.ir

مقدمه

هر صفحه‌ای از وب که دارای یکی از ویژگی‌های «فهرست نشدن توسط موتورهای جست‌وجو» یا «بهره‌مندی از امکانات سامانه‌های ناشناس‌ساز»[۱] باشد، عنوان «وب‌پنهان»[۲] به آن اطلاق می‌شود.[۳] این حوزه از اینترنت، در سال‌های اخیر توجه پژوهشگران و سیاستگذاران را به خود جلب کرده است.[۴] مقالهٔ حاضر از منظر حقوق بین‌الملل به بررسی وب‌پنهان می‌پردازد.

آنچه توجه به وب‌پنهان را به‌عنوان بخشی از وب جهانی ضروری می‌کند، ویژگی‌های عظمت و گمنامی آن است. پژوهش‌های انجام شده به‌صورت تقریبی وب پنهان را بیش از ۴۰۰ برابر وب‌سطحی برآورد کرده‌اند.[۵] علاوه بر این، وب‌پنهان سطح بالایی از گمنامی و امنیت را به خاطر فلسفهٔ ایجاد و همچنین ساختار و ویژگی‌های فنی خود فراهم می‌آورد[۶] که علاوه بر کاربردهای مثبت و مشروع، محیط مناسبی برای ارتکاب جرائم در سطح بین‌المللی فراهم می‌آورد. در این بخش بزرگ و ناشناخته از اینترنت تنها تا سال ۲۰۱۰، حدود ۱۰۰,۰۰۰ سایت حاوی محتوای تروریستی و افراطی‌گری به ۱۵ زبان فعال بوده است.[۷]

---

۱. سامانه‌های ناشناس‌ساز (Anonymizing Services) مانند تور (TOR)، این امکان را در اختیار طرف‌های ارتباط قرار می‌دهد تا با پوشاندن ردپای خود در اینترنت، هویت و موقعیت مکانی خود را پنهان کنند.

۲. وب‌پنهان (Hidden Web) به‌عنوان اصطلاحی که وب‌عمیق (Deep Web) و وب‌تاریک (Dark Web) را دربرمی‌گیرد و در مقابل وب‌سطحی (Surface Web) قرار دارد، در این نوشته مورد استفاده قرار گرفته است.
See: Hatta, M. "Deep Web, Dark Web, Dark Net: a Taxonomy of "Hidden" Internet" *Annals of Business Administrative Science*, 19, 2020, p 277.

3. Al Nabki, M. et al. "Classifying Illegal Activities on TOR Network Based on Web Textual Contents" In *Proceedings of the 15th Conference of the European Chapter of the Association for Computational Linguistics,* 1, 2017, p 35.

4. Lusthaus, J. "Beneath the Dark Web: Excavating the Layers of Cybercrime's Underground Economy", In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 2019: 1. & Finklea, K. "*Dark Web*", Congressional Research Service, United States, Prepared for Members and Committees of Congress, 2017, p 1.

۵. در پژوهشی در سال ۲۰۰۱ ضمن تاکید بر نامشخص بودن ابعاد وب‌پنهان، برخی برآوردها از آن ارائه شد که بر اساس آن، اطلاعات عمومی مندرج در وب‌پنهان ۴۰۰ تا ۵۵۰ برابر بزرگتر از وب سطحی است.
See: Bergman, M. "White Paper: The Deep Web: Surfacing Hidden Value", *The Journal of Electronic Publishing*, Vol. 7, Issue 1, 2001, p 1.
در مقاله‌ای در سال ۲۰۱۹ ضمن تاکید مجدد بر ناشناخته بودن اندازه وب‌پنهان، همچنان گزارش فنی برگمن در سال ۲۰۰۱ به عنوان پراستنادترین مرجع برای تخمین اندازه وب‌پنهان معرفی شده است.
See: Hernández, I. et al. "Deep Web Crawling: A Survey" *World Wide Web*, 22, 2019, p 1578.

6. Kavallieros, D. et al. "Using the Dark Web" In Akhgar, B. et al. (eds.) *Dark Web Investigation*, Springer, 2021, p 27.

7. Chen H. *Dark web: Exploring and Data Mining the Dark Side of the Web*. Springer, 2011, p 3.

در این نوشته، پس از بررسی ضرورت واکنش حقوقی بین‌المللی به وب‌پنهان وضعیت موجود و انتظارها از حقوق بین‌الملل در برابر آن بررسی می‌شود تا مشخص شود که حقوق بین‌الملل موجود، چگونه می‌تواند در مواجهه با معضلات، چالش‌ها و تعارض‌ها در سطح بین‌المللی در خصوص وب‌پنهان کارآمد باشد؟ به عبارت دیگر از حقوق بین‌الملل موجود دربارهٔ وب‌پنهان، انتظار چه کارکردهایی می‌توان داشت؟ فرضیهٔ پژوهش آن است که با توجه به ویژگی‌های وب‌پنهان، واکنش حقوقی بین‌المللی به آن و تدوین قواعد خاص بین‌المللی ضرورت دارد. اما هنوز پاسخ حقوقی خاص، مناسب و فراگیر در سطح بین‌المللی به وب‌پنهان شکل نگرفته است و این امر از یک‌سو منجر به محرومیت کاربران قانونمند از حقوق مشروع خود و از سوی دیگر مصونیت کاربران هنجارشکن از تعقیب و دادرسی می‌گردد. برای رسیدن به قواعد خاص بین‌المللی، کاربرد قواعد موجود حقوق بین‌الملل برای حل چالش‌های بین‌المللی خاص وب‌پنهان و استفاده از ابزارها و ظرفیت‌های حقوق بین‌الملل برای دستیابی به نقاط نظر مشترک در سطح جهانی دربارهٔ وب‌پنهان اهمیت دارد.

۱. ضرورت توجه ویژه به وب‌پنهان

شناخت ضرورت توجه به وب‌پنهان از منظر حقوقی، نیازمند توجه به مرز مفاهیم «وب‌سطحی» و «وب‌پنهان» است. تفکیک میان این دو، ضرورت توجه مجزا به وب‌پنهان را آشکار می‌کند.

وصف ذاتی وب‌پنهان که آن را مهم و متمایز می‌کند، قرار گرفتن در حجاب گمنامی به لطف امکانات سامانه‌های ناشناس‌ساز است. این بخش از وب‌جهانی توسط موتورهای جست‌وجو، فهرست نمی‌شود و تنها توسط تقاضای مستقیم و هدفمند و از طریق وارد کردن نشانی صفحات، توسط ایجادکنندگان آنها یا کاربران تعریف شده، قابل دسترسی هستند.[1] همچنین به لطف بهره‌مندی از امکانات سامانه‌های ناشناس‌ساز، طرف‌های ارتباط عمداً ردپای اینترنتی، هویت، موقعیت مکانی و محتویات خود را از دید شاهدان بیرونی پنهان می‌کنند.[2] بنابراین ابعاد و میزان گمنامی در وب‌پنهان با وب‌سطحی قابل مقایسه نیست؛ در بخش سطحی وب، هر چند فرد

1. Raghavan, S. & Garcia-Molina, H. (2001), "Crawling the Hidden Web", Published in *Proceedings of 27th International Conference on Very Large Pages (VLDB)*, Roma, 2001, p 129.
2. Goldberg, I. "Privacy Enhancing Technologies for Internet III: Ten Years Later", Published in Alessandro Acquisit, A., Gritzalis, S., Lambrinoudakis, C & di Vimercati, S. (eds.) *Digital Privacy: Theory, Technology and Practice*, Auerbach Publications, 2007, p 9.

ممکن است بخشی از هویت خود را به روش‌هایی مانند استفاده از نام مستعار مخفی نماید، سطحی از گمنامی که در آن هویت کامل، موقعیت مکانی، محتوا و... قابل شناسایی نباشد، در وب‌سطحی ممکن نیست. گمنامی وب‌پنهان سطح بالایی از محرمانگی و امنیت را به خاطر فلسفهٔ ایجاد و همچنین ساختار و ویژگی‌های فنی خود فراهم می‌آورد.[1]

وصف ذاتی گمنامی، وب‌پنهان را از وب سطحی متمایز می‌کند و به دنبال آن استفادهٔ دوگانهٔ مشروع یا نامشروع از اینترنت در این لایه از وب اهمیت ویژه‌ای می‌یابد. وب‌پنهان از یک‌سو محل فعالیت کاربران قانون‌مند متمایل به گمنامی، مانند روزنامه‌نگاران و فعالان سیاسی و اجتماعی، قربانیان و شاهدان جرائم، نجات‌یافتگان از خشونت خانگی، قربانیان تبعیض، شرکت‌کنندگان در نظرسنجی‌ها یا رأی‌گیری‌های آنلاین و افرادی که تلاش می‌کنند دیدگاه‌هایشان را نه بر مبنای منبع، بلکه بر مبنای محتوا در معرض قضاوت قرار دهند، است.

از سوی دیگر، این فناوری در موارد متعددی ابزار نقض قوانین ملی و بین‌المللی از طریق استفاده‌های نامشروعی قرار می‌گیرد که از آن جمله می‌توان به هرزه‌نگاری کودکان، معاملهٔ مواد مخدر و روان‌گردان، اسلحه، اقلام ممنوعه در برخی کشورها یا کالاهای مشمول مقررات مالیاتی یا محدودیت‌های صادرات و واردات و تبلیغات، تأمین مالی، عضوگیری و تدارک فعالیت‌های تروریستی و... اشاره کرد. تعقیب متهم و انتساب جرم در محیط وب‌پنهان بسیار دشوارتر از وب‌سطحی است.[2]

آنچه توجه‌ها را به وب‌پنهان بیشتر جلب می‌نماید، آن است که این سطح از گمنامی در بخشی از وب وجود دارد که چندصد برابر وب سطحی عظمت دارد. برای دریافت بزرگی وب‌پنهان تعابیر مختلفی استفاده شده که مهم‌ترین آنها تشبیه وب‌پنهان به بخش ناپیدای کوه

1. Kavallieros, D. et al. op. cit. p 27.

۲. وب‌سایت سیلک‌رود و مسدود شدن آن، مهم‌ترین پروندهٔ مرتبط با وب‌پنهان است که این موضوع را به کانون توجه بین‌المللی کشاند. در اکتبر ۲۰۱۳ در پی مرگ چندین نفر در نتیجهٔ مصرف مواد مخدری که از طریق وب‌سایت سیلک‌رود فروخته شده بود، پلیس فدرال آمریکا در جریان عملیاتی و از طریق دسترسی به رایانه شخصی «راس ویلیام اولبریکت» این وب‌سایت را مسدود کرد و وی نیز به عنوان ذهن پشت عملیات مجرمانه این وب‌سایت دستگیر شد. وی در نهایت به اتهام ارتکاب جرایم «زمینه‌چینی و معاونت در قاچاق مواد مخدر»، «زمینه‌چینی برای پولشویی»، «نفوذ به سیستم‌های رایانه‌ای» و «تداوم اعمال مجرمانه» محکوم شد.
See: United States of America v. Ross William Ulbricht, a/k/a "Dread Pirate Roberts", a/k/a "DPR", a/k/a Silk Road, United States District Court Southern District of New York, Indictment, 14 CRIM 068, February 2014.

یخ است.[1] قسمتی از کوه یخ که پیدا و قابل مشاهده است، تنها درصد اندکی از حجم کلی آن را دربرمی‌گیرد. این بخش پیدا، مشابه وب‌سطحی و بخش ناپیدا و بزرگ‌تر کوه یخ، وب‌پنهان است.

واقعیت‌های عملی موجود نشان می‌دهد که امکان سلب وصف گمنامی به‌روش‌هایی مانند وضع محدودیت‌ها و ممنوعیت‌ها یا قطع اینترنت وجود ندارد؛ چراکه از یک‌سو دانش فنی و نیروی انسانی متخصص فعال در این حوزه بسیار بیش از آن‌چیزی است که دولت‌ها در اختیار دارند و در نتیجه هر عملی در قالب محدودیت یا ممنوعیت با عکس‌العمل فعالان وب‌پنهان برای دور زدن آن روبرو خواهد شد و از سوی دیگر، دولت‌ها را در مرز نقض حق‌های بشری و مسئولیت بین‌المللی قرار خواهد داد. بنابراین تنها گزینهٔ موجود پیشِ روی دولت‌ها در مواجهه با وب‌پنهان، توسل به ابزارهای حقوقی و تنها راهکار ممکن، ایجاد تعادل میان حمایت از کاربردهای مثبت وب‌پنهان و مقابله با استفاده‌های نامشروع خواهد بود.

بدیع‌بودن، مسئلهٔ مهم دیگری است که ضرورت پرداختن به وب‌پنهان را توجیه می‌کند. توجه خاص و ویژه پژوهشگران و سیاستگذاران در دنیا به این بخش بزرگ از فضای اینترنت، در حدود یک دههٔ گذشته افزایش یافته است.[2] در گزارش ارائه‌شده به کنگرهٔ آمریکا، ضمن اشاره به اینکه وب‌پنهان مورد توجه پژوهشگران، مجریان قانون و سیاستگذاران قرار گرفته، تأکید شده است که هنوز اطلاعات اندکی در خصوص این بخش از وب جهانی وجود دارد و دولت‌ها با چالش‌های جدی در خصوص مدیریت فناوری‌های در حال پیشرفتی مانند رمزنگاری و انتساب جرم در یک محیط گمنام مواجه‌اند.[3] علاوه بر این، حوزهٔ وب‌پنهان به دلیل گره خوردن با مسائل فنی مختلف، حائز پیچیدگی‌های متعددی است. یکی از دلایل تأخیر در واکنش‌های ملی و بین‌المللی مناسب به این موضوع نیز کمبود آگاهی، دانش فنی و نیروی انسانی متخصص در این حوزه می‌باشد.

با توجه به آنچه گفته شد، اوصاف گمنامی، کاربردهای دوگانهٔ مشروع و نامشروع، عظمت، تازگی و پیچیدگی‌های فنی وب‌پنهان ضرورت توجه ویژه به آن را برجسته کرده و سبب شده که در سال‌های اخیر این موضوع مورد توجه پژوهشگران و سیاستگذاران قرار گیرد.

1. Bailurkar, R. Chaursia, P. & Goswami, A. "The Deep Web", *International Journal of Scientific and Engineering Research*, 8.2, 2017, p 60.
2. Lusthaus, op. cit. p 1.
3. Finklea, op. cit. p 15.

۲. ضرورت واکنش حقوقی بین‌المللی به وب‌پنهان

در نگاه نخست، دلیل لزوم واکنش حقوقی بین‌المللی به وب‌پنهان، ناکافی بودن واکنش‌های حقوقی ملی است. اما دلایل دیگری نیز برای توجیه مداخلهٔ حقوق بین‌الملل در حوزهٔ وب‌پنهان وجود دارد:

۲.۱. مسئله فراسرزمینی؛ پاسخ فراسرزمینی

نخستین و قطعی‌ترین دلیل در توجیه ضرورت واکنش حقوقی بین‌المللی آن است که وب‌پنهان به‌عنوان پدیده‌ای فراسرزمینی، واکنش مناسب فراسرزمینی را می‌طلبد.[۱] هیچ کشوری نمی‌تواند ادعای کنترل بر اینترنت را مطرح کند. اینترنت موضوع حقوق بین‌الملل شناخته می‌شود[۲] و تنظیم‌گری و مقررات‌گذاری در حوزه‌های مختلف اینترنت مانند وب‌پنهان، به‌تنهایی توسط هیچ کشوری مقدور نخواهد بود.[۳]

۲.۲. جبران خلأ ناشی از عدم واکنش برخی دولت‌ها

برخی از دولت‌ها به‌دلایلی همچون فقدان آگاهی، دانش فنی و نیروی انسانی متخصص، قادر به واکنش حقوقی کافی و مناسب به وب‌پنهان نیستند. این امر، سبب افزایش استفاده‌های زیان‌بار از آن در قلمرو این کشورها و ورود آسیب به شهروندان می‌شود. همچنین با توجه به خصیصهٔ فراسرزمینی، وب‌پنهان تبدیل به بهشت مجرمان بین‌المللی و خطری برای امنیت جهانی می‌شود که پنهان کردن رد آثار جرم در آن ساده و فرایندهای اجرایی لازم برای مقابله با این اعمال دشوار است. بنابراین آثار انفعال برخی کشورها، در عمل متوجه همهٔ دولت‌ها و جامعهٔ جهانی خواهد بود. اقدامات حقوقی بین‌المللی از یک سو کاستی‌های فنی و انسانی این قبیل دولت‌ها برای مقابله با وب‌پنهان را پوشش می‌دهد و از سوی دیگر از تبدیل خطرات ناشی از انفعال برخی دولت‌ها به معضلی با آثار بین‌المللی، جلوگیری می‌کند.

1. Chertoff, M. "A Public Policy Perspective of the Dark Web", *Journal of Cyber Policy*, 2, 2017, pp 32-34.
2. Land, M. "Toward an International Law of the Internet", *Harvard International Law Journal*, 54, 2013, p 394.
۳. ر.ک: رجبی، عبداله و نسرین ترازی، **بررسی انتقادی حاکمیت حقوقی ساختار فنی اینترنت بر فضای مجازی**، فصلنامه تحقیقات حقوقی، ۱۳۹۶، شماره ۸۰، صص ۳۰۴-۳۰۵.

۲.۳. وب‌پنهان و تهدید علیه صلح و امنیت بین‌المللی

برخی از اعمال زیان‌باری که تحت پوشش گمنامی فراهم شده توسط وب‌پنهان واقع می‌شود، نه‌تنها تهدیدی برای جامعه در داخل قلمرو دولت‌ها است، بلکه در سطحی کلان‌تر می‌تواند تهدیدی علیه صلح و امنیت بین‌المللی نیز به شمار آید. به عنوان مثال یکی از فعالیت‌های رایج در محیط وب‌پنهان که عمدتاً در قالب رمزبازارها صورت می‌گیرد، خرید و فروش تسلیحات غیرمجاز است. این شکل از معاملات چارچوب‌های فعلی حقوق بین‌الملل در زمینهٔ کنترل تسلیحات را تهدید می‌نمایند.

از سوی دیگر یکی از نگرانی‌های جدی در ارتباط با وب‌پنهان، استفاده گروه‌های تروریستی از امکانات ناشناس‌ساز این محیط برای مقاصدی همچون تبلیغات، تدارک اطلاعات، تأمین مالی، عضوگیری، دستیابی به تسلیحات سایبری و تسهیل حملات سایبری است. از آنجا که فناوری همچون وب‌پنهان به تسهیل فعالیت گروه‌های تروریستی کمک نموده، توجه حقوقی بین‌المللی به این مسئله در راستای کنترل خطرات ناشی از این شکل از سوءاستفاده از وب‌پنهان ضروری به نظر می‌رسد؛ چنان‌که در گزارش سال ۲۰۱۷ دبیر کل سازمان ملل متحد در خصوص تهدیدات گروه تروریستی داعش برای صلح و امنیت بین‌الملل به شورای امنیت، تأکید شده که بر اساس اعلان دولت‌های عضو، ارتباطات داخلی و فرایند عضوگیری این گروه به سمت استفاده از شیوه‌های مخفی در حال حرکت است که از جمله می‌توان به افزایش استفاده از وب‌پنهان و کدگذاری اشاره کرد.[۱] بنابراین استفاده گروه‌های تروریستی از وب‌پنهان در راستای بسط فعالیت‌های تروریستی خود، به تهدیدی جدی و واقعی برای صلح و امنیت بین‌المللی بدل شده است.[۲]

علاوه بر موارد فوق، وب‌پنهان با فراهم آوردن ارتباطات امن و ناشناس و پشتیبانی از رمزبازارها، در کنار تدارک زیرساخت‌هایی برای پرداخت ناشناس از طریق رمزارزها، راه را برای ارتکاب جرائم سازمان‌یافته، به‌خصوص قاچاق و پولشویی در سطحی وسیع هموار کرده و در

1. United Nations Security Council, *Fourth Report of Secretary-General on the Threat Posed by ISIL (Daesh) to International Peace and Security and the Range of United Nations Efforts in Support of Member States in Countering the Threat*, S/2017/97: 2/20.
2. Denker, K. et al. "Darknets as Tools for Cyber Warfare" In Reuter, C. (ed.) *Information Technology for Peace and Security*. Wiesbaden: Springer Vieweg, 2019, p 123.

عمل منجر به تضعیف چارچوب‌های حقوقی بین‌المللی موجود در زمینهٔ مقابله با اقسام جرائم سازمان‌یافته بین‌المللی، بخصوص در بُعد مالی شده است.

۲.۴. مغایرت برخی راهکارهای حقوقی ملی با چارچوب‌های حقوق بین‌الملل

اکتفا به عملکرد صرفاً حاکمیت‌محور دولت‌ها در حوزهٔ وب‌پنهان، می‌تواند منجر به بروز ناهنجاری‌های بین‌المللی و نقض چارچوب‌های بنیادین مستقر و موجود حقوق بین‌الملل شود و مسئولیت بین‌المللی آنها را به‌دنبال داشته باشد.

به‌عنوان نمونه می‌توان به گرایش برخی دولت‌ها به استفاده از تکنیک‌های تعقیب شبکه‌ای برای مقابله با جرایم ارتکابی در وب‌پنهان اشاره کرد. با توجه به نامعلوم بودن هویت و موقعیت مکانی کاربران وب‌پنهان این خطر وجود دارد که رایانه و فرد موضوع عملیات اجرایی این قبیل دولت‌ها، در قلمرو صلاحیتی دولت دیگری باشد و در نتیجه با اجرای این عملیات صلاحیت قانونی و اجرایی یک دولت در قلمرو صلاحیتی دولت دیگر اعمال شود که بر اساس چارچوب‌های حقوق بین‌الملل موجود چنین اقدامی اعمال صلاحیت فراسرزمینی محسوب می‌شود و پذیرفته و مشروع نمی‌باشد.

از سوی دیگر دولت‌هایی که با مجرمانه قلمداد کردن اصل استفاده از وب‌پنهان سعی در ممنوع و محدود کردن دسترسی کاربران به این فضا دارند، نیز در مسیر نقض هنجارهای پذیرفته شده وب‌پنهان در حرکت‌اند. واکنش این دسته از دولت‌ها که وب‌پنهان را به طور کلی تهدیدی علیه امنیت ملی خود تلقی می‌کنند، عمدتاً فراتر از حد ضرورت و تناسب است و می‌تواند منجر به تضییع حقوق بشری آنلاین کاربران شود.

عوامل فوق در کنار هم سبب شده است که وب‌پنهان توجه حقوق بین‌الملل را به‌خود جلب نماید؛ به نحوی که کمیسر اتحادیه اروپا در امور مهاجرت می‌گوید: «وب‌پنهان در حال تبدیل شدن به پناهگاه جرائم گسترده است. این امر تهدیدی برای جوامع و اقتصاد ما محسوب می‌شود که تنها با هم در مقیاس جهانی می‌توانیم با آن روبرو شویم».[1]

1. Kavallieros, D. et al. op. cit. p 3.

۳. وضعیت فعلی حقوق بین‌الملل و وب‌پنهان

کاربران قانونمند وب‌پنهان برای جلوگیری از دخالت و نظارت گسترده دولت‌ها و بازیگران خصوصی، به وصف گمنامی این فناوری و حمایت‌هایی که از آن در پناه حقوق بشر ممکن می‌شود، امید بسته‌اند. بنابراین کارکردهای مثبت وب‌پنهان عمدتاً مورد حمایت حقوق بین‌الملل بشر قرار دارد.

البته در اسناد و رویه‌های حقوق بین‌الملل، هنوز دلایل کافی برای پذیرش حق مستقلی به نام حق گمنامی وجود ندارد. اما این امر به معنی عدم امکان حمایت از گمنامی در نظام بین‌المللی حقوق بشر نیست. ممنوعیت گمنامی فراهم شده به‌وسیلهٔ وب‌پنهان، با حق آزادی بیان و عقیده و حق حریم خصوصی همخوانی ندارد. بااین‌حال، از یک‌سو، کارکردهای منفی وب‌پنهان را نمی‌توان نادیده گرفت و از سوی دیگر هر دو حق حریم خصوصی و آزادی بیان، حقوقی مطلق نیستند و بر اساس مصالح اجتماعی محدودیت‌پذیر می‌باشند؛ از این رو گمنامی نیز مطلق نخواهد بود و بر اساس ملاحظات مشروعی که در چارچوب نظام بین‌المللی حقوق بشر پذیرفته شده‌اند، قابل تحدید است.

راهکار معقول برای تدوین قواعد بین‌المللی در حوزهٔ وب‌پنهان، اولویت دادن به اصل آزادی استفاده از وب‌پنهان برای حمایت از کارکردهای مثبت و در مقابل، تعدیل و تحدید آن بر اساس واقعیت‌های موجود و ملاحظات مشروع پذیرفته‌شده در حقوق بین‌الملل در راستای کنترل کارکردهای منفی این فناوری است.[۱] در حال حاضر می‌توان مدعی شد که وب‌پنهان، به‌عنوان موضوعی دارای اهمیت و وصف بین‌المللی، در سطح بین‌المللی با واکنش حقوقی خاص، مناسب و فراگیری همراه نبوده است. در ادامه به بررسی این ادعا پرداخته می‌شود.

۱. در این زمینه، دادگاه اروپایی حقوق بشر در پرونده احمد ایلدریم علیه ترکیه بر این نکته تأکید می‌کند که محدودیت مجاز لزوماً باید بر مبنای محتوایی خاص باشد و ممنوعیت‌های کلی بر عملکرد وب‌سایت‌ها و سیستم‌های ارتباطی با حق افراد در دریافت یا انتقال اطلاعات مغایرت دارد. چنین محدودیت‌هایی همچنین باید بر اساس موشکافانه‌ترین بررسی‌ها و احتیاطات بر محتوایی خاص اعمال شده باشد و از چارچوب حقوقی قطعی و دقیقی پیروی کند.
See: European Court of Human Rights, Ahmet Yildirim v. Turkey, 311/10, 2012, pp 30 & 64.

۳.۱. وب‌پنهان، مغفول در نظام حقوقی بین‌المللی

وب‌پنهان بخش مهم و ناپیدای اینترنت و جدیدتر، پیچیده‌تر و ناشناخته‌تر از آن است. در حالی سخن از واکنش حقوقی در سطح بین‌المللی به وب‌پنهان می‌گوییم که با گذشت حدود سه دهه از رواج استفاده فراگیر از اینترنت، همچنان فقدان نظام حقوقی جامع و منسجم در سطح بین‌المللی برای اینترنت، احساس می‌شود. تلاش‌هایی که تاکنون برای نظام‌مندی اینترنت در سطح بین‌المللی صورت گرفته است، توفیق چندانی در ایجاد نظم حقوقی جامع که پاسخگویی خصائص ذاتی اینترنت و چالش‌های فرامرزی آن باشد، نداشته‌اند. بخش قابل توجهی از انفعال حقوق بین‌الملل در برابر وب‌پنهان، ریشه در دلایل ناکامی ایجاد چارچوب حقوقی بین‌المللی برای اینترنت به طور کلی دارد.

عامل مؤثر در واکنش ناکافی نظام حقوقی بین‌المللی نسبت به اینترنت و دشواری تحقق اجماع بین‌المللی، شکاف عمیق در دیدگاه‌ها و مواضع دولت‌ها در خصوص مسائل چالشی حوزهٔ اینترنت، مثل حریم خصوصی، آزادی بیان، گردش آزاد اطلاعات، امنیت ملی و... است. به‌عنوان مثال، عمده کشورهای اروپایی در مواجهه با محتویات زیان‌بار در محیط آنلاین، بر حذف آنها تأکید دارند؛ درحالی‌که ایالات متحده بر اساس اصلاحیه اول قانون اساسی خود، آزادی بیان را نسبت به حفاظت از شهروندان و جامعه در برابر محتویات زیان‌بار دارای اولویت می‌داند.[۱] همچنین در مورد تقابل احتمالی آزادی بیان و حریم خصوصی، اروپا حریم خصوصی شهروندان را واجد اولویت و ایالات متحده آزادی بیان را مقدم می‌داند. برخی دیگر از دولت‌های قدرتمند همچون روسیه و چین نیز در مواجهه با وب‌پنهان بیش از هر چیز بر مسئله امنیت ملی توجه دارند و موضع خود در برابر این قبیل تحولات را بر مبنای این ملاحظه تنظیم می‌کنند.[۲ ۳]

1. Breckheimer, P.J. "A Haven for Hate: The Foreign and Domestic Implications of Protecting Internet Hate Speech Under the First Amendment", *Southern California Law Review*, 75, 2001, pp 1493-1494.

2. Mendel, T. et al. *Global Survey on Internet Privacy and Freedom of Expression*. UNESCO, 2012. pp 74-48; Kukkola, J. "The Russian National Segment of the Internet as a Source of Structural Cyber Asymmetry", In Stevens, T. Ertan, A. Floyd, K. & Pernik, P. (eds.) In *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*, Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2020: ,p 13.

۳. در خصوص سیاست کشور چین در قبال اینترنت، ر.ک: انصاری، باقر و شیما عطار، **حمایت از داده‌ها در چین؛ مطالعهٔ تطبیقی با رویکرد حمایت از داده‌ها در امریکا و اتحادیهٔ اروپا**، مجله مطالعات حقوق تطبیقی، دوره ۱۳، ۱۴۰۱، شماره ۳، صص ۱۰۶-۱۰۷.

این تفاوت‌ها موجب شده که دستاوردهای جامعهٔ بین‌المللی، محدود به اسنادی با طرف‌ها و دامنهٔ موضوعی محدود باشد که هر چند در استخراج برخی از اصول حقوقی برای اینترنت مؤثر هستند، ولی در تأمین انتظارها برای شکل‌گیری چارچوب حقوقی جهانی که موضوعات و چالش‌های اساسی مرتبط با اینترنت را پوشش دهد، ناکام بوده‌اند. از جمله این تلاش‌ها می‌توان به تدوین کنوانسیون شورای اروپا راجع به جرائم سایبری، موسوم به کنوانسیون بوداپست،[1] مقررات رادیویی و ارتباطات راه دور اتحادیه جهانی مخابرات[2] و دستورالعمل حفاظت از داده‌های اتحادیهٔ اروپا[3] اشاره کرد. مجمع جهانی جامعهٔ اطلاعاتی در جریان دو اجلاس در سال‌ها ۲۰۰۳[4] و ۲۰۰۵[5]، مبادرت به ارائهٔ طرح‌هایی پیشنهادی برای تدوین کنوانسیونی نمود که تحت لوای سازمان ملل متحد بیانگر اصول کلی حاکم بر اینترنت باشد. با این حال، چنان‌که از مذاکرات مجمع جهانی جامعه اطلاعاتی برمی‌آید، میان بازیگران اصلی حوزهٔ اینترنت، به‌خصوص دولت‌ها، اختلاف‌نظرهای جدی راجع به اصول و هنجارهای بنیادین این حوزه وجود دارد و بعد از گذشت نزدیک به دو دهه توفیقی در زمینه تدوین کنوانسیون مورد نظر این مجمع حاصل نشده است.

در شرایطی که دولت‌ها پس از دهه‌ها در تدوین چارچوب حقوقی بین‌المللی مناسب برای حکومت بر اینترنت ناتوان بوده‌اند و نظام موجود، علی‌رغم احراز برخی اصول و قواعد همچنان دارای کاستی‌های قابل توجهی می‌باشد، طبیعی است که حوزهٔ نوظهورتر و به مراتب پیچیده‌تر وب‌پنهان، در سطح بین‌المللی مغفول مانده باشد. پیچیدگی مقولهٔ وب‌پنهان به طور کلی و محرومیت بسیاری از کشورها از زیرساخت‌های فنی و نیروی انسانی متخصص در این حوزه نیز سبب شده که خطرات و تهدیدهای ناشی از وب‌پنهان توسط تعداد قابل توجهی از دولت‌ها درک نشود و از این رو اراده‌ای برای اقدامی حقوقی در سطح بین‌المللی شکل نگیرد. در کنار ناآگاهی

1. Council of Europe, "EU Cybercrime Treaty (Budapest Convention)", European Treaty Series, No. 185, Budapest, 2001.
2. International Telecommunication Union, "ITU Radio Regulations", International Telecommunication Union, 1992 (Current version: Edition of 2020).
3. European Parliament, "General Data Protection Regulation (GDPR)", European Parliament and Council of the European Union, 2016.
4. World Summit on the Information Society, "Declaration of Principles (Building the Information Society: A Global Challenge in the New Millennium)", WSIS-03/Geneva/Doc/4-E, December 2003 & World Summit on the Information Society, "Action Plan", WSIS-03/Geneva/Doc/5-E, December 2003.
5. World Summit on the Information Society, "Tunis Agenda for the Information Society", WSIS-05/Tunis/Doc/6(Rev.1)-E, November 2005 & World Summit on the Information Society, "Tunis Commitment" WSIS-05/Tunis/Doc/7-E, November 2005.

این گروه از دولت‌ها، گرایش برخی دیگر به اتخاذ سیاست‌های صرفاً محدود و ممنوع‌کننده، دستیابی به چارچوبی حقوقی را که ضمن برخورد با تبعات ناهنجار استفاده از وب‌پنهان، حافظ حقوق قطعی کاربران قانون‌مند باشد، دشوار کرده است.

بنابراین نه‌تنها سند حقوقی خاصی به مقوله نظام‌مندی وب‌پنهان اختصاص نیافته، بلکه با نگاهی به اسناد بین‌الملل محدود موجود در زمینه اینترنت نیز می‌توان دریافت که جز برخی موارد محدود در اسناد عام این حوزه نیز مقرره‌ای برای حکومت بر این حوزه تدوین نشده است. علاوه بر این، دورنمایی از شکل‌گیری عرف بین‌المللی نیز به چشم نمی‌خورد. عملکرد متشتت دولت‌ها در مواجهه با وب‌پنهان عملا احراز رویه هم‌سوی دولت‌ها، به‌عنوان یکی از عناصر دوگانه شکل‌گیری عرف بین‌المللی را با دشواری مواجه کرده است. در چنین شرایطی انفعال برخی از دولت‌ها نیز بر این چالش دامن می‌زند. با توجه به تحولات سریع فناوری نوظهوری همچون وب‌پنهان، شکیبایی برای شکل‌گیری رویه هم‌سوی دولت‌ها که با باور به الزام‌آور بودن توأم باشد، مطلوب نیست.

۳.۲. حقوق بین‌الملل موجود و وب‌پنهان

دو دیدگاه در خصوص ارتباط حقوق بین‌الملل عمومی و حقوق اینترنت و چگونگی واکنش حقوقی بین‌المللی به مقوله اینترنت مطرح شده است. دیدگاه اول با عنوان رویکرد «حقوق سایبر»[1] تأکید دارد که اینترنت اشکال جدید و بی‌سابقه‌ای از تعاملات اجتماعی را سبب شده است. این مدیوم با ساختار سرزمین‌محور حقوق بین‌الملل که مبتنی بر دولت حاکم می‌باشد، بیگانه است و سرعت بالا و حجم عظیم ارتباطات، سبب شده که قواعد حقوقی موجود کارکردی برای نظام‌مندی این حوزه نداشته باشند. از این رو قواعد خاص و جدیدی برای حکومت بر این حوزه لازم است و قواعد موجود حقوق بین‌الملل عام و حتی قواعد بین‌المللی حاکم بر اشکال سنتی ارتباطات مناسب و کافی نخواهند بود. در نتیجه تنها قواعدی که به‌طور خاص متناسب با ویژگی‌های منحصر به فرد دنیای اینترنت تکوین یافته و تدوین می‌شوند، قابلیت حکومت بر آن را دارد.

1. Cyber Law

از سوی دیگر، رویکرد موسوم به «حقوق واقعی»[1] تأکید دارد که اینترنت به لحاظ کارکردی تفاوتی با سایر فناوری‌های ارتباط راه دور ندارد و زمینه‌ساز نوعی از تعامل اجتماعی به حساب می‌آید. از این رو کلیه قواعدی که برای حکومت بر رفتار اجتماعی موجودیت‌های حقیقی و قانونی وضع شده، در صورت لزوم برای تعاملات تسهیل شده از طریق اینترنت نیز قابل اعمال است. در نتیجه کلیه مقررات موجود حقوق بین‌الملل، اعم از مقررات حقوق بین‌الملل عام و مقررات خاص ناظر بر ارتباطات راه دور بر چالش‌های ناشی از دنیای سایبر نیز حاکم خواهد بود.

با ملاحظهٔ واقعیت‌های حاکم بر جامعهٔ بین‌الملل، ضرورت واکنش سریع حقوقی به مقولهٔ اینترنت به صورت کلی و نیز چالش‌های جزئی‌تر آن، فقدان ارادهٔ سیاسی و اجماع مورد نیاز برای طراحی چارچوب‌های حقوقی مناسب و کافی و تشتت عملکرد دولت‌ها، رویکرد حقوق سایبر اگرچه منطقی به نظر می‌رسد، عملاً در کوتاه‌مدت، کارآمد و راهگشا نیست و در نهایت جامعهٔ جهانی را به سمت وضعیت اولیه معتقد به آزادی مطلق فضای سایبر سوق می‌دهد که امروزه دیگر مطلوب و پذیرفتنی نیست. رویکرد حقوق واقعی نیز توجه کافی به ویژگی‌ها و امتیازات اینترنت و حوزه‌های خاص آن مانند وب‌پنهان ندارد و در عمل نمی‌تواند پاسخگوی چالش‌های حقوقی کنونی و آینده آن باشد.

با این اوصاف، به نظر می‌رسد جمع دو رویکرد نتیجهٔ منطقی و منطبق با واقعیات را فراهم می‌آورد؛ در کوتاه‌مدت که حقوق بین‌الملل قواعد خاص مربوط به اینترنت و وب‌پنهان را تدارک ندیده است، مقررات موجود حقوق بین‌الملل، اعم از مقررات حقوق بین‌الملل عام و مقررات خاص، ناظر بر ارتباطات راه دور ظرفیت‌های ارزشمندی هستند که برای پاسخ به نیازها و چالش‌های موجود ناگزیر مورد استفاده قرار می‌گیرند. به همین دلیل در اجلاس‌های دوگانه مجمع جهانی جامعهٔ اطلاعاتی، اعمال مقررات عام و از پیش موجود حقوق بین‌الملل بر حوزهٔ اینترنت و کلیه بخش‌های نوظهور آن از جمله وب‌پنهان، مورد تأیید قرار گرفته است. این مجمع بر امکان و ضرورت استفاده از مکانیزم‌های حقوق داخلی و بین‌المللی موجود، تأکید داشته است.[2] ولی با توجه به آنچه در خصوص اهمیت وب‌پنهان و ضرورت توجه مستقل حقوق بین‌الملل به

1. Real Law
2. Kurbalija, J. "Internet Governance and International Law" In Drake, WJ. (ed.), *Reforming Internet Governance: Perspectives from the Working Group on Internet Governance*, New York: United Nations Information and Communication Technologies Task Force, 2005,p 106.

آن گفته شد، این مقررات موجود همراه با خلأهای جدی بوده و پاسخگوی نیازهای کنونی و آینده نمی‌باشد و تدوین مقررات خاص گریزناپذیر به نظر می‌رسد.

به همین دلیل است که مجمع مذکور ضمن پذیرش حوزه‌های کاملاً فاقد قاعده که نیاز به نظام‌مندی ویژه دارند، طرح‌هایی پیشنهادی برای تدوین کنوانسیونی خاص را نیز در کنار تأکید بر اعمال مقررات عام و از پیش موجود حقوق بین‌الملل ارائه می‌نماید. تا زمان شکل‌گیری اراده‌ای منسجم برای ایجاد قواعد حاکم بر مناسبات کاربران وب‌پنهان، باید به قواعدی که پیش‌تر به‌عنوان قواعد حقوق بین‌الملل قوام یافته‌اند، متوسل شد.

۴. انتظارها از حقوق بین‌الملل

کارکردهای حقوق بین‌الملل در پاسخ به چالش‌های موجود در خصوص وب‌پنهان را از چند نظر می‌توان بررسی کرد: در وهلهٔ نخست قواعد و اصول مستقر حقوق بین‌الملل که در قالب منابع مختلف این نظام تجلی می‌یابند، به اشکال مختلف توانایی نظام‌مند کردن وب‌پنهان و پر کردن خلأهای حقوقی مربوط به این حوزه را دارند. از سوی دیگر استفادهٔ حداکثری از ظرفیت‌های حقوق بین‌الملل می‌تواند ضمن کمک به گذر از وضعیت بی‌قاعدگی در حوزهٔ وب‌پنهان، زمینه را برای تدوین چارچوب‌های حقوقی منسجم و کارآمد، فراهم کند.

۴.۱. کاربرد ظرفیت‌های موجود حقوق بین‌الملل عام و وب‌پنهان

با نگاهی به گنجینهٔ حقوق بین‌الملل عام می‌توان دریافت که برخی از اسنادی که در حوزه‌های مختلف تدوین یافته‌اند، با نگاه به آینده و معضلات بالقوهٔ آن، چنان دامنهٔ وسیعی دارند که امکان اعمال آن بر طیف گسترده‌ای از موضوعات وجود دارد. این قبیل اسناد که عمدتاً در زمرهٔ حقوق بین‌الملل عام طبقه‌بندی می‌شوند و برخی آنها امروزه خصیصهٔ عرفی یافته‌اند، برای موضوع نوظهوری همچون وب‌پنهان نیز کاربرد دارند.

به‌عنوان مثال، میثاق بین‌الملل حقوق مدنی و سیاسی اگرچه چندین دهه پیش از فراگیر شدن اینترنت و وب‌پنهان تدوین شده، اما با بیان موسع از موضوعاتی همچون حق حریم خصوصی یا حق آزادی بیان تا حدودی به روشن شدن برخی ابهامات در بعضی از جنبه‌های – عمدتاً مثبت و مشروع– استفاده از وب‌پنهان کمک کرده است. اسناد دیگری همچون کنوانسیون

تجارت تسلیحات،[1] کنوانسیون برن در حمایت از آثار ادبی و هنری،[2] مقررات ارتباطات راه دور بین‌المللی و کنوانسیون ملل متحد علیه جرائم سازمان‌یافته فراملی[3] نیز با دامنهٔ موضوعی محدودتر، حاوی مقرراتی هستند که در خصوص تهدیدهای ناشی از اعمال نامشروعی که در چارچوب وب‌پنهان صورت می‌گیرد، تا حدودی می‌توانند مؤثر و راهگشا باشند.

رژیم‌های حقوقی بین‌المللی طراحی شده برای مقابله با تجارت غیرمجاز تسلیحات و موادمخدر نیز حاوی مقرراتی است که می‌تواند بر مبارزه با مبادلات ناظر بر این قبیل اقلام که در بازارهای وب‌پنهان جریان دارند، مؤثر باشند. اگرچه هیچ یک از اسناد بین‌المللی که در این زمینه تدوین شده‌اند، همچون کنوانسیون تجارت اسلحه و کنوانسیون‌های سه‌گانه ملل متحد راجع به مبارزه با موادمخدر و روان‌گردان،[4] به تجارت ناشناس این اقلام در محیطی به نام وب‌پنهان صریحاً اشاره ندارند، اجرای مناسب مقررات آنها با محدود کردن زمینه‌های این شکل از تجارت و متعهد کردن دولت‌ها به پیشگیری و مقابله با آن، مبانی لازم برای واکنش‌های حقوقی، قضایی و اجرایی دولت‌ها را شکل می‌دهند.

همین امر در خصوص مسئلهٔ تروریسم که به یکی از ابعاد پرخطر وب‌پنهان تبدیل شده نیز صادق است. اسناد بین‌الملل متعددی تاکنون در زمینهٔ مقابله با اشکال مختلف عملکرد تروریست‌ها و نیز شیوه‌های تقویت آنها در سطوح منطقه‌ای و بین‌المللی تدوین شده‌اند که از آنها می‌توان به‌عنوان مبانی حقوقی مناسبی برای احراز تعهد دولت‌ها نسبت به مقابله با این رفتارها، قطع نظر از اینکه در چه محیط یا با استفاده از چه ابزاری واقع شده باشند، یاد کرد.

به‌عنوان مثال، یکی از اشکال استفاده از وب‌پنهان در خدمت تروریسم، تأمین مالی به‌وسیله تبلیغات، استفاده از پلتفرم‌های ارتباطی امن و روش‌های پرداخت ناشناس است. در این خصوص

1. United Nations, "The Arms Trade Treaty", April 2013.
2. Berne Convention for the Protection of Literary and Artistic Works", September 1886.
3. "United Nations Convention against Transnational Organized Crime (Palermo Convention)", December 2000.
۴. اسناد سه گانه سازمان ملل متحد شامل: کنوانسیون واحد در خصوص مواد مخدر (۱۹۶۱)، کنوانسیون راجع به مواد روان‌گردان (۱۹۷۱) و کنوانسیون ملل متحد بر علیه قاچاق مواد مخدر و روان‌گردان (۱۹۸۸).
See: "Single Convention on Narcotic Drugs", March 1961 & "Convention on Psychotropic Substances", February 1971 & "United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances", December 1988.

کنوانسیون مبارزه با تأمین مالی تروریسم[1] مقررات ضروری برای متعهد کردن دولت‌ها به مقابله با اقدامات می‌باشد.

همچنین قطعنامه‌های متعدد شورای امنیت در زمینه مبارزه با تروریسم نیز در این راستا قابل استناد هستند. به‌عنوان مثال، قطعنامه ۱۶۲۴ شورای امنیت[2] در خصوص ممنوعیت تحریک به ارتکاب اعمال تروریستی، بر فعالیت گستردهٔ گروه‌های تروریستی در زمینهٔ تبلیغ، عضوگیری و تشویق افراد به ارتکاب این قبیل رفتارها که در پوشش امن ناشناسی فراهم شده در محیط وب‌پنهان صورت می‌گیرند، قابل اعمال است.

علی‌رغم کاستی‌هایی که در زمینهٔ اسناد تدوین شده در زمینهٔ حقوق بین‌الملل اینترنت به‌طور خاص وجود دارد، به هر روی قواعدی هر چند اندک، در طول سه دهه اخیر در این حوزه شکل گرفته‌اند که با تفسیری موسع از این مقررات امکان اعمال آنها در حوزهٔ خاصی همچون وب‌پنهان نیز وجود دارد. از جملهٔ این اسناد می‌توان به کنوانسیون جرائم سایبری شورای اروپا اشاره کرد. این سند علی‌رغم منطقه‌ای بودن و تعداد محدود طرف‌های عضو، ضمن بیان تعهد دولت‌ها در خصوص وضع مقررات در حوزه‌هایی چون سوءاستفاده از دستگاه‌های ارتباطی، نقض حقوق معنوی و هرزه‌نگاری کودکان، با تأکید بر ضرورت تقویت همکاری‌های بین‌المللی حداکثری، سریع، مؤثر و قابل اتکا در راستای مقابله با جرائم سایبری، راهکارهایی را برای تسهیل این همکاری‌ها معرفی می‌کند. با توجه به اینکه برخی از جرائم رایج در محیط وب‌پنهان در این سند نیز مورد اشاره قرار گرفته‌اند، در سطحی نسبتاً محدود مقررات آن نسبت به وب‌پنهان قابل اعمال است.

مقررهٔ عمومی حفاظت از داده‌های اتحادیه اروپا نیز با وجود کاستی‌هایی مشابه کنوانسیون فوق، تا حدودی در بیان موضوعات تضمین‌کنندهٔ حقوق کاربران وب‌پنهان، کارآمد است. از جملهٔ این حقوق می‌توان به حق حفاظت از داده‌های شخصی، حق بر فراموش شدن و حق محدود کردن پردازش داده‌ها اشاره کرد. همچنین این مقرره پردازش داده‌هایی را که عمداً به گونه‌ای ذخیره شده‌اند که شخص موضوع آن داده‌ها قابل شناسایی نباشند، از دامنهٔ مقررات عام این سند

1. United Nations, "International Convention for the Suppression of the Financing of Terrorism", December 1999.
2. United Nation Security Council Resolution on Prohibition of Incitement to Commit Terrorist Acts, S/RES/1624, 2005.

راجع به پردازش داده‌های متعلق به اشخاص خارج کرده و به صورت ضمنی این دسته از داده‌ها را مستحق حمایت ویژه دانسته است.

در مجموع می‌توان گفت بخش قابل توجهی از آنچه که امروز به‌عنوان اصول حقوق بین‌الملل در خصوص اینترنت شناخته می‌شود و دربارهٔ وب‌پنهان نیز قابل اعمال است، برآمده از اسناد حقوق بین‌الملل عام، عرف‌های بین‌المللی و اصول کلی حقوقی و گاه قواعد آمره‌ای است که با دامنهٔ شمول وسیع خود برای پاسخگویی به چالش‌های حقوقی وب‌پنهان در سطح بین‌المللی کاربرد دارند.

۴.۲. سایر ظرفیت‌های حقوق بین‌الملل در رابطه با وب‌پنهان

حقوق بین‌الملل واجد ظرفیت‌هایی است که اگرچه کارکرد محدودی نسبت به منابع سنتی حقوق بین‌الملل دارد، توسل به آنها می‌تواند راهگشا باشد و زمینهٔ شکل‌گیری قواعد خاص، جامع و تکامل‌یافته برای وب‌پنهان باشد.

۴.۲.۱. اسناد غیرالزام‌آور و حقوق نرم

اسناد بین‌المللی که در زمرهٔ اسناد نرم طبقه‌بندی می‌شوند، می‌توانند در فراهم آوردن زمینهٔ برون‌رفت از چالش‌های ناشی از عدم تدوین سند الزام‌آور بین‌المللی برای وب‌پنهان کارگشا باشند. تاکنون در زمینهٔ اینترنت به صورت عام تلاش‌های قابل توجهی در زمینهٔ تدوین اسناد حقوق نرم صورت گرفته که در نتیجه آنها تا حدودی زمینه‌های تدوین چارچوب‌های حقوقی الزام‌آور فراهم شده است.

از جملهٔ این دستاوردها می‌توان به اعلامیه نهایی اجلاس سال ۲۰۰۳ مجمع جهانی جامعه اطلاعاتی، برنامه عمل اجلاس ۲۰۰۵ مجمع جهانی جامعه اطلاعاتی، دستورالعمل‌های دوگانهٔ تالین در خصوص حقوق بین‌الملل قابل اعمال بر جنگ سایبری که در سال‌های ۲۰۱۳[1] و ۲۰۱۷[2] توسط گروه کارشناسان بین‌المللی به دعوت مرکز عالی همکاری‌های دفاع سایبری ناتو

1. NATO Cooperative Defence Center of Excellence, "Tallinn Manual on the International Law Applicable to Cyber Warfare", 2013.
2. NATO Cooperative Defence Center of Excellence, "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations", 2017.

تدوین شده و گزارش‌ها، قطعنامه‌ها و اعلامیه‌های سازمان ملل متحد و سایر سازمان‌های بین‌المللی در خصوص نظام‌مندی اینترنت و مسائل مرتبط با آن اشاره کرد.

چنان‌که بررسی شد، یکی از چالش‌های نظام‌مندی وب‌پنهان، تفاوت رویکرد دولت‌ها نسبت به مسائل زیربنایی این پدیده، از جمله موضوع گمنامی است. توسل به اسناد نرم حقوق بین‌الملل زمینهٔ اعتمادسازی متقابل را فراهم می‌کند و با توجه به بار رسمی کمتر نسبت به اسناد الزام‌آور، نگرانی‌ها و تردیدهای دولت‌هایی را که به‌دلیل موانع داخلی و تفاوت در سیاست‌های عمومی، آماده پذیرش چارچوب‌های حقوقی سخت نیستند، برطرف می‌کند و همسو شدن دولت‌ها در بخش‌هایی را که حداقل اتفاق‌نظر در خصوص آنها وجود دارد، ممکن می‌سازد.

تدوین چنین اسنادی که در پی برگزاری مجامعی متشکل از تعداد قابل توجهی از دولت‌ها با رویکردها و سطوح مختلف فناوری تدوین می‌شود، توجه دولت‌های نسبتاً منفعل‌تر را به تحولات نوینی همچون وب‌پنهان جلب می‌کند. در چنین مجامعی دغدغه‌های دولت‌های پیشگام و بهره‌مند از توان فنی و انسانی بهتر در زمینهٔ فناوری برای سایر دولت‌ها مطرح می‌شود و زمینهٔ آشنایی دولت‌های کمتر بهره‌مند از فناوری با معضلات بالقوه و بالفعل وب‌پنهان و در نتیجه درک ضرورت واکنش حقوقی توسط آنها، همگام با سایر دولت‌های پیشرفته فراهم می‌آید.

به علاوه انعطاف‌پذیر بودن اسناد نرم بین‌المللی این امکان را فراهم می‌آورد که رویکردهای جدید و متفاوت دربارهٔ پدیده‌های نوینی همچون وب‌پنهان، فرصت آزمون و خطا داشته باشند و در صورت نیاز، متناسب با تحولات سریع، اصلاح و سازگار شوند. این راهکار زمینه‌ای را فراهم می‌آورد که سازوکارهای جدید قانونی که در سطوح ملی آزمایش شده‌اند، مجال طرح و معرفی یابند و رویکردهای نوینی که کمتر در بدنهٔ حقوق بین‌الملل سنتی جایگاهی داشته‌اند، اما با واقعیت‌های دنیای فناوری و اینترنت سازگاری بیشتری دارند، در فضایی دور از تردیدها و ابهامات دولت‌ها مطرح شوند و مورد بررسی قرار گیرند.

البته اگرچه اسناد نرم حقوق بین‌الملل می‌توانند ابزاری ارزشمند برای حرکت در مسیر نظام‌مندسازی وب‌پنهان باشند و تا امروز نیز در عرصهٔ اینترنت به صورت عام کارکردهای مثبتی داشته‌اند، تاکنون جز برخی اشاره‌های محدود و غیرمستقیم به پیامدهای استفاده از وب‌پنهان در برخی گزارش‌های سازمان‌های بین‌المللی، شواهدی از بروز ارادهٔ دولت‌ها در بیان دیدگاه‌ها و

مواضع خود در خصوص وب‌پنهان به چشم نمی‌خورد و تنها می‌توان از آنها به‌عنوان ظرفیتی بالقوه در راستای نظام‌مندی این بخش پیچیده و پرچالش اینترنت یاد کرد.

۴.۲.۲. همکاری‌های بین‌المللی

مبانی عام همکاری‌های بین‌المللی در موارد ضرورت در برخی منابع حقوق بین‌الملل قابل تشخیص است که می‌تواند به‌عنوان یکی از ظرفیت‌های موجود حقوق بین‌الملل مورد توجه و استناد قرار گیرد.

اهداف ذکر شده در منشور ملل متحد چارچوب کلی تعهد دولت‌ها به همکاری در مواقع ضرورت را بیان کرده است. ماده ۱ منشور ملل متحد، یکی از اهداف این سازمان را دستیابی به همکاری بین‌المللی در حل معضلات بین‌المللی اعم از اقتصادی، اجتماعی، فرهنگی، بشردوستانه و یا برای ارتقای تشویق احترام به حقوق بشر و آزادی‌های بنیادین دانسته است. همین ماده که محتوای آن در اسناد دیگری همچون اعلامیه اصول حقوق بین‌الملل درباره روابط دوستانه و همکاری میان دولت‌ها مطابق منشور ملل متحد[1] مورد تصریح قرار گرفته، با بیانی موسع دولت‌های عضو را در زمینه طیف گسترده‌ای از موضوعات مکلف به همکاری کرده است. بی‌شک این دامنهٔ وسیع از موضوعات، وب‌پنهان را نیز دربرمی‌گیرد.

از سوی دیگر، برخی از اسناد نرم حقوق بین‌الملل از جمله اسناد ژنو ۲۰۰۳ و تونس ۲۰۰۵ مجمع جهانی جامعه اطلاعاتی ضمن اشاره به ضرورت همکاری‌های بین‌المللی در زمینهٔ اینترنت از تعهد دولت‌ها به تقویت همکاری‌ها به منظور دستیابی به پاسخ مشترک به چالش‌های این حوزه و اجرای برنامه‌ای پیش‌بینی شده در این اسناد سخن گفته‌اند که این امر از دید جامع تعداد قابل توجهی از دولت‌ها نسبت به مقوله همکاری بر مبنای اصول کلیدی مندرج در این اسناد حکایت دارد. این اسناد، همکاری‌های بین‌المللی در زمینه‌های مرتبط با وب‌پنهان، به‌خصوص در حوزه‌هایی همچون اجرای قانون و تعقیب و مجازات مجرمان را توجیه می‌نماید.

علی‌رغم فقدان سازوکار خاص، مناسب و فراگیر برای همکاری بین‌المللی دربارهٔ وب‌پنهان، الزام به همکاری‌های بین‌المللی در خصوص برخی از ابعاد منفی وب‌پنهان از قبیل معاملات

1. United Nations General Assembly, "Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations", A/Res/2625, 1971.

موادمخدر و روان‌گردان، هرزه‌نگاری، تروریسم، تجارت اسلحه و سایر اشکال جرائم سازمان‌یافته وجود دارد.

از جمله می‌توان به تعهد دولت‌های عضو کنوانسیون حقوق کودک[1] نسبت به اتخاذ کلیه تدابیر لازم ملی، دوجانبه و چندجانبه برای پیشگیری و مقابله با بهره‌برداری از کودکان در محتویات حاوی «هرزه‌نگاری»،[2] قطعنامهٔ موسوم به همکاری بین‌المللی بر علیه معضل جهانی موادمخدر،[3] تأکید ماده ۱۳ پروتکل اختیاری کنوانسیون مقابله با جرائم سازمان‌یافته فرامرزی ناظر بر منع ساخت و قاچاق تسلیحات،[4] همکاری دولت‌ها در سطوح دوجانبه، منطقه‌ای و بین‌المللی در راستای اهداف این سند، ماده ۱۸ کنوانسیون مبارزه با تأمین مالی تروریسم[5] و همچنین قطعنامه‌های متعدد مجمع عمومی[6] و شورای امنیت[7] سازمان ملل متحد که مکرراً بر ضرورت همکاری میان دولت‌ها در مبارزه با اشکال مختلف فعالیت‌های تروریستی و شیوه‌های تسهیل عملکرد آنها به‌عنوان تهدیدی برای صلح و امنیت بین‌المللی تأکید نموده‌اند، اشاره کرد.

1. United Nations, "Convention on the Rights of the Child", November 1989.

۲. ماده ۳۴، بند c کنوانسیون حقوق کودک

3. United Nations General Assembly, Resolution on "International Cooperation against the World Drug Problem", A/RES/53/115, 1999.

4. "Protocol against the Illicit Manufacturing of and Trafficking of Firearms, Their Parts and Components and Ammunition Supplementing the United Nations Convention against Transnational Organized Crimes", 2001.

5. United Nations, "International Convention for the Suppression of the Financing of Terrorism" 1999.

۶. از جمله اسنادی که به تصویب مجمع عمومی سازمان ملل متحد رسیده و به مسئله همکاری دولت‌ها در مبارزه با تروریسم اشاره دارد، می‌توان به اعلامیه تدابیر برای حذف تروریسم بین‌المللی (۱۹۹۴) و نیز راهبرد جهانی ضد تروریسم سازمان ملل متحد (۲۰۰۶) اشاره کرد.

See: United Nations General Assembly, Resolution on "Measures to Eliminate International Terrorism", A/RES/49/60, December 1994 & United Nations General Assembly, Resolution on "The United Nations Global Counter-Terrorism Strategy", A/RES/60/288/ September 2006.

۷. قطعنامه‌های ۱۳۷۳، ۱۳۷۷، ۱۴۵۶ (که بر نقش کمیته ضد تروریسم در همکاری میان دولت‌ها تاکید می‌کند)، ۱۵۴۰ (با تاکید بر همکاری دولت‌ها برای مقابله با تروریسم در چارچوب کنوانسیون تسلیحات بیولوژیک و سمی و همکاری در راستای جلوگیری از قاچاق سلاح‌های هسته‌ای، شیمیایی و بیولوژیک)، ۱۵۶۶ به طرق مختلف به الزام دولت‌ها به همکاری برای مقابله با اشکال مختلف تروریسم و روش‌های تسهیل فعالیت آنها اشاره دارند.

See: United Nations Security Council, S/RES/1373, September 2001 & United Nations Security Council, S/RES/1377, November 2001 & United Nations Security Council, S/RES/1456, January 2003 & United Nations Security Council, , S/RES/1450, April 2004 & United Nations Security Council, S/RES/1566, October 2004.

در این میان برخی اسناد، حاوی الزامات صریح‌تری هستند. به‌عنوان مثال، قطعنامه ۱۶۲۴ شورای امنیت تأکید می‌کند که با توجه روند روزافزون جهانی شدن لازم است که دولت‌ها در راستای جلوگیری از بهره‌برداری تروریست‌ها از فناوری‌های نوین پیچیده، ارتباطات و منابع برای تحریک به ارتکاب و پشتیبانی از اعمال تروریستی همکاری داشته باشند.[1]

1. United Nation Security Council Resolution on Prohibition of Incitement to Commit Terrorist Acts, S/RES/1624, 2005, p 2.

نتیجه‌گیری

فقدان واکنش حقوقی خاص، مناسب و فراگیر به وب‌پنهان در سطح بین‌المللی، آثاری از قبیل مصونیت و امنیت کاربران هنجارشکن، محروم شدن کاربران قانونمند از حقوق مشروع خود در برخی دولت‌ها و قرار گرفتن دولت‌ها در معرض مسئولیت بین‌المللی را به دنبال دارد. در این شرایط، کاربرد قواعد موجود حقوق بین‌الملل برای چالش‌های بین‌المللی خاص وب‌پنهان است، راهکاری کوتاه‌مدت محسوب می‌شود و نمی‌تواند پاسخگوی همهٔ نیازها باشد. همچنین همسوسازی مقررات ملی و تدوین اسناد دوجانبه یا چندجانبه راجع به همکاری‌های اجرایی و قضایی در خصوص جرائمی که در محیط وب‌پنهان واقع می‌شود نیز می‌تواند کاستی راهکارهای صرفاً ملی و خلأهای ناشی از فقدان قواعد بین‌المللی در این حوزه را در کوتاه‌مدت تا حدودی جبران نماید.

اما رویکرد مطلوب و بلندمدت، شکل‌دهی قواعد خاص بین‌المللی برای وب‌پنهان است که حقوق بین‌الملل با رعایت دو ملاحظهٔ مهم، ناگزیر به سوی آن حرکت خواهد کرد. ملاحظهٔ نخست مربوط به تلاش برای حذف موانع رسیدن به اجماع جهانی در حوزهٔ وب‌پنهان شامل شکاف عمیق مواضع دولت‌ها در خصوص مسائل چالشی، اختلاف‌نظرهای جدی راجع به اصول و هنجارهای بنیادین این حوزه و فقدان یا نقصان زیرساخت‌های فنی و نیروی انسانی متخصص است. اسناد غیرالزام‌آور و حقوق نرم و همکاری‌های بین‌المللی بهترین ظرفیت‌های حقوق بین‌الملل برای عبور از این چالش‌ها محسوب می‌شوند.

ملاحظهٔ دوم ضرورت توجه به واقعیت‌های موجود در وب‌پنهان به‌خصوص حجم قابل توجه فعالیت‌های غیرقانونی است که با سوءاستفاده از حجاب گمنامی انجام می‌گیرد. با توجه به این واقعیت‌ها، آزادی مطلق فضای سایبر کارآمد نیست؛ بلکه راهکار معقول برای تدوین قواعد بین‌المللی در حوزهٔ وب‌پنهان، اولویت دادن به آزادی فضای سایبر از جمله وب‌پنهان برای حمایت از کارکردهای قانونمند و تعدیل و تحدید این آزادی‌ها بر اساس واقعیت‌های موجود و ملاحظات مشروع پذیرفته شده در حقوق بین‌الملل می‌باشد.

فهرست منابع

الف) منابع فارسی

مقاله

۱.انصاری، باقر و شیما عطار، **حمایت از داده‌ها در چین؛ مطالعهٔ تطبیقی با رویکرد حمایت از داده‌ها در امریکا و اتحادیهٔ اروپا**، مجله مطالعات حقوق تطبیقی، دوره ۱۳، ۱۴۰۱، شماره ۳، صص ۹۱-۱۱۳.

۲.رجبی، عبداله و نسرین ترازی، **بررسی انتقادی حاکمیت حقوقی ساختار فنی اینترنت بر فضای مجازی**، فصلنامه تحقیقات حقوقی، دوره ۲۰، ۱۳۹۶، شماره ۸۰، صص ۳۰۷-۳۸۳.

ب) منابع انگلیسی

Books

3.Chen H. *Dark web: Exploring and Data Mining the Dark Side of the Web*. Springer, 2011.

4.Finklea, K. "*Dark Web*", United States: Congressional Research Service, Prepared for Members and Committees of Congress, 2017.

5.Mendel, T. Puddephatt, A. Wagner, B. Hawtin, D. & Torres, N. *Global Survey on Internet Privacy and Freedom of Expression*. UNESCO, 2012.

Articles and Book Chapters

6.Al Nabki, M.W. Fidalgo, E. Alegre, E. & De Paz, I. "Classifying Illegal Activities on TOR Network Based on Web Textual Contents" In *Proceedings of the 15th Conference of the European Chapter of the Association for Computational Linguistics*, 1, 2017, pp 35-43.

7.Bailurkar, R. Chaursia, P. & Goswami, A. "The Deep Web", *International Journal of Scientific and Engineering Research*, 8.2, 2017, pp 60- 63.

8.Bergman, M. "White Paper: The Deep Web: Surfacing Hidden Value", *The Journal of Electronic Publishing*, 7.1, 2001, pp 1-17.

9.Breckheimer, P.J. "A Haven for Hate: The Foreign and Domestic Implications of Protecting Internet Hate Speech Under the First Amendment", *Southern California Law Review*, 75, 2001, pp 1493-1528.

10. Chertoff, M. "A Public Policy Perspective of the Dark Web", *Journal of Cyber Policy*, 2, 2017, pp 26-38.
11. Denker, K. Schäfer, M. & Steinebach, M. "Darknets as Tools for Cyber Warfare" In Reuter, C. (ed.) *Information Technology for Peace and Security*. Wiesbaden: Springer Vieweg, 2019.
12. Goldberg, I. "Privacy Enhancing Technologies for Internet III: Ten Years Later", Published in Alessandro Acquisit, A., Gritzalis, S., Lambrinoudakis, C & di Vimercati, S. (eds.) *Digital Privacy: Theory, Technology and Practice*, Auerbach Publications, 2007, pp 3-16.
13. Hatta, M. "Deep Web, Dark Web, Dark Net: a Taxonomy of "Hidden" Internet" *Annals of Business Administrative Science*, 19, 2020, pp 277-292.
14. Hernández, I. Rivero, C.R. & Ruiz, D. "Deep Web Crawling: A Survey" *World Wide Web*, 22, 2019, pp 1577–1610.
15. Kavallieros, D. Myttas, D. Kermitsis, E. Lissaris, E. Giataganas, G. & Darra, E. "Using the Dark Web" In Akhgar, B. Gercke, M. Vrochidis, S. & Helen G. (eds.) *Dark Web Investigation*, Springer, 2021.
16. ---------- "Understanding the Dark Web" In Akhgar, B. Gercke, M. Vrochidis, S. & Helen G. (eds.) *Dark Web Investigation*, Springer, 2021.
17. Kukkola, J. "The Russian National Segment of the Internet as a Source of Structural Cyber Asymmetry", In Stevens, T. Ertan, A. Floyd, K. & Pernik, P. (eds), *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*, Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2020.
18. Kurbalija, J. "Internet Governance and International Law" In Drake, WJ. (ed.), *Reforming Internet Governance: Perspectives from the Working Group on Internet Governance*, New York: United Nations Information and Communication Technologies Task Force, 2005.
19. Land, M. "Toward an International Law of the Internet" *Harvard International Law Journal*, 54, 2013, pp 393 – 458.
20. Lusthaus, J. "Beneath the Dark Web: Excavating the Layers of Cybercrime's Underground Economy", In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 2019, pp 1-7.
21. Raghavan, S. & Garcia-Molina, H. (2001), "Crawling the Hidden Web", Published in *Proceedings of 27th International Conference on Very Large Pages (VLDB)*, Roma, 2001, pp 129-138.

Documents

22. Berne Convention for the Protection of Literary and Artistic Works", September 1886.
23. Council of Europe, "EU Cybercrime Treaty (Budapest Convention)", European Treaty Series, No. 185, Budapest, 2001.
24. European Parliament, "General Data Protection Regulation (GDPR)", European Parliament and Council of the European Union, 2016.
25. International Telecommunication Union, "ITU Radio Regulations", International Telecommunication Union, 1992 (Current version: Edition of 2020).
26. NATO Cooperative Defence Center of Excellence, "Tallinn Manual on the International Law Applicable to Cyber Warfare", 2013.
27. NATO Cooperative Defence Center of Excellence, "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2017.
28. Protocol Against the Illicit Manufacturing of and Trafficking of Firearms, Their Parts and Components and Ammunition Supplementing the United Nations Convention against Transnational Organized Crimes", 2001.
29. United Nations General Assembly, "Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations", A/Res/2625, 1971.
30. United Nations General Assembly, Resolution on "International Cooperation against the World Drug Problem", A/RES/53/115, 1999.
31. United Nations General Assembly, Resolution on "Measures to Eliminate International Terrorism", A/RES/49/60, December 1994.
32. United Nations General Assembly, Resolution on "The United Nations Global Counter-Terrorism Strategy", A/RES/60/288/ September 2006.
33. United Nations, "The Arms Trade Treaty", April 2013.
34. "United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances", December 1988.
35. "United Nations Convention against Transnational Organized Crime (Palermo Convention)", December 2000.
36. United Nations, "Convention on Psychotropic Substances", February 1971.
37. United Nations, "Convention on the Rights of the Child", November 1989.

38. United Nations, “International Convention for the Suppression of the Financing of Terrorism” 1999.
39. United Nations “Single Convention on Narcotic Drugs”, March 1961.
40. United Nations Security Council, “Fourth Report of Secretary-General on the Threat Posed by ISIL (Daesh) to International Peace and Security and the Range of United Nations Efforts in Support of Member States in Countering the Threat”, S/2017/97, 2017.
41. United Nations Security Council, S/RES/1373, September 2001.
42. United Nations Security Council, S/RES/1377, November 2001.
43. United Nations Security Council, S/RES/1456, January 2003.
44. United Nations Security Council, S/RES/1450, April 2004.
45. United Nations Security Council, S/RES/1566, October 2004.
46. United Nation Security Council, “Resolution on Prohibition of Incitement to Commit Terrorist Acts”, S/RES/1624, September 2005.
47. World Summit on the Information Society, “Action Plan”, WSIS-03/Geneva/Doc/5-E, December 2003.
48. World Summit on the Information Society, “Declaration of Principles (Building the Information Society: A Global Challenge in the New Millennium)”, WSIS-03/Geneva/Doc/4-E, December 2003.
49. World Summit on the Information Society, “Tunis Agenda for the Information Society”, WSIS-05/Tunis/Doc/6(Rev.1)-E, November 2005.
50. World Summit on the Information Society, “Tunis Commitment” WSIS-05/Tunis/Doc/7-E, November 2005.

Cases

51. European Court of Human Rights, Ahmet Yildirim v. Turkey, 311/10, 2012.
52. United States of America v. Ross William Ulbricht, a/k/a "Dread Pirate Roberts", a/k/a "DPR", a/k/a Silk Road, United States District Court Southern District of New York, Indictment, 14 CRIM 068, February 2014.