نشریه علمی آفاق امنیت

۶۱

سال شانزدهم
زمستان ۱۴۰۲

مقاله پژوهشی

تاریخ دریافت:
۱۴۰۲/۰۳/۱۰
تاریخ پذیرش:
۱۴۰۲/۰۹/۲۹
صص: ۱۹۱-۱۶۲

شاپا چاپی: ۱۸۵۷-۲۵۳۸
الکترونیکی: ۵۲۵۰-۲۶۴۵

امکان‌سنجی حفظ امنیت ملی از طریق نظارت بر اینترنت و شبکه‌های اجتماعی از منظر قواعد بین‌المللی و رویه دولت‌ها

یاسر امین الرعایا [۱] | حسین امین الرعایا [۲*]

چکیده

از زمان پیدایش اینترنت و بالأخص گسترش شبکه‌های اجتماعی یکی از موضوعات مهم در امنیت ملی نظارت بر این شبکه‌ها بوده است؛ چراکه این شبکه‌ها درواقع میزبان یک مخزن وسیع و رو به رشد از داده‌ها هستند که همه آن‌ها به صورت دیجیتال است. واقعیت آن است که در زمینه شبکه‌های اجتماعی شاهد یک پارادوکس هستیم. از یک‌سو ضرورت دسترسی مردم به اطلاعات آزاد و از سوی دیگر تعهد ذاتی دولت‌ها در حفظ حریم خصوصی اطلاعات و نیز تأمین منافع عمومی و امنیت ملی. این تناقض در ایران از زمان مطرح‌شدن طرح «حمایت از حقوق کاربران و خدمات پایه کاربردی فضای مجازی» موردتوجه ویژه قرار گرفت. بطوریکه عده‌ای با نقد مواد این طرح نظارت بر اینترنت و شبکه‌های اجتماعی را به‌مثابه نقض قواعد حقوق بشری و غیرممکن دانسته وعده‌ای دیگر نظارت بر اینترنت و شبکه‌های مجازی را یک ضرورت تلقی نمودند. پرسشی که نوشتار حاضر در پی پاسخ به آن است، این مسئله است که با توجه به قواعد بین‌المللی و رویه کشورها آیا دولت‌ها می‌توانند جهت نظارت بر اینترنت و شبکه‌های اجتماعی برای حفظ امنیت ملی خود اقدام به وضع قانون نمایند؟ در پاسخ به این پرسش، پژوهش پیش‌رو با رویکردی توصیفی- تحلیلی و با استفاده از منابع کتابخانه‌ای و اسناد و رویه‌های قضائی معتبر بین‌المللی نگارش یافته و بر این فرض استوار است که اصول، قواعد و رویه عملی دولت‌ها و ازجمله جمهوری اسلامی ایران تماماً بر حق دولت‌ها نسبت به قانون‌گذاری جهت نظارت بر اینترنت و شبکه‌های اجتماعی تأکید می‌نماید.

کلیدواژه‌ها: امنیت ملی، نظارت، شبکه‌های اجتماعی، اینترنت، قواعد بین‌الملل، رویه دولت‌ها

DOR: 20.1001.1.25381857.1402.16.61.6.2

۱. نویسنده مسئول: پژوهشگر حقوق بین الملل و مدرس دانشگاه تهران، تهران، ایران aminroaya.yaser@yahoo.com
۲. دانشجوی دکتری حقوق بین‌الملل دانشگاه علامه طباطبایی، محقق حوزه سایبر و فضای مجازی، ایران، تهران

مقدمه

اینترنت به‌عنوان مؤلفه اصلی فضای مجازی یک فناوری با استفاده دوگانه است که می‌تواند بسته به نیت کاربران برای اهداف خوب یا بد استفاده شود. در حال حاضر، بیش از ۵ میلیارد کاربر اینترنت در جهان وجود دارد که بخش اعظم آن‌ها در آسیا و سپس در اروپا، آمریکای لاتین، کره‌ی شمالی، آفریقا و اقیانوسیه هستند. (Digital 2022 April Global Statshot Report (Apr 2022)) هرچند که ابداع اینترنت به دوران جنگ ویتنام بازمی‌گردد؛ اما استفاده عمومی از آن تنها دو دهه است که رواج یافته و امروزه به ابزاری جداناشدنی از زندگی هر فرد تبدیل شده است. به‌طوری‌که امروزه حتی در دورافتاده‌ترین نقاط جهان نیز استفاده از اینترنت مرسوم است. همچنین دسترسی همه افراد به شبکه اینترنت، امکان مبادله اطلاعات را در کم‌ترین و سریع‌ترین زمان ممکن فراهم کرده و این موضوع اینترنت را به مهم‌ترین ابزار ارسال و دریافت اطلاعات تبدیل کرده است. در حوزه تبادل اطلاعات امروزه شبکه‌های اجتماعی و پیام‌رسان‌ها به‌عنوان مهم‌ترین ابزار در این حوزه شناخته می‌شوند. اهمیت شبکه‌های اجتماعی تا جایی است که عده‌ای این رسانه‌ها را به‌عنوان یک ابزار غیرمتعارف طبقه‌بندی می‌نمایند؛ چراکه از یک‌سو افراد زیادی قادر به دستیابی به این شبکه‌ها می‌باشند و از سویی دیگر محتوای این شبکه‌ها توسط کاربران تهیه و منتشر می‌گردد. (Költzow,2013:10) در عین حال، رایگان بودن دسترسی به این شبکه‌ها موجب شده تعداد بسیار زیادی از مردم به این شبکه‌ها جهت به اشتراک گذاشتن اطلاعات گرایش پیدا نمایند. (Rosine, 2019: 53) به‌واقع ویژگی بارز شبکه‌های اجتماعی این است که این شبکه‌ها از قدرت عضوگیری بسیاری زیادی برخوردار هستند تا جائی‌که این شبکه‌ها می‌توانند نگرش‌ها و باورهای یک جامعه را تغییر و به سمت و سویی خاص هدایت نمایند (Fagan: 2018:396) لذا واقعیت این است که محیط اینترنت و بالأخص رسانه‌های اجتماعی نقش بسیار مؤثری در تولید هنجارها و ناهنجاری‌ها بر عهده‌دارند. همین مسئله باعث شده است که در سال‌های اخیر، مسائلی همچون حکمرانی اینترنت و قانون‌گذاری بر پلتفرم‌های دیجیتال از یک زمینه تخصصی در مطالعات اینترنت و رسانه‌های دیجیتال به خط مقدم بحث‌های علمی، سیاست‌گذاری و جامعه‌شناسی تغییر پیدا کند. واکنش‌ها به این موضوع بسیار متنوع بوده است. چراکه اگرچه شبکه‌های اجتماعی سبب تغییر و تحولات مثبت و شگرفی در حوزه ارتباطات شده، درعین‌حال

مخاطراتی نیز به همراه داشته است. ادوارد اسنودن در سال ۲۰۱۳ در خصوص گستره نظارت آژانس امنیت ملی ایالات‌متحده (ان اس ای)[1] نه‌تنها بر شهروندان ایالات‌متحده، بلکه کاربران شبکه‌های اجتماعی و شخصیت‌های سیاسی در سراسر جهان افشاگری‌هایی را صورت داد. ارتباطات نزدیکی که بین این آژانس و بسیاری از شرکت‌های پیشرو فناوری دیجیتال در جهان آشکار شد، روشن کرد که در عمل هیچ جدایی ساختاری بین اینترنت جهانی، سرمایه خصوصی و آژانس‌های نظارتی وجود ندارد.[2] همین امر بر تصویب نهایی مقررات حفاظت از داده‌های عمومی اتحادیه اروپا[3] تأثیر گذاشت. (Flow & Martin, 2022: 1) این موضوعات سبب شده است که کشورهای مصرف‌کننده یا دریافت‌کننده این پلتفرم‌ها خواهان اطمینان از این نکته باشند که کشورهای صاحب پلتفرم‌ها وشبکه های اجتماعی از این برتری در فضای اینترنت برای تضعیف حاکمیت، امنیت ملی، منافع تجاری و غیره آن‌ها استفاده نکنند. بدین‌جهت است که تمامی کشورها به دنبال مکانیسمی هستند که ضمن حمایت از دسترسی همه افراد به اینترنت و شبکه‌های اجتماعی، نظارت بر این شبکه را مدیریت نمایند. به‌عبارت‌دیگر این بر عهده مقامات ملی است که اطمینان حاصل کنند که این بستر تهدید علیه نظم و امنیت ملی ایشان محسوب نمی‌شود.[4] در ایران نیز توجه به نظارت بر اینترنت و شبکه‌های اجتماعی سال‌های متمادی است که

1. Nantioanl Security Agency(NSA)

۲. همچنین این افشاگری که جزئیات همکاری بین رسانه‌های اجتماعی و آژانس امنیت ملی ایالات‌متحده تحت پروژه‌ای به نام پریسم (PRISM) را افشا نمود تاثیر به سزایی بر اهمیت نظارت بر رسانه‌های اجتماعی و توجه جهانی به آن ایجاد نمود بطوریکه از آن زمان به بعد شیوه‌های نظارتی دولت‌ها گسترش یافت. (Cohen , 2017: 116-119)

3. General Data Protection Regulation (GDPR)

۴. در این خصوص به عنوان مثال مقام معظم رهبری تاکید می‌نمایند: «متأسّفانه در فضای مجازی کشور ما هم که آن رعایتهای لازم با وجود این همه تأکیدی که من کردم صورت نمی‌گیرد و در یک جهاتی واقعاً ول است. همه‌ی کشورهای دنیا روی فضای مجازی خودشان دارند اِعمال مدیریّت می‌کنند، [در حالی که] ما افتخار میکنیم به اینکه ما فضای مجازی را ول کرده‌ایم! این افتخار ندارد. فضای مجازی را بایستی مدیریّت کرد .» (مقام معظم رهبری، سخنرانی نوروزی با مردم، ۱۴۰۰/۱/۱) همچنین ایشان در سخنرانی مورخ ۱۴۰۱/۴/۷ در جمع مسئولین قضایی بیان داشتند: «نکته‌ی هفتم، مسئله‌ی امنیّت روانی مردم است. یکی از حقوق عامّه که گفتم اشاره میکنم این است؛ ... هر چند وقت یا چند روز یک بار، گاهی چند ساعت یک بار یک شایعه‌ای، یک دروغی، یک حرفی را یک آدم مشخّصی یا نامشخّصی در فضای مجازی منتشر میکند، مردم را نگران میکند، ذهن مردم را خراب میکند. یک دروغی را مطرح میکند، شایع میکند، خب، این امنیّت روانی مردم از بین میرود. یکی از وظایف قوّه‌ی قضائیّه برخورد با این مسئله است. البتّه اینجا هم من شنیدم بعضی گفتند که قانون نداریم؛ اوّلاً می‌شود از همین قوانین موجود استفاده کرد و حکم این را فهمید؛ اگر قانون هم ندارید، سریع قانون تهیّه کنید؛ اینها چیزهای مهمّی است.....»

مطرح‌شده لکن به هنگام مطرح‌شدن طرح «حمایت از حقوق کاربران و خدمات پایه کاربردی فضای مجازی»[1] بسیار داغ گردید.[2] به‌طوریکه از یک‌سو عده‌ای به حاکمیت بر نظارت بر فضای اینترنت و شبکه‌های اجتماعی تأکید دارند و از سوی دیگر کم نیستند نهادهای بین‌المللی[3] و کارشناسان داخلی و خارجی‌ای که تصویب نهایی این طرح را به‌مثابه ادامه تلاش مجلس شورای اسلامی برای محدود کردن اینترنت (خبرگزاری بی‌بی‌سی فارسی ، ۶ دی ۱۴۰۰) و یا پایان اینترنت آزاد در ایران و معادل «اینترنت ملی» می‌دانستند؛ چیزی شبیه آنچه در چین و کره شمالی جریان دارد. (دویچه وله فارسی، طرح صیانت از حقوق کاربران یا حذف مردم ایران از دهکده جهانی؟ ، ۷ مرداد ماه ۱۴۰۰) جدای از رسانه‌های خارجی، برخی از شخصیت‌های داخلی[4] و خبرگزاری‌های داخلی با نقد بخش‌هایی از این طرح درصدد ناکارآمد جلوه دادن اصل این طرح برآمدند. به‌عنوان نمونه، یکی از این خبرگزاری‌ها با تأکید بر غیرمنطقی بودن مجوز پیام‌رسان‌های داخلی و خارجی بیان می‌دارد: « واقعیت این است که طرح صیانت می گوید هر محتوایی که روی شبکه اینترنت جهانی قرار می گیرد چه در داخل کشور و چه در خارج کشور تهیه‌شده باشد باید از یک شورای خاص، مجوز فعالیت بگیرد. ... به‌خودی‌خود این تلقی که هرکسی هرجایی خواست کاری انجام بدهد باید از دولت مجوز بگیرد، باعث محدود شدن فعالیت‌ها یا دست‌کم حق بر دسترسی به محتویات آزاد اینترنت می‌شود.» (خبر آنلاین ، ۵/۷/ ۱۴۰۰)هرچند این طرح ضعف‌های بسیاری در حوزه اطلاع‌رسانی، وضعیت کسب‌وکارهای اینترنتی و غیره دارد، لکن به نظر می‌رسد نوع

---

۱. طرح حمایت از حقوق کاربران فضای مجازی و خدمات پایه کاربردی که در ابتدا با عنوان طرح ساماندهی پیام‌رسان‌های اجتماعی و طرح صیانت از حقوق کاربران در فضای مجازی و ساماندهی پیام رسان‌های اجتماعی مطرح گردید نام طرحی است که توسط نمایندگان دوره یازدهم مجلس شورای اسلامی پیشنهاد شده‌است. این طرح، یکی از خبرسازترین و پرحاشیه‌ترین طرح‌های مطرح شده در مجلس شورای اسلامی‌ست که با خود، انتقادات وسیعی را به همراه آورد (https://fa.wikipedia.org)

۲. این طرح در شش فصل و ۳۴ ماده تهیه گردید.

۳. سازمان گزارشگران بدون مرز روز چهارشنبه ششم مرداد ضمن محکوم کردن طرح محدودکننده اینترنت در ایران، این قانون را «تبعیضِ دیجیتال» علیه حق آگاهی مردم و برگرفته از روش سانسور در چین خواند.(رادیو فردا، ۲۰۲۱/۷/۸)

۴. حمدجواد آذری جهرمی، وزیر وقت ارتباطات و فناوری اطلاعات، این طرح را عامل انسداد فضای مجازی و مبهم‌تر شدن حکمرانی سایبری دانست.(پایگاه خبری تحلیلی انتخاب ۱۴۰۰/۴/۷) و یا سیدمحمد خاتمی در واکنش به این طرح گفت: «این طرح با روح قانون اساسی مغایر است و در کوتاه مدت حاصل آن نارضایتیِ به حقِّ مردم و خللِ بیشتر در زندگیِ تحت‌فشار آنان است و هزینه‌های بی‌فایده، بلکه پرضرر برای کشور و ملت و دولت دارد»(پایگاه خبری تحلیلی سلام نو، ۱۴۰۰/۵/۹)

واکنش‌ها به تصویب این طرح نه از جنس مخالفت‌ها با برخی از ابهامات مطروحه، بلکه مخالفت با اصل نظارت بر اینترنت و شبکه‌های اجتماعی از طریق تصویب این طرح می‌بود. حال سوای از تحلیل‌های سیاسی، نوشتار حاضر به دنبال پاسخ به این مسئله است که با توجه به قواعد حاکم بر حقوق بین‌الملل آیا دولت‌ها می‌توانند جهت نظارت بر اینترنت و شبکه‌های اجتماعی اقدام به وضع قانون نمایند؟ در پاسخ به این پرسش، مقاله پیشرو که با رویکردی توصیفی- تحلیلی و با استفاده از منابع کتابخانه‌ای و اسناد و رویه‌های قضائی معتبر بین‌المللی نگارش یافته است، بر این فرض استوار است که رویه بین‌المللی دولت‌ها و اصول قواعد بین‌المللی نظارت بر بستر اینترنت و شبکه‌های اجتماعی را به رسمیت شناخته‌اند.

چارچوب نظری

اینترنت، حقوق بشر و تکالیف دولت‌ها

با نگاهی به اسناد بین‌المللی حقوق بشری محرز می‌گردد یکی از حقوق مسلمی که آحاد یک جامعه به موجب حق دسترسی به اطاعات و حق آزادی بیان از آن برخوردار می‌باشند «حق دسترسی به اینترنت» می‌باشد. واقعیت آن است که بهره مندی از آزادی بیان و حق دسترسی آزاد به اطلاعات در زمره نسل اول حقوق بشر قرار دارد. برخورداری از حقوق نسل اول نیز مستلزم عدم دخالت حکومت در فرایند اعمال این حقوق و آزادی‌ها می‌باشد. (حبیب نژاد ، عصاره ، ۱۳۹۰ : ۱۹۲) در اهمیت حق آزادی بیان لازم به ذکر است که این حق در تمامی اسناد بین‌المللی حقوق بشر ازجمله ماده ۱۳ کنوانسیون آمریکایی حقوق بشر، ماده ۱۹ اعلامیه جهانی حقوق بشر ، ماده ۱۰ کنوانسیون اروپایی حقوق بشر، ماده ۱۹ میثاق بین‌المللی مدنی و سیاسی، ماده ۲۲ اعلامیه قاهره و ماده ۱۰ منشور آفریقایی حقوق بشر و ملت‌ها آمده است.

دربند ۲ ماده ۱۹ میثاق بین‌المللی مدنی و سیاسی، خصیصه‌ها و شاخصه‌های آزادی بیان ذکرشده است.[1] بر اساس این بند و استفاده از کلمه «هر وسیله دیگر»، آزادی بیان با هر ابزار و وسیله‌ای می‌باشد لذا با توجه به پیشرفت‌های فناورانه و تغییر و تحولی که در حوزه ارتباطات و

۱. بند ۲ ماده ۱۹ میثاق بین‌المللی مدنی و سیاسی :« هر کس حق آزادی بیان دارد. این حق شامل آزادی تفحص و تحصیل و اشاعه اطلاعات و افکار از هر قبیل بدون توجه به سر حدات خواه شفاهاً یا به صورت نوشته یا چاپ یا به صورت هنری یا به هر وسیله دیگر بانتخاب خود می‌باشد.»

اطلاعات صورت گرفته است، می‌توان دسترسی به اینترنت را به‌عنوان یکی از مصادیق آزادی بیان محسوب نمود . بـه عبـارتی دیگـر فضای بازی که اینترنت در اختیار مردمان جهان قرار داده است میدانی وسیع برای به‌کارگیری آزادی بیان به وجود آورده اســت و دسترســی بــه اطلاعــات موجــود در ایــن شبکه پهناور باعث شده تا افراد بتوانند به آسانی نسبت به ابراز عقاید و نظرات خود اقدام نمایند(امین الرعایا و همکاران ، ۱۴۰۰ : ۱۰۲) در این خصوص گزارشگر ویژه پیشبرد و حمایت از حق آزادی عقیده و بیان[1] در گزارش خـود بـه کمیسـیون حقـوق بشـر اظهـار مـی‌دارد؛ «چنانچه مردم دسترسی به اطلاعات و اینترنت نداشته باشند، آزادی بیـان از هرگونـه کـارایی تهـی می‌شود. دسترسی به اطلاعات برای شیوه زندگی مردم سالارانه جنبه اساسی دارد.» (همان) همچنین مفاد اسناد حقوق بشری نشان می‌دهد که وظیفه دولت‌هاسـت تـا امکانـات و ابـزار مناسـب جهـت بهره‌مندی مردم از این حق را ایجاد نمایند. بر این اساس در حوزه دسترسی به اینترنـت ایـن وظیفـه دولت‌هاست که زیرساخت‌هـای لازم، ابزارهـا، امکانـات و فنـاوری‌هـای موردنیـاز بـرای برقـراری ارتباط اینترنتی و تبادل اطلاعات مانند کابل، افزارها، مودم‌ها، رایانه‌ها و نرم‌افزارهای ضروری برای اتصال به اینترنت به‌عنوان یک وسـیلهٔ ارتبـاط جهـانی را در دسـترس افـراد قـرار دهنـد. (انصـاری، ۶۶:۱۳۹۹)

چالش‌های محتوایی شبکه‌های اجتماعی

واقعیت آن است که هرچند دسترسی به اینترنت و شبکه‌های اجتماعی به‌عنوان یک حق بشری محسوب می‌گردد لکن با نگاهی به شبکه‌های اجتماعی درمی‌یابیم که درزمینه محتوا این شـبکه‌هـا دارای چالش‌هایی می‌باشند: یکی از چالش‌های شبکه‌های اجتماعی توجه به این موضوع است کـه این شبکه‌ها در یک دهه اخیـر بـه‌طـور قابـل‌ملاحظـه‌ای بـرای افـزایش رعـب و وحشـت، جـذب، تحریـک، تـرور و تبلیـغ مورداسـتفاده گـروه‌هـای تروریسـتی (ماننـد داعـش) و نیـز جهـت ایجـاد جنبش‌های اجتماعی جهان مورداستفاده قرارگرفته‌اند (رسولی، غفوریان: ۱۰-۲۶) بـه‌عبـارتی‌دیگـر ماهیت شبکه‌های اجتماعی، پتانسیل ایجاد اطلاعات غلط به‌طور گسترده را دارا می‌باشد. امری کـه برای بسیاری از کشورها نگران‌کننده است. همچنین چالش دیگر، مشکلات اخلاقی، تعدی نسـبت

۱. این گزارشگر در سال ۱۹۹۳ توسط کمیسیون حقوق بشر منصوب گردید.

به حریم خصوصی و نیز نقض‌های امنیتی و خلاف نظم عمومی می‌باشد (Rosine, 2019: 54) تجربه استفاده از شبکه‌های اجتماعی نشان داده است که رسانه‌های اجتماعی در برخی مواقع نقش بسیار زیادی در ایجاد بحران داشته‌اند و در برخی مواقع در سراسر جهان به شروع اعتراض‌ها و حتی انقلاب‌ها کمک کرده‌اند. در اعتراضات ایران در سال‌های ۹۶ و ۹۸ و ۱۴۰۱ و همچنین در قیام‌های مصر تا ترکیه شبکه‌های اجتماعی به‌عنوان ابزار سازمان‌دهی فوق‌العاده مخالفان موجب گردیدند که این اعتراضات شکل گرفته و چشم‌انداز ملی و بین‌المللی این کشورها را با سرعت و به شکل بی‌سابقه‌ای تغییر دهند. به‌عنوان‌مثال در سال ۱۳۹۸ رسانه‌های اجتماعی نقش بسیار پررنگی در هدایت اعتراضات داخل ایران داشتند. حتی وزیر دفاع سابق آمریکا در ژوئن سال ۲۰۰۹ اظهار می‌نماید :«فنّاوری رسانه‌های اجتماعی مانند توییتر نقش حیاتی در آشوب‌های ایران داشته و یک دارایی استراتژیک برای آمریکا محسوب می‌شوند» (امین‌الرعایا و همکاران ، ۱۴۰۰: ۱۱۹) موسسه رند نیز در گزارشی با عنوان «قدرت اجبار»، شبکه‌های اجتماعی و رسانه‌های جهانی را از ابزارهای مهم در جهت تحرکات داخلی و حامیان خارجی آن‌ها قلمداد کرده که درنهایت می‌توانند کشور هدف را به تسلیم و تأمین منافع آمریکا وادار کنند.(همان) همچنین جامعه بین‌الملل خوب به یاد دارد که افشای گسترده داده‌های شخصی نظیر انتشار داده‌های هویتی تقریباً ۵۰ میلیون تبعه‌ی ترکیه، یا حدود دوسوم از جمعیت ترکیه، در شبکه‌های اجتماعی در آوریل ۲۰۱۶، یک بحران ملی را در آن کشور ایجاد کرد. (Al Jazeera ,2016) این موارد باعث شده است که اکثر کشورها به دنبال راه چاره‌ای در این خصوص باشند.برای نمونه امانوئل ماکرون، رئیس‌جمهور فرانسه، در سخنرانی در جلسه عمومی افتتاحیه مجمع حاکمیت اینترنت در سال ۲۰۱۸، نیاز به «راه سوم» در حکمرانی اینترنت، بین آزادی‌خواهی درک شده در دره سیلیکون و دولت‌گرایی اقتدارگرایانه اینترنت چین را مطرح کرد و استدلال کرد که مقررات پلتفرم برای بازگرداندن مسئولیت‌پذیری و اعتماد، پیش‌شرطی برای حفظ ارزش‌های آزادی و دموکراسی مرتبط با دیدگاه اولیه اینترنت باز است.(Flow & Martin, 2022: 2) جدای از موضوعات مطروحه، شبکه‌های اجتماعی در برخی موارد موجب افزایش خشونت علیه افراد و گروه‌های خاص گردیده است. به‌عنوان‌مثال فیس بوک موجب گسترش نفرت و تحریک خشونت علیه مسلمانان روهینگیا در میانمار گردید (Stecklow ,2018) همچنین شبکه‌های اجتماعی موجب اختلاف بین بودائیان و

مسلمانان در سریلانکا شده است (Taub,and Fisher ,2018) در خصوص نقش شبکه‌های اجتماعی در جذب نیرو برای گروه‌های مسلح، شایان‌ذکر است بسیاری از گروه‌های تروریستی از رسانه‌های اجتماعی برای استخدام نیرو استفاده می‌کنند که می‌توان به ملحق شدن زنان و حتی کودکان در بخش‌های مختلف جهان به داعش در عراق و سوریه با استفاده از تبلیغات داعش و پیام‌های عضوگیری در فضای سایبر اشاره کرد. تا جائیکه مثلاً در سال ۲۰۱۳ تلگرام به ابزاری کاربردی برای گروه تروریستی داعش تبدیل شد؛ زیرا از تلگرام علاوه بر عضوگیری، افزایش بودجه و برای بر عهده گرفتن مسئولیت پس از انجام حمله‌ی تروریستی استفاده می‌کردند. (Segall ,2015).علاوه بر این، در ۱۵ آگوست ۲۰۱۷ ، دیوان کیفری بین‌المللی[1] حکم دستگیری محمود مصطفی بوسیف الورفال[2] را به جرم ارتکاب جنایت جنگی در لیبی صادر نمود و بسیاری از اطلاعاتی که مرجع تحقیقات دیوان بین‌المللی کیفری به آن استناد نمود، مطالبی بود که توسط مرکز رسانه‌ای تیپ الصاقیه[3] که بوسیف الورفال در آن کار می‌کرد در شبکه‌های اجتماعی منتشرشده بود (Prosecutor v. Mahmoud Mustafa Busayf Al-Werfalli, 2017) در خصوص نقش رسانه‌های اجتماعی در زمینه نقض امنیت ملی دولت‌ها به‌عنوان نمونه در ژانویه سال ۲۰۱۵ نخست‌وزیر سابق انگلستان خواهان جرم انگاری سرویس‌های پیام‌رسان آنلاین شد. ازاین‌جهت که انگلستان برای حفاظت از امنیت ملی، حتی با مجوز دادگاه یا احضاریه، به آن‌ها دسترسی ندارد. در گزارش کمیته‌ی اطلاعات و امنیت مجلس این کشور، در این خصوص این‌چنین بیان‌شده است : «ما به این مسئله به شکلی گسترده‌تر نگاه کردیم و فهمیدیم که هیچ‌کدام از ارائه‌دهندگان سرویس‌های ارتباطاتی[4] آمریکا خود را ملزم به تبعیت از مجوزهای کشور انگلستان که تحت مقررات قانون اختیارات رسیدگی مصوب سال ۲۰۰۰ است، نمی‌دانند. درنتیجه، حتی اگر سازمان اطلاعات داخلی دلایلی برای رفتن به دنبال اطلاعات تحت مجوز داشته باشد، شرکت مدنظر ممکن است پاسخگو نباشد (ما متوجه شدیم که ارائه‌دهندگان سرویس‌های ارتباطاتی خارجی می‌توانند اطلاعات را درزمانی که تهدیدی فوری علیه جان فرد مطرح باشد فراهم آورند، اما این به نهادها در زمان تلاش برای محرز کردن تهدید از سوی یک فرد کمکی نمی‌کنند).....»

1. International Criminal Court (ICC)
2. Mahmoud Mustafa Busayf Al-Werfalli
3. Al-Saiqa Brigade's
4. Communications Service Providers (CSPs)

(Report on the intelligence relating to the murder of Fusilier Lee Rigby ,2014).

توجه به احتمال نقض امنیت ملی از سوی پلتفرم‌ها در سال ۲۰۲۰ از سوی رئیس‌جمهور وقت ایالات‌متحده نیز مورد تاکید قرار گرفت بطوریکه دونالد ترامپ در سخنرانی خود از تهدید گسترش برنامه‌های تلفن همراه در ایالات‌متحده که توسط شرکت چینی تیک تاک ارایه می‌گردد و تاثیر آن بر امنیت ملی، سیاست خارجی و اقتصاد ایالات‌متحده صحبت کرد. رییس جمهور وقت آمریکا تاکید نمود که تیک‌تاک که اکنون بیش از ۱۷۵ میلیون کاربر در ایالات‌متحده دارد به دلیل جمع آوری بخش‌های وسیعی از اطلاعات کاربران خود می‌تواند آسیب‌های امنیتی، ایمنی و اجتماعی شدیدی موجب گردد بنابراین، دونالد ترامپ رئیس‌جمهور وقت ایالات‌متحده تعاملات تجاری میان اشخاص با شرکت تیک‌تاک را بر اساس قانون اختیارات اضطراری اقتصادی بین‌المللی[1] ممنوع کرد.[2](Exec. 2020)

مکانیسم جامعه بین‌الملل جهت نظارت بر شبکه‌های اجتماعی: ایجاد تعهد از طریق قانون‌گذاری

در ابتدای این مبحث ذکر این نکته لازم است که به‌موجب معاهدات متعدد بین‌المللی حق دسترسی به اینترنت به‌موجب قواعد حقوق بین‌الملل به‌عنوان یکی از حق‌های بشری و تحت عنوان «آزادی بیان» مطرح‌شده است و هرگونه خلل در آن به‌گونه‌ای نقض این حق به شمار می‌رود. بااین‌وجود آزادی مطلق بیان نه تنها در هیچ سند بین‌المللی‌ای بلکه در هیچ کشوری موردقبول نمی‌باشد.[3] از طرفی نظر به اینکه اینترنت به‌خصوص در آمریکا که نقش بسیار مهمی در توسعه اینترنت و شبکه‌های اجتماعی داشته توسط بخش خصوصی ایجادشده و دولت آمریکا بخش خصوصی را تا حدودی خودگردان باقی گذاشته است با این باور که این رویکرد «بدون مداخله»

1. International Emergency Economic Power Act (IEEPA)

۲. در خصوص ممنوعیت دسترسی شهروندان آمریکا به پلتفرم تیک تاک، اتحادیه آزادی‌های مدنی آمریکا معتقد است که مسدودسازی دسترسی شهروندان به نرم‌افزار تیک‌تاک به‌نوبه خود نوعی نقض آزادی بیان می‌باشد . به اعتقاد ایشان دولت آمریکا زمانی می‌تواند دسترسی به تیک تاک را مسدود نماید که خطر جدی و قریب‌الوقوعی برای امنیت ملی داشته باشد درصورتی‌که هیچ مدرکی برای این وجود ندارد و همچنین تنها راه مقابله با خطرات این برنامه مسدودسازی آن نیست. (Leventoff,2023)

۳. در خصوص شرایط اعمال محدودیت بر حق آزادی بیان و حق دولتها در این خصوص رجوع شود به امین الرعایا و همکاران ، ۱۴۰۰ : ۹۷-۱۲۵

سبب ارتقاء نوآوری فناورانه و نه تضعیف آن می‌شود. (امین الرعایا ، ۱۴۰۰ : ۵۱۰) بدین دلیل عده‌ای نظارت بر فضای سایبری را، از طریق یک سازمان بین‌المللی متشکل از کشورهای عضو شامل اتحادیه مخابرات بین‌المللی یا سازمان ملل گزینه‌ای امکان‌پذیر و موفقیت‌آمیز نمی‌دانند (IT Countrey Justice, 2014) ولی بااین‌حال بسیاری از کشورها با مشارکت در طرح‌های بین‌المللی خواهان ایجاد سازمانی بین‌المللی برای تأسیس سازوکار قانونی بر این رسانه‌ها می‌باشند. نمونه این مشارکت‌ها را می‌توان در کنوانسیون «مقابله با استفاده از فناوری اطلاعات و ارتباطات برای اهداف مجرمانه» که هم‌اکنون در حال اجراست، مشاهده کرده ولی به نظر می‌رسد کشورهای صاحب این فناوری اجازه چنین سازوکارهایی در عرصه بین‌المللی را نخواهند داد. لذا به دلیل این خلأ در حقوق بین‌الملل، کشورها روش‌های متفاوتی را در جهت کنترل بر اینترنت و شبکه‌های اجتماعی اتخاذ نموده‌اند. از میان روش‌های مختلف نظارت بر اینترنت، شدید ترین آن‌ها شامل قطع دسترسی به اینترنت[1] است. در موارد دیگر برخی از دولت‌ها از کنترل خود بر ساختار اینترنت محلی از طریق کاهش عمدی سرعت اتصال، به‌ویژه در دفاتر روزنامه، هتل‌ها و خانه‌ها استفاده کرده‌اند. تعدادی دیگر از کشورها سعی کرده‌اند از طریق ارسال‌های سازمان‌یافته، بحث‌های آنلاین را دست‌کاری کنند. همچنین مکانیسم فیلتر نمودن اینترنت و شبکه‌های اجتماعی و نیز سانسور همراه با فشار جهت نظارت بر اینترنت از دیگر راهکارهای این حوزه می‌باشد. لکن به نظر می‌رسد بهترین مکانیسم جهت نظارت بر شبکه‌های اجتماعی متعهد نمودن پلتفرم‌های شبکه‌های اجتماعی از طریق وضع قانون می‌باشد.[2] شایان ذکر است در مورد حق دولتها جهت نظار بر شبکه‌هلی اجتماعی گزارشگر ویژه سازمان امنیت و همکاری اروپا درزمینهٔ آزادی بیان بر قانونی بودن نظارت بر ارائه‌دهنده سرویس‌های اینترنتی تأکید نمود (Joint Declaration of the Three Special Rapporteurs for Freedom of Expression ,2011). در این خصوص

---

۱. مانند قطع دسترسی مردم کره شمالی به اینترنت.

۲. یکی از رویکردها در این زمینه را می توان در آیین نامه رفتار داوطلبانه کمیسیون اروپا در سال ۲۰۱۶ در مورد مقابله با سخنان غیرقانونی نفرت پراکنی آنلاین مشاهده کرد که اکنون در پنجمین سال خود قرار دارد (کمیسیون اروپا، ۲۰۲۱)، که برای جلوگیری از سوء استفاده از مهاجران در طول سال ۲۰۱۵ معرفی شد. در این طرح نظارت بر محتوا، همه پلتفرم‌های اصلی با سازمان‌های غیردولتی در سراسر اروپا همکاری می‌کنند تا بر اساس گزارش‌هایشان با سخنان مشوق عداوت و تنفر مقابله کنند، و کمیته ای ارزیابی می‌کند که پلت‌فرم‌ها تا چه اندازه به تعهدات خود عمل می‌کنند.(Flow & Martin, 2022: 17)

دولت‌ها دو مکانیسم را برای نظارت بر شبکه‌های اجتماعی مورداستفاده قرار می‌دهند : یک. تصویب قوانین برای محتوای شبکه‌ها که در این مکانیسم کشورها محتوای غیرقانونی را در زمینه‌های داخلی و منطقه‌ای مشخص می‌کنند. دو. تعیین قوانین برای پلتفرم‌های شبکه‌های اجتماعی جهت مسئولیت‌پذیر نمودن محتوای غیرقانونی تولیدشده توسط کاربران (Sander,2021: 166) برای نمونه امروزه استفاده از برنامه تیک‌تاک[1] در کشورهای اروپا، کانادا و آمریکا ممنوع اعلام‌شده است (The New York Times,2023) و دولت‌ها دسترسی مردم به این شبکه پیام‌رسان را محدود کرده‌اند. اگر صرفاً به قواعد عام و کلی رجوع شود، این‌گونه محدودیت‌ها بایستی به‌عنوان نقض صریح حقوق بشر و آزادی بیان افراد تلقی شود ولی در واقعیت دولت‌ها با قانون‌گذاری در این حوزه سعی می‌کنند حاکمیتشان بر فضای مجازی را نشان‌دهند بااینکه در بسیاری از حالات این مقررات گذاری به‌عنوان نقض صریح آزادی بیان شناخته می‌شود.

نوع نظارت بر شبکه‌های اجتماعی : نظارت پیشگیرانه

تعهد دولت‌ها به نظارت بر شبکه‌های اجتماعی مبتنی بر نظارت پیشگیرانه[2] می‌باشد که این نوع نظارت بر اعمال استانداردهای سخت‌گیرانه بر مدیریت شبکه‌های اجتماعی مبتنی می‌باشد. (Kleinzschmidt ,2010:346) این نظارت که به‌عنوان دکترین نظارت سخت‌گیرانه[3] نیز مطرح می‌گردد، مسئولیتی را بر شبکه‌های اجتماعی ایجاد می‌نماید، حتی اگر آن‌ها هیچ‌گونه آگاهی از محتوای مطالب غیرقانونی موجود در بستر پلتفرم خود نداشته باشند .(Bird , Smythe, 2012: 19-22) به‌عبارت‌دیگر، به‌موجب این دکترین صاحبان پلتفرم‌ها مسئول اقدامات صورت گرفته در شبکه اجتماعی خود می‌باشند بدون توجه به هرگونه سهل‌انگاری یا تقصیری که از طرف آن‌ها به‌طور مرسوم استفاده می‌شود. این مدل از اجرای قانون در شبکه‌های اجتماعی انگیزه‌های قوی برای صاحبان پلتفرم‌های شبکه‌های اجتماعی جهت مسدود کردن همه محتوای بالقوه غیرقانونی به‌منظور

---

۱. تیک‌تاک یک پلتفرم رسانه اجتماعی ویدیوهای کوتاه است که برای ارائه آن‌ها به کاربران بر اساس علایق آن‌ها، به هوش مصنوعی متکی است. این پلتفرم چینی در سال ۲۰۲۲ حدود ۹/۴ میلیارد دلار درآمد ایجاد کرد. همچنین در سال ۲۰۲۲، ۱/۴ میلیارد کاربر فعال ماهانه داشت و انتظار می‌رود تا پایان سال ۲۰۲۳ به ۱/۸ میلیارد کاربر برسد. تیک‌تاک در همه مناطق دنیا به‌عنوان برنامه‌ای پرکاربر شناخته می‌شود بطوریکه این پلتفرم در امریکا بیش از ۱۸۳ میلیون، در اروپا ۲۵۷ میلیون، در امریکای لاتین ۲۸۵ میلیون کاربر فعال دارد. جهت مطالعه بیشتر رجوع شود به (Iqbal, 2023).

2. Proactive monitoring.
3. Legal doctrine of strict liability.

اجتناب از هرگونه مسئولیت ایجاد می‌کند ولی در عوض آزادی عمل و تجارت آن‌ها را دستخوش تغییرات گسترده‌ای قرار می‌دهد و انگیزه سرمایه‌گذاران در این حوزه را به‌شدت کاهش می‌دهد. بر همین اساس رویه آمریکا و کشورهای اروپایی به نسبت بر آزادی عمل پلتفرم‌ها و عدم مسئولیت این نوع پلتفرم‌هاست ولی در عوض در کشورهای جهان سوم، رویه بر مسئولیت داشتن این‌گونه از پلتفرم‌ها اشاره دارد. برای نمونه در ایران و در سال ۱۴۰۰ مدیرعامل پلتفرم دیوار به جرم «فراهم آوردن موجبات فساد و فحشاء از طریق جذب زنان تن‌فروش» محکوم شد.(دیوار بلاگ، ۱۴۰۰)

خودکنترلی شبکه‌های اجتماعی

آنچه مسلم است شرکت‌های مالک پلتفرم‌های اجتماعی همچون توییتر، فیس بوک و اینستاگرام برای انجام کنترل نسبت به مقامات دولت‌ها در موقعیت بهتری قرار دارند چراکه این کنترل کم‌هزینه‌تر و همچنین برخلاف دولت‌ها، شبکه‌های اجتماعی در همه بازارهایی که در آن فعال هستند، قادر به تعیین قوانینی متناسب با جریان داده‌هایی که در حال انتقال می‌باشد و همچنین سرعت رشد فناوری‌ای که هرروز در حال تغییر است، هستند. علاوه براین، آن‌ها می‌توانند از فنّاوری‌های مؤثرتری[1] استفاده کنند (George, Scerri, 2007: 10) بااین‌حال آیا پلتفرم‌ها می‌توانند برخلاف میل کاربران خود، قواعدی را ایجاد نمایند؟به‌عبارتی‌دیگر ابراز تنفر، انزجار، تبلیغ، خشونت یا صحبت کردن برای موردی دلخواه که گاه با حریم شخصی و تجاری افراد و شرکت‌های دیگر در تضاد است و بسیاری از موضوعات دیگر، به درخواست و علایق کاربران مرتبط است و کاربر برای اشاعه آن‌ها شبکه اجتماعی خاص را انتخاب می‌کند. حال پلتفرم می‌بایست میان سودی که از طریق جذب کاربران و فعالیت‌ها آن‌ها کسب می‌کند و الزامات حاکمیتی رابطه‌ای برقرار کند والا خود در تنگنا قرار می‌گیرد. در این رابطه یکی از محققین در این حوزه استدلال می‌کند که اتکا به خودتنظیمی شرکت و مسئولیت اجتماعی در مواجهه با مدل‌های کسب‌وکار که شیوه‌های انحصاری و اخلاقی مشکوکی را ترویج می‌کنند همیشه ناکافی است و می‌بایست دولت‌ها قواعدی را وضع نمایند. از طرفی برخی دیگر از پژوهشگران این حوزه با بررسی دقیق مفهوم مسئولیت اجتماعی شرکتی[2] استدلال می‌کنند که این مسئولیت تنها در

1. Effective.
2. Corporate social responsibility (CSR).

صورتی می‌تواند نقش معناداری داشته باشد که با مقررات دولتی همراه باشد. به بیانی دیگر دولت‌ها قواعدی را بر پلتفرم و نه کاربر تحمیل کنند. (Flow & Martin, 2022: 16) در مقابل، نیکلاس سوزور استدلال می‌کند که تصمیمات تعدیل محتوا در پلتفرم‌های دیجیتال همیشه به میزانی از اصلاح نیاز دارد و خودتنظیمی پلتفرم همیشه بخشی از ترکیب نظارتی خواهد بود و دولت‌ها نیز باید از ابزار نظارتی مناسبی برخوردار باشند. (Suzor,2019: 39) رویکرد آخر سبب می‌شود تا شرکت‌ها مدل های نظارتی متفاوتی را اتخاذ کنند که این رویکرد بخشی از مدل کسب‌وکار آنهاست و تابع قراردادی است که آنها به کاربران خود و سهام‌داران متعدد ارائه می‌دهند.

بخش ۲۳۰ قانون نجابت ارتباطات دولت کلینتون که در سال ۱۹۹۶ تصویب شد، یکی از معدود مواد از آن قانون است که از چالش دادگاه عالی جان سالم به در برده است، معمولاً سنگ بنای تمایز پلت فرم با ناشر است، با این ایده که «واسطه‌های اینترنتی (پلتفرم‌ها) برای مسدود کردن، حذف یا کاهش رتبه محتوا در سایت‌های خود مشمول وضعیت حقوقی ناشران نمی‌شوند و نمی‌توانند ازنظر قانونی در قبال محتوای ارسال‌شده توسط کاربران خود پاسخگو باشند. (Gillespie, 2017:262) این استدلال در اینترنت سبقه تاریخی دارد و به متن Ithiel de Sola Pool در سال ۱۹۸۳، باز می‌گردد که ابتدا این استدلال را متبلور کرد که اشکال جدید فناوری‌های ارتباط الکترونیکی به «سیاست آزادی» نیاز دارند (de Sola Pool, 1983) که آن‌ها را به‌وضوح از صنایع چاپی و پخش متمایز می‌کند. سوای از این موضوع، دولت آمریکا سیاست آزادی را در پیش‌گرفته است و تنظیم‌گری در این خصوص را به خود شرکت‌ها واگذار کرده است. بااین‌حال به نظر می‌رسد رویکرد آمریکا بیشتر منافع محور بوده است چراکه اغلب پلتفرم‌های بزرگ در این کشور قرار دارند و از طرفی قانون FISA[1] این اختیار را به آژانس‌های نظارتی آمریکا می‌دهد تا هر اطلاعاتی که این آژانس‌های نیاز دارند از افرادی غیر از تابعین این کشور در اختیار آن‌ها قرار دهد. به‌عبارتی‌دیگر ازاین‌جهت آمریکا مهم‌ترین حامی آزادی بیان است که تمامی پلتفرم‌های مهم در این حوزه را در اختیار دارد ولی در عوض آمریکا به دلیل ابزارهای نظارتی که برای تمامی مردمان جهان اتخاذ می‌کند؛ توسط گزارشگران بدون مرز در سال ۲۰۱۴ به‌عنوان یکی از دشمنان اینترنت نیز شناخته‌شده است. (Reporters Without Borders, 2014)

1. The Foreign Intelligence Surveillance Act (FIsa)

از طرفی رویکرد اتحادیه اروپا با تصویب قوانین جدیدی که در این حوزه اتخاذ کرده است مانند قانون خدمات دیجیتالی[1] و بازارهای دیجیتالی[2] مصوب دسامبر ۲۰۲۲ این نکته را می‌رساند که اتحادیه اروپا از رویکرد خودتنظیمی شرکت‌ها به‌علاوه نظارت خارجی بهره برده است. در ماده ۷ قانون خدمات دیجیتالی هیچ تعهد اضافی‌ای توسط کشورها بر پلتفرم‌ها نباید تحمیل شود. تصمیم برای حفظ این رژیم احتمالاً به دلیل خطر بالای پیامدهای منفی هم برای شرکت‌ها و هم برای حقوق اساسی کاربران بوده است. ولی در عوض در ماده ۸، پلتفرم‌ها متعهد می‌شوند تا «بعد از دریافت دستور اقدام علیه یک مورد خاص از محتوای غیرقانونی، صادرشده توسط مقامات قضایی ملی یا اداری مربوطه» «بدون تأخیر ناروا» اقدامات لازم را ترتیب دهند. این نشان می‌دهد که اگرچه خودتنظیمی پلتفرم‌ها و عدم مسئولیت آن‌ها در این اتحادیه به رسمیت شناخته می‌شود ولی نظارت خارجی بر آن‌ها نیز به‌عنوان یک اصل پذیرفته شده است.

بااین‌حال، واقعیت آن است که هرچند به ادله بیان‌شده مسئولیت صاحبان شبکه‌های اجتماعی است که بر محتوای این شبکه‌ها نظارت داشته باشند لکن این مسئولیت به معنای نادیده گرفتن وظایف نظارتی دولت‌ها نخواهد بود چرا که در جامعه بین‌الملل دولت‌ها ملزم به رعایت و محافظت از حقوق اساسی خود هستند (Kaesling, 2018:159-160).

کنوانسیون‌های بین‌المللی و حق دولت‌ها جهت نظارت بر شبکه‌های اجتماعی

در خصوص نظارت بر شبکه‌های اجتماعی بسیاری از کنوانسیون‌های حقوق بشری و غیر حقوق بشری بر حق دولت‌ها جهت نظارت بر شبکه‌های اجتماعی و سایت‌های اینترنتی تأکید می‌نمایند. بطوریکه کنوانسیون‌های حقوق بشری نقش دوگانه‌ای را برای دولت‌ها ایجاد می‌نمایند: از یک‌سو حکم عدم ممنوعیت اشکال خاصی از آزادی بیان و حق بر حریم خصوصی را صادر می‌کنند و از طرف دیگر انواع محدودیت‌هایی که می‌توانند توسط دولت‌ها اعمال شوند را بیان می‌کند. به‌عنوان‌مثال هرچند به‌موجب ماده ۱۷ کنوانسیون حقوق مدنی سیاسی[3] «هیچ‌کس نباید در زندگی خصوصی و خانواده و اقامتگاه یا مکاتبات مورد مداخلات خودسرانه (بدون مجوز) یا خلاف قانون قرار گیرد و همچنین شرافت و حیثیت او نباید مورد تعرض غیرقانونی واقع شود.» لکن از سوی دیگر ماده (۲) ۲۰ همان کنوانسیون همه دولت‌ها را متعهد نموده است که از «هرگونه

1. Digital Services Act(DSA)
2. Digital Market Act(DMA)
3. International Covenant on Civil and Political Rights (ICCPR)

دعوت (ترغیب) به کینه (تنفر) ملی یا نژادی یا مذهبی که محرک تبعیض یا مخاصمه یا اعمال زور باشد» ممانعت نمایند .همچنین کمیته‌ی حقوق بشر، در نظریه تفسیری شماره ۱۶ خود در خصوص ماده ۱۷ کنوانسیون بین‌المللی حقوق مدنی و سیاسی (General Comment no. 16,1988) با قبول غیر مطلق بودن این حق بر حق دولت‌ها بر مداخلات مجاز از طریق وضع قوانین و مقررات در خصوص منافعی که مربوط به منافع جامعه می‌باشد تأکید می‌نماید.[1] این حق دولت‌ها در دخالت در حریم خصوصی در ماده ۸ کنوانسیون اروپایی حقوق بشر ۱۹۵۰ نیز بیان‌شده است: «۱- هر کس از حق احترام به زندگی خصوصی و خانوادگی، خانه و مراسلات خود برخوردار است. ۲- در اجرای این حق هیچ مداخله‌ای نباید از سوی هیچ‌یک از مقامات دولتی صورت گیرد مگر مداخلات منطبق بر قانون و مواردی که در یک جامعه‌ی مردم‌سالار به دلایل حفظ امنیت ملی، ایمنی عمومی یا رفاه اقتصادی کشور، پیشگیری از هرج‌ومرج و جرائم، حفاظت از سلامتی و اخلاقیات یا حفاظت از حقوق سایرین ضروری تشخیص داده شوند.» ماده ۱۹ کنوانسیون حقوق مدنی و سیاسی عین همین حق برای دولت‌ها در خصوص حق آزادی بیان که دسترسی به اینترنت و شبکه‌های اجتماعی یکی از مصادیق آن می‌باشد را به رسمیت شناخته است : « ۲ .هر کس حق آزادی بیان دارد. .... بند ۳ اعمال حقوق مذکور دربند ۲ این ماده مستلزم حقوق و مسئولیت‌های خاص است و لذا ممکن است تابع محدودیت‌های معینی بشود که در قانون تصریح‌شده و برای امور ذیل ضرورت داشته باشد: الف. احترام حقوق باحیثیت دیگران. ب. حفظ امنیت ملی یا نظم عمومی یا سلامت یا اخلاق عمومی.» سوای از ماده ۱۹ کنوانسیون حقوق مدنی و سیاسی، ماده ۱۰ کنوانسیون اروپایی حقوق بشر در خصوص این دولت‌های عضو بیان می‌دارد: «هرکس از حق آزادی بیان برخوردار است. ... اعمال این آزادی‌ها، ... ممکن است نیازمند ... محدودیت‌ها یا مجازاتی باشند که ... به‌منظور حفظ منافع امنیت ملی، تمامیت ارضی یا ایمنی عمومی جهت ممانعت از ایجاد هرج ومرج یا ارتکاب جرائم، حفاظت از سلامتی و اخلاقیات مردم، حمایت از آبرو یا حقوق سایرین، جلوگیری از افشای اطلاعات محرمانه یا حفظ اقتدار و بی‌طرفی دستگاه قضاوت لازم و ضروری هستند.» همچنین کنوانسیونِ شورای اروپا در مورد جرائم سایبری، با پروتکل الحاقی

۱. نظریه تفسیری شماره ۱۶ کمیته‌ی حقوق بشر در خصوص ماده ۱۷ کنوانسیون حقوق مدنی و سیاسی «۷- همان‌قدر که زندگی افراد در جامعه ضرورت دارد، حمایت از حریم شخصی آن‌ها نیز به همان نسبت ضرورت می‌یابد. ... این کمیته توصیه می‌کند که کشورها باید در گزارش خود قوانین و مقررات حاکم بر مداخلات مجاز در زندگی شخصی را لحاظ نمایند. ماده ۸ تصمیم برای استفاده از این مداخلات مجاز باید تنها توسط نهاد منسوب شده تحت قانون و بر مبنای پرونده صورت گیرد»

خود، از دولت‌های عضو می‌خواهد که فعالیت‌های مختلف در فضای سایبری ازجمله «توزیع یا در دسترس قرار دادن مطالب نژادپرستانه و بیگانه هراسی برای عموم از طریق یک سیستم رایانه‌ای» را جرم انگاری کنند. (commissioner for human rights, 2012:13) دستورالعمل ۴۶/۹۵ اتحادیه‌ی اروپا[1] که درزمینه حمایت از داده‌های شخصی افراد و نیز انتقال آزادانه این داده‌ها می‌باشد، در ماده ۱۳ خود استثنائاتی را برای دولت‌های عضو در جهت وضع قانون در راستای محدود نمودن این حق به رسمیت می‌شناسد که عبارت است از: الف) امنیت ملی ب) دفاع ج) امنیت عمومی د) پیشگیری، تحقیق، کشف و تعقیب مجرمان جرائم، یا نقض اصول اخلاقی ه) منافع اقتصادی یا مالی مهم یک کشور عضو یا اتحادیه اروپا، ز) حمایت از داده‌های افراد و یا حمایت از حقوق و آزادی‌های دیگران (Directive 95/46/EC,1995: Article 13) کنوانسیون ۱۰۸ که به‌عنوان اولین سند بین‌المللی الزام‌آور در بین کشورهای اروپایی درزمینه محافظت از افراد در برابر سوءاستفاده‌هایی که ممکن است همراه با جمع‌آوری و پردازش داده‌های شخصی صورت گیرد، محسوب می‌گردد در ماده ۹ استثنائاتی را برای این تکلیف دولت‌های عضو قائل شده است:« ... عدول از مفاد مواد ...این کنوانسیون زمانی مجاز خواهد بود که چنین عدولی توسط قانون دولت‌ها پیش‌بینی‌شده باشد در جهت :الف) حفاظت از امنیت ملی، امنیت عمومی، منافع پولی یک دولت، یا برخورد با جرائم جنایی؛ ب) حفاظت از داده‌ها، سوژه‌ها و حقوق و آزادی‌ها دیگران (European Treaty Series - No. 108, 1981: Article 9). گذشته از کنوانسیون‌های حقوق بشری، با دقت در دیگر کنوانسیون‌های بین‌المللی در زمینه ارائه خدمات اینترنتی این موضوع محرز می‌گردد که این کنوانسیون‌ها به دولت‌ها در زمینه وضع قانون و برقراری نظم و حفاظت از جامعه‌ی خود در برابر خطر، منافع مشروعی را اعطا می‌نماید. یکی از این کنوانسیون‌ها اتحادیه بین‌المللی مخابرات[2] می‌باشد که به نظر می‌رسد مواد اساسنامه این اتحادیه بین‌المللی، اختیار گسترده و وسیعی به کشورهای عضو[3]، هم در سطح بین‌الملل و هم در سطح داخلی در زمینه حفظ قانون و نظم و حفاظت از جامعه‌ی خود اعطا کرده است[4] به‌عنوان‌مثال این کنوانسیون تصریح می‌نماید: «اعضاء اتحادیه این

1. European Union
2. International Telecommunication Union (ITU)

۳. عضویت ایران در این نهاد بین‌المللی در تاریخ ۹ تیرماه ۱۳۶۸ هجری شمسی و تصویب آن در مجلس شورای اسلامی صورت پذیرفت.

۴. اتحادیه بین‌المللی مخابرات یک آژانس تخصصی سازمان ملل متحد است که مسئولیت کلیه امور مربوط به فناوری اطلاعات و ارتباطات را بر عهده دارد. این اتحادیه در ۱۷ می ۱۸۶۵ به عنوان اتحادیه بین‌المللی تلگراف تأسیس شد. لکن با ظهور فن‌آوری‌های ارتباطی جدید، درحال حاضر این نهاد در زمینه پهنه اینترنت، فناوری‌های بی‌سیم و شبکه‌های نسل بعدی نیز فعال است. جهت مطالعه بیشتر ر.ک.: (جباری،۱۳۹۳ : ۱۴۱-۱۷۲)

حق را دارند که از ارسال هرگونه تلگرام خصوصی که ممکن است برای امنیت کشورشان خطرناک باشد و یا مخالف قوانین و نظم عمومی آن کشور باشد جلوگیری کنند ...» (ماده ۲۳ قانون راجع به تصویب اساسنامه و اصلاح مقاوله نامه (کنوانسیون) اتحادیه بین‌المللی مخابرات) همچنین این کنوانسیون تصریح می‌نماید: «کشورهای عضو توافق کردند تا در جهت تضمین محرمانگی مکاتبات بین‌المللی، تمام راه‌کارهایی که مطابق با سیستم مخابراتی مورداستفاده‌شان است را بکار گیرند.» تا جائیکه این کنوانسیون تصریح می‌نماید که دولت‌ها این حق را خواهند داشت که این نوع ارتباطات را به‌منظور اطمینان از انطباق آن‌ها با قوانین داخلی خود و اجرای قراردادهای بین‌المللی که در آن سهیم هستند با مقامات صالحه در میان بگذارند (ماده ۲۶، همان) بنابراین به‌موجب این کنوانسیون‌ها دولت‌ها در جهت حفظ امنیت ملی، اخلاق عمومی، سلامت عمومی می‌توانند قوانینی را برای شبکه‌های اجتماعی در جهت متعهد نمودن آن‌ها وضع نمایند و ارائه‌کنندگان خدمات اینترنتی باید از قانون کشوری که در آن فعالیت می‌کنند، تبعیت نمایند چراکه در غیر این صورت دولت میزبان می‌تواند نسبت به تعلیق و یا قطع اینترنت اقدام نماید هرچند الزام به رعایت قواعد حقوق بشری در زمینه فضای مجازی نیز از موضوعاتی است که دولت‌ها می‌بایست نسبت به آن اهتمام داشته باشند.

رویه قضایی بین‌المللی و نظارت بر شبکه‌های اجتماعی

با نگاهی به رویه قضایی بین‌المللی می‌توان استدلال نمود که این محاکم در رویهٔ خود اعمال نظارت از سوی دولت‌ها بر شبکه‌های اجتماعی را پذیرفته‌اند. به‌عنوان نمونه مرجع تجدید نظر[1] دیوان اروپایی حقوق بشر[2] در قضیه دلفی علیه استونی، به این نتیجه رسید که کشورها می‌توانند بر شبکه‌های خبری به دلیل عدم انجام اقدامات لازم برای حذف نظرات «به‌وضوح غیرقانونی»[3] که موجب تکثیر سخنان نفرت‌انگیز و تهدیدهای مستقیم برای تمامیت جسمانی افراد می‌گردد، ایجاد مسئولیت نمایند. (Delfi AS v. Estonia, 2015:para. 159) همچنین در پرونده MTE علیه مجارستان مجدداً دیوان بر مسئولیت نظارت بر شبکه‌های اجتماعی جهت حذف نظرات به‌وضوح غیرقانونیِ کاربران خود تأکید نمود. (Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt(MTE) v. Hungary,2016:para 91) این رویکرد مشابه توسط دیوان عالی آرژانتین در پرونده بلن

1. Grand Chamber
2. European Court of Human Rights (ECtHR)
3. clearly unlawful

رودریگز مورد تائید قرار گرفت. (Rodriguez M. Belén c/Google Inc,2014:para 18) به‌طوری‌که دیوان عالی کشور آرژانتین معتقد بود که موتورهای جستجو و شبکه‌های اجتماعی در صورت آگاهی واقعی از محتوای غیرقانونی و عدم انجام اقدامات اصلاحی مسئولیت دارند و می‌بایست بر آن‌ها نظارت نمایند. البته ذکر این نکته لازم است که دیوان اروپایی حقوق بشر نه‌تنها بر مشروع بودن نظارت بر شبکه‌های اجتماعی در آراء خود تأکید نموده، بلکه در آراء متعددی تصریح می‌نماید که دولت‌ها در نظارت دارای حاشیه مجاز تفسیر[1] می‌باشند.[2] در قضیه Big Brother Watch & Others دیوان اروپایی تأکید نمود که کشورها جهت اعمال نظارت دارای حاشیه مجاز تفسیر گسترده[3] می‌باشند (Christakis, Bouslimani ,2020:8) طبق رویه دیوان اروپایی حقوق بشر، اعطا این حاشیه مجاز تفسیر نه‌تنها به‌عنوان تهدید قلمداد نمی‌گردد، بلکه برای دستیابی به یک هدف مشروع است که همانا مبارزه با تروریسم جهانی می‌باشد. ازاین‌رو چنین مکانیسم‌هایی به‌عنوان یک اقدام «ارزشمند» تلقی می‌شوند (Big Brother Watch and Others v. United Kingdom, 2018:paras176.211.384-385) البته با نگاهی به رویه دیوان اروپایی حقوق بشر[4] و نیز دیوان دادگستری اتحادیه اروپا[5] محرز می‌گردد که این دو نهاد قضائی به بررسی موضوع «ضرورت» نظارت دولت‌ها به شبکه‌های اجتماعی می‌پردازند. بدین معنا که بررسی می‌نمایند که آیا چنین شیوه‌های نظارتی بر شبکه‌های اجتماعی «بسیار ضروری»[6] و دارای «هدف مشروع»[7] می‌باشد یا خیر. (Sander, 2021:185).[8]

---

1. Margin of Appreciation

۲. دکترین حاشیه مجاز تفسیر با اعطاء آزادی عمل و اختیار به دولت‌های عضو کنوانسیون اروپایی حقوق بشر از یک طرف اطمینانی در جهت حمایت از حاکمیت و منافع ملی آنها ایجاد می‌نماید و از طرفی دیگر این موضوع را اثبات می‌نماید که پایبندی به معاهدات بین‌المللی در عین احترام به منافع ملی دولت‌ها امکان‌پذیر می‌باشد. لذا حاشیه مجاز تفسیر همراه با اصول حاکم بر آن عملی «تفسیری» محسوب می‌گردد که به دولت‌های عضو کنوانسیون اروپایی جهت تفسیر مواد کنوانسیون اروپائی حقوق بشر در مواقع اضطراری که حاکمیت ملی این کشورها به خطر می‌افتد اعطا می‌گردد جهت مطالعه بیشتر رجوع کنید به (احمدی نژاد، امین الرعایا، ۱۳۹۵:۱۱۶ -۱۳۹)

3. Wider Margin of Appreciation.
4. European Court of Human Rights (Ecthr).
5. Court of Justice of The European Union (CJEU).
6. Strictly Necessary
7. Legitimate Purpose

۸. جدای از محاکم بین‌المللی شورای حقوق بشر نیز سازمان ملل به این نتیجه رسیده است که کشورها در خصوص افرادی که ارتباطات آنها تحت نظارت مستقیم است باید تدابیری اتخاذ کنند تا با کمک سه آزمون «قانونی بودن»، «مشروعیت» و «ضرورت» اطمینان حاصل شود که بدون توجه به ملیت یا مکان از هرگونه تداخل به حق حفظ حریم خصوصی جلوگیری شود.
(Concluding Observations on the Fourth Periodic Report of the United States of America, 2014: para. 22.)

رویه عملی دولت‌ها و نظارت بر شبکه‌های اجتماعی

با دقت درمجموع قانون‌گذاری‌های صورت گرفته از ناحیه کشورها مشخص می‌گردد که دولت‌ها رویه‌های متفاوتی را جهت متعهد نمودن شبکه‌های اجتماعی در خصوص مطالب منتشرشده از ناحیه کاربران از طریق قانون‌گذاری اعمال می‌نمایند.

مسئول نمودن شبکه‌های اجتماعی

واقعیت آن است که دولت‌ها نسبت به حفظ داده‌های شخصی کاربران اینترنت خود و عدم تعارض محتوای شبکه‌های اجتماعی با قوانین جاری خود بسیار حساس هستند. بنابراین در رویه عملی دولت‌ها تعیین نحوه نظارت بر شبکه‌های اجتماعی نه فقط از طریق قانون‌گذاری، بلکه از طریق شبکه گسترده‌ای از فاکتورهای دیگر صورت می‌پذیرد. به‌طوری‌که زمینه‌هایی فراهم می‌گردد که از طریق آن صاحبان پلتفرم‌های اجتماعی متعهد می‌شوند نسبت به حذف محتواهای غیرقانونی اقدام نمایند (Sander, 2021:175). به‌عنوان‌مثال در اتحادیه اروپا وظایف پلتفرم‌های شبکه‌های اجتماعی در برخورد با اعمال غیرقانونی در قانون تجارت الکترونیک مصوب سال ۲۰۰۰ بیان‌شده است.[1] در این قانون تکالیفی بر ارائه‌دهندگان خدمات اینترنتی بالأخص ارائه‌دهندگان شبکه‌های اجتماعی تصویب و اعمال می‌گردد. به‌عنوان نمونه بر اساس بند ۴۶ ماده ۱۴ این قانون، ارائه‌دهندگان خدمات اینترنتی می‌بایست در صورت بروز اعمال غیرقانونی دسترسی به اطلاعات را غیرممکن و یا محدود نماید. (Directive of the European Parliament and of the Council,2000: Artice 14(46)). این موضوع در ماده ۸ دستورالعمل ۴۶/۹۵ که برگرفته از ماده‌ی ۶ کنوانسیون ۱۰۸ شورای اروپا درزمینهٔ حفاظت از دستهٔ خاصی از داده‌ها یا داده‌های حساس می‌باشد نیز قیدشده است. این ماده شبکه‌های اجتماعی را متعهد می‌نماید که از انتشار داده‌هایی که تفاوت‌های نژادی یا قومیتی، نظرات سیاسی، باورهای غلط مذهبی یا فلسفی، داده‌هایی مرتبط با سلامت یا داده‌هایی که حریم خصوصی را افشاء می‌کند، ممانعت به عمل آورند. (Directive 95/46/EC,1995: Article 8) . همچنین با توجه به انتشار اطلاعات جعلی در رسانه‌های اجتماعی در آستانه انتخابات ریاست جمهوری ۲۰۱۶ آمریکا، پارلمان اروپا و کمیسیون به‌ویژه نگران اخبار جعلی در آستانه انتخابات اتحادیه اروپا در سال ۲۰۱۹ گردیدند. بدین منظور در آوریل ۲۰۱۸، کمیسیون اروپا به پلتفرم‌های

1. E- Commerce Directive of 2000 (ECD)

آنلاین شبکه‌های اجتماعی مأموریت داد تا قانون عمل به اطلاعات نادرست[1] را تا جولای ۲۰۱۸ تصویب نمایند. این قانون، پلتفرم‌های شبکه‌های اجتماعی را متعهد نمود که نسبت به جلوگیری از اخبار جعلی اقدامات لازم را انجام دهند. (Kaesling, 2018: 155) البته در سال ۲۰۱۶ نیز کمیسیون اروپایی به‌منظور مبارزه با سخنان غیرقانونی نفرت‌انگیز آنلاین، قانون نحوه برخورد با سخنان نفرت‌انگیز غیرقانونی آنلاین را تصویب نمود. (code of Conduct on countering illegal hate speech online, 2016) این منشور اخلاقی موردقبول فیس‌بوک، مایکروسافت، توییتر، یوتیوب، گوگل، اینستاگرام و اسنپ‌چت قرار گرفت. (European Commission, Daily News , 2018) به‌موجب این قانون شبکه‌های اجتماعی متعهد به دسترسی به «اخطار معتبر»[2] در کمتر از بیست‌وچهار ساعت پس از اطلاع‌رسانی از سوی دولت‌ها در خصوص اخطار «لزوم دسترسی به چنین محتوایی را حذف یا غیرفعال کنید» می‌باشند. همچنین در مارس ۲۰۱۸، کمیسیون توصیه‌نامه دیگری را در خصوص اقدامات مؤثر برای مقابله محتوای غیرقانونی آنلاین منتشر کرد (Commission Recommendation :March 2018) این توصیه‌نامه همکاری شبکه‌های اجتماعی را در زمینه‌هایی فراتر از اطلاع‌رسانی و اعلان اخطار داوطلبانه، در برخورد با انتشار سخنان تنفرانگیز متعهد می‌نماید. (Ibid) جدای از مقررات مورداشاره «مقررات عمومی حفاظت از داده‌های اتحادیه اروپا»[3] ازلحاظ ساختاری، یک سیستم چندلایه است که مجموعه‌ای از اصول حفاظتی را بر کنترل تعهدات و مسئولیت‌های کنترل‌کننده و پردازشگر داده‌ها ایجاد می‌نماید. (Regulation (EU) of Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement: 2016) به‌عنوان نمونه، مرجع حفاظت از داده‌های فرانسه در سال ۲۰۱۹، گوگل را به دلیل کوتاهی در رعایت مقررات عمومی حفاظت از داده‌های اتحادیه اروپا ۵۰ میلیون یورو جریمه نمود. در گزارش این مرجع نظارتی تأکید شده است که شبکه‌های اجتماعی می‌بایست به الزامات «مقررات عمومی حفاظت از داده‌های اتحادیه اروپا » پایبند باشند (French Data Protection,2019). یا کمیسیون محافظت از داده‌ها در ایرلند[4] اینستاگرام را به خاطر مدیریت نامناسب

1. proposes an EU-wide Code of Practice, Brussels, 26 April 2018.
2. valid notifications.
3. EU's General Data Protection Regulation (GDPR),2016.
4. Data Protection Commissioner

اطلاعات نوجوانان ۴۰۵ میلیون یورو جریمه کرد. این پرونده حدود دو سال پیش آغازشده بود و بالاخره در شهریورماه سال ۱۴۰۱ نهایی شد. این احکام تنها بخشی از محکومیت‌های صادره برای این شرکت‌های بزرگ فناوری می‌باشد که در اتحادیه اروپا در حال فعالیت هستند. به جهت مسئول بودن شبکه‌های اجتماعی است که مدیرعامل تیک‌تاک در جلسه عمومی ۲۳ مارس ۲۰۲۳ در مقابل نمایندگان سنا تعهدات بسیار مهمی به مانند: حفاظت از داده‌های ایالات‌متحده در برابر دسترسی خارجی، ایمنی برای کاربران به‌ویژه نوجوانان، شفافیت تیک تاک و اجازه نظارت و.... ارایه نمود. (Hendrix,2023)

معرفی نمایندگی از سوی شبکه‌های اجتماعی

ابتدایی‌ترین و بدیهی‌ترین مکانیسم جهت مسئول نمودن شبکه‌های اجتماعی معرفی نمایندگی رسمی از سوی شبکه‌های اجتماعی جهت برقراری ارتباط با مقامات دولتی و جوابگو بودن به هنگام نقض تعهد می‌باشد. این موضوع در آلمان و به هنگام پیدا نمودن راهکاری جهت برخورد با سخنان نفرت‌انگیز و اخبار جعلی در شبکه‌های اجتماعی که در داخل کشور آلمان مستقر نبودند، مطرح گردید. بدین منظور قانون‌گذاران آلمان با تصویب قانون «بهبود اجرای حقوق شبکه‌های اجتماعی» شبکه‌های اجتماعی خارجی مستقر در آلمان را مکلف نمودند که نماینده‌ای را در این کشور معرفی نمایند تا بتوانند به درخواست‌های مقامات اجرای قانون پاسخ دهند (Act to Improve the Enforcement of Rights on Social Networks,2017:Article1(3)(6),5) همچنین بنابر ماده ۴ قانون نظارت بر شبکه‌های اجتماعی ترکیه ارائه‌دهندگان شبکه‌های اجتماعی خارجی با بیش از یک‌میلیون دسترسی روزانه از ترکیه موظف‌اند حداقل یک نفر را که اطلاعات تماس وی باید در وب‌سایت آن به‌گونه‌ای مشخص و قابل‌دسترس باشد، به‌عنوان نماینده در ترکیه برای پیگیری موارد ضروری تعیین کنند تا بدین‌وسیله تشریفات مربوط به اطلاعیه‌ها، یادداشت‌ها یا درخواست‌های هر مرجع قانونی یا اداری و نیز پاسخگویی به درخواست‌های ارائه‌شده به‌موجب این قانون و اطمینان از انجام سایر تعهدات در محدوده این قانون میسر گردد. همچنین به‌موجب این قانون ارائه‌دهنده شبکه اجتماعی مسئول به اشتراک گذاشتن اطلاعات هویتی و تماس این فرد با مقامات است. همچنین بر اساس این قانون اگر فرد تعیین‌شده یک شخص حقیقی باشد، باید

شهروند ترکیه باشد. ((Turkish Internet Law ,2020: Article4(1)) به‌موجب ماده ۴ قانون نظارت بر شبکه‌های اجتماعی ترکیه مقامات برای کسانی که به تعهدات خود در تعیین نماینده عمل نکنند، اطلاعیه‌ای ارسال می‌کند و مراتب را به‌طور مقتضی به مقامات اعلام می‌کند. درصورتی‌که ظرف ۳۰ روز پس از ابلاغ مربوطه به این تعهد خود عمل نکنند، رئیس‌جمهور حق دارد ده میلیون لیره ترکیه جریمه اداری برای ارائه‌دهنده شبکه اجتماعی صادر کند. درصورتی‌که ظرف ۳۰ روز پس از اجرای جریمه به تعهدات فوق عمل نشود، سی میلیون لیره ترکیه جریمه اداری اضافی به شرکت ارائه‌دهنده شبکه اجتماعی تعلق می‌گیرد و اگر ظرف سی روز پس از صدور جریمه دوم به این تعهد عمل نشود، اشخاص حقیقی و حقوقی، از درج آگهی‌های اضافی و انعقاد قراردادهای جدید یا انجام معاملات مالی با شبکه اجتماعی منع می‌شوند. مضافاً اینکه درصورتی‌که ظرف سه ماه پس از اجرای ممنوعیت ارائه‌دهنده موردنظر به تعهدات فوق عمل نکند، رئیس‌جمهور می‌تواند از دادگاه کیفری صلح درخواست نماید تا پنجاه‌درصد پهنای باند ترافیک اینترنت ارائه‌دهندهٔ شبکه اجتماعی را کاهش دهد. درصورتی‌که ظرف ۳۰ روز پس از اجرای رأی قاضی، تعهد موردنظر انجام نشود، رئیس‌جمهور از دادگاه کیفری صلح درخواست می‌کند تا پهنای باند ترافیک اینترنت ارائه‌دهنده شبکه اجتماعی را به میزان ۹۰ در هر واحد کاهش دهد. ((Turkish Internet Law ,2020: Article4(2)) . همچنین «قانون بهبود اجرای حقوق شبکه‌های اجتماعی»آلمان تأکید می‌نماید که اگر شبکه یک نماینده داخلی را تعیین نکند جریمه‌ای تا سقف ۵ میلیون یورو ممکن است در نظر گرفته شود (Act to Improve the Enforcement of Rights on Social Networks,2017:Article1-2). بدیهی است در صورت معرفی نماینده از سوی پلتفرم شبکه اجتماعی امکان شکایت از این شبکه نیز میسر می‌گردد. موضوعی که در پرونده مکس شرمز مورد تصریح قرار گرفت. در این پرونده، مکس شرمز شکایتی علیه «نمایندگی اروپایی فیس‌بوک در دوبلین» مطرح نمود که طی آن خواهان و ۲۵۰۰۰ کاربر دیگر فیس‌بوک از این شبکه اجتماعی به دلیل نقض حقوق خود ازجمله ردیابی غیرقانونی داده‌های آن‌ها بر اساس قوانین اتحادیه اروپا و نیز دخالت فیس‌بوک در برنامه نظارتی پریسم آژانس امنیت ملی ایالات‌متحده شکایت نمودند. لذا بدیهی است در این پرونده و موارد

مشابه در صورت عدم ایجاد نمایندگی، شکایت از پلتفرم و مسئول نمودن آن امری غیرممکن می‌گردد (Maximillian Schrems v. Data Protection Commissioner ,2014)

ایجاد مکانیسمی جهت شکایت از شبکه‌های اجتماعی و اعمال قانون بر آن‌ها

طبیعی است ایجاد مسئولیت تنها برای شبکه‌های اجتماعی بدون ایجاد مکانیسمی جهت شکایت از ایشان و اعمال مجازات نمی‌تواند شبکه‌های اجتماعی را متعهد به رعایت قوانین و مقررات دولت‌ها گرداند. بدین‌جهت ماده ۲۲ دستورالعمل ۹۵/۴۶ اروپا که در خصوص حراست از داده‌های خصوصی افراد می‌باشد، اشعار می‌دارد: «... کشورهای عضو بایستی برای هر شخصی، حقی در خصوص راه‌حل قضایی نسبت به نقض حقوق تضمین‌شده وی توسط قوانین ملی مقرر دارند.» همچنین به‌موجب ماده ۲۳ این دستورالعمل کشورهای عضو بایستی مقرر کنند که هر شخصی که درنتیجه عملیات پردازش غیرقانونی یا هر اقدام ناسازگار با قوانین ملی تصویب‌شده، پیرو این دستورالعمل متحمل آسیب شده مستحق دریافت غرامت از شبکه برای آسیب متحمل شده می‌باشد. (Directive 95/46/EC,1995: Article 22,23) همچنین در کشور آمریکا دو قانون حمایت مالکیت‌های فکری ۱ و قانون توقف نقض مالکیت‌های فکری آنلاین [۲]به دادستان کل این مجوز را می‌دهد که با نظارت قضایی به تأمین‌کنندگان خدمات اینترنتی دستور دهد تا دسترسی به نام‌های دامنهٔ چنین سایت‌هایی را که به فعالیت‌های ناقض مالکیت‌های فکری می‌پردازند، مسدود کنند، حتی اگر این سایت‌ها مطالب و محتوای قانونی نیز داشته باشند۳. (رستم علی زاده، حاجی ملامیرزایی، ۱۳۹۹ :۱۳۶۷) جدای از مطالب قوانین مطروحه «قانون بهبود اجرای حقوق شبکه‌های اجتماعی»آلمان مکانیسمی را جهت شکایت از شبکه‌های اجتماعی ایجاد نموده است. بطوریکه به‌موجب این قانون، شبکه‌های اجتماعی موظف به ایجاد یک‌رویه شکایات مربوط به محتوای غیرقانونی گردیدند که اجازه می‌دهد محتوای غیرقانونی به‌موقع حذف شود. بدین‌صورت که محتوایی که «به‌وضوح غیرقانونی است» بیست‌وچهار ساعت پس از دریافت شکایت باید در داخل مسدود شود. اگر غیرقانونی بودن کمتر آشکار است در این صورت

1. Preventing Real Online Threats to Economic Creativity and Theft of Intellectual ,Property Act of 2011 Protect IP Act (PIPA)
2. Stop Online Piracy Act (SOPA) House Judiciary Committee; October 26, 2011
۳. این دو قانون در پی هدف قراردادن سایت‌هایی هستند که در خارج از ایالات متحده قرار گرفته‌اند و دارای مطالبی هستند که حقوق مالکیت‌های فکری این کشور را نقض می‌کنند.

شبکه‌های اجتماعی ۷ روز فرصت جهت بررسی و امحا آن مطلب دارند. این تعهد شبکه‌های اجتماعی به خودتنظیمی مقررات[1] می‌بایست تضمین نماید که ظرف مدت ۷ روز موضوع بررسی گردد و همچنین در این مقررات باید قواعد حاکم بر آئین دادرسی و مکانیسم شکایت نیز پیش‌بینی گردد. البته شبکه‌های اجتماعی که عمداً یا سهل‌انگارانه تعهدات فوق را نقض کنند، ممکن است جریمه شوند. بر اساس این قانون اگر عامل تعیین‌شده به درخواست اطلاعات واکنش نشان ندهد، جریمه‌ای تا سقف ۵ میلیون یورو (حدود ۵/۷ میلیون دلار آمریکا) ممکن است وضع شود. برای سایر تخلفات، شبکه اجتماعی ممکن است تا ۵۰ میلیون یورو جریمه شود. (Act to Improve the Enforcement of Rights on Social Networks,2017:Article1-2)

همچنین طبق قوانین آلمان، افراد آسیب‌دیده می‌توانند مسدود نمودن حساب متخلف را از اپراتور پلتفرم (به‌طور موقت) درخواست کنند(Kaesling, 2018:153) کشور سوئد جهت مدیریت محتوای غیرقانونی شبکه‌های اجتماعی قانون مسئولیت برای شبکه آگهی‌های الکترونیکی در سال ۱۹۹۸ را تصویب نموده است. طبق ماده ۱ این قانون شبکه اجتماعی الکترونیکی سیستم‌های واسطه‌ایی هستند که کاربران می‌توانند داده‌ها را بارگذاری کنند، اخبار را بخوانند و تبادل پیام با سایر کاربران داشته باشند. هدف قانون مذکور این است که ارائه‌دهنده‌های خدمات شبکه‌های اجتماعی را برای حذف پیام‌هایی که به‌وضوح سخنان نفرت‌انگیز، پورنو گرافی کودکان، تصویربرداری غیرقانونی خشونت، کپی‌رایت را تشویق و یا نقض می‌کند متعهد نماید (Act on Responsibility for Electronic Bulletin Boards,1198: Article1) بنابر ماده ۵ این قانون صاحبان و ارائه‌دهندگان خدماتِ اخباری مبتنی بر اینترنت باید به‌منظور انجام تعهدات خود برای حذف یا مسدود کردن غیرقانونی مطالب، نظارت نمایند بنابراین شبکه‌های اجتماعی به‌طورکلی موظف به نظارت بر پلت فرم‌های خود هستند. همچنین این قانون نیز صاحبان شبکه‌های اجتماعی را متعهد به ایجاد مکانیسمی می‌کند که افراد را نسبت به طرح شکایت علیه آن پلتفرم در صورت وقوع اقدامات غیرقانونی مساعدت نماید. (Ibid, Article5) در انگلستان نیز کمیته امور داخلی مجلس عوام طی یک توصیه‌نامه به دولت تکلیف نموده که دولت می‌بایست اقدام به اعمال تحریم‌ها و جریمه‌های بیشتر برای شرکت‌های رسانه‌های اجتماعی‌ای نماید که محتوای غیرقانونی را در یک بازه زمانی دقیق حذف نمی‌کنند. (House of Commons, 2017:14)

1. Agency of Regulated Self-Regulation

انتقال محل ذخیره دادها به داخل

یکی از بهترین مکانیسم‌ها جهت نظارت بر شبکه‌های اجتماعی و جلوگیری از سوءاستفاده از داده های افراد، انتقال محل ذخیره داده‌ها به داخل کشورها است. این ایده منجر به این شد که شرکتی به نام ورن گلوبال[1] برای ذخیره داده‌های مشتریان خود، ایسلند را انتخاب و عملیاتی کند. انتخاب ایسلند نه‌تنها بر اساس هزینه‌های پایین راه‌اندازی این مراکز، بلکه بر اساس اصلاح قانون ایسلند باهدف تبدیل آن کشور به کشوری با پیشرفته‌ترین مراکز حریم خصوصی داده‌ها در جهان با حراست مناسب از ارائه‌دهندگان خدمات اینترنت و مخابراتی بوده است. (Gaedtke, 2014) همچنین به اعتقاد برخی حکم پرونده شرمس در دیوان دادگستری اروپا در سپتامبر ۲۰۱۵به این معنا بود که ذخیره داده در خارج از اتحادیه اروپا توسط سرویس غیراروپایی به‌صورت رسمی برای ذخیره اطلاعات افراد مستقر در اتحادیه اروپا ریسک‌پذیر است. (Kelion, 28 Oct 2015) بدین‌جهت است که مایکروسافت وعده داده که اطلاعات ابری را خارج از منطقه‌ای که مشتریان آن را قرار می‌دهند، منتقل نکند و این شرکت تحت حاکمیت همه قوانین و مقررات محلی خواهد بود. به‌علاوه، مایکروسافت قادر به دسترسی به داده‌ها در ابر بدون مجوز متولی داده‌ها یا مشتریان نخواهد بود و در صورت اعطای مجوز توسط متولی داده‌ها، صرفاً این کار را تحت نظارت‌های آن کشورها انجام می‌دهد. این سبب می‌شود که دسترسی به داده‌ها برای مراجع خارجی دشوار شود. (Kelion,10 Nov 2015) همچنین به‌موجب ماده ۳۷ قانون امنیت سایبری چین اپراتورهای ساختارهای کلیدی باید اطلاعات حساس و شخصی جمع‌آوری‌شده توسط خود و تولیدشده در حین عملیات در کشور چین را حفظ کنند (Cybersecurity Law of of China, 2016:. Article 37) آن‌ها می‌توانند این اطلاعات را به میزانی به خارج از کشور ارسال کنند که مطابق با قوانین شورای حکومت کشور چین باشد. زمانی که این اپراتورها محصول یا خدمات شبکه را که بر امنیت سایبری اثرگذار هستند، تحصیل نمایند، بازرسی امنیت ملی لازم می‌شود. همین‌طور بند ۵ ماده ۴ قانون اینترنت ترکیه در این خصوص بیان می‌دارد: «ارائه‌دهندگان شبکه‌های اجتماعی خارجی یا محلی با بیش از یک‌میلیون دسترسی روزانه از ترکیه موظف‌اند تمام اقدامات لازم را برای ذخیره داده‌های متعلق به کاربران در ترکیه در داخل ترکیه انجام دهند.»

1. Verne Global

(Turkish Internet Law ,2020: Article4(5)) به‌علاوه به‌موجب ماده ۵ قانون اصلاحیه فدرال روسیه که درباره حفظ داده‌های شخصی است و از تاریخ ۱ سپتامبر ۲۰۱۶ الزام‌آور شده است، اپراتوری که اقدام به ثبت، ذخیره‌سازی، به‌روزرسانی یا اصلاح و بازیابی اطلاعات شخصی شهروندان فدراسیون روسیه می‌کند، بایستی اطلاعات مرتبط را در مراکز داده واقع در سرزمین روسیه ذخیره‌سازی کند (Federal Law No. 242-FZ, 2014: Article2(1)). همچنین در ایالات متحده آمریکا به جهت نگرانی‌های امنیتی مقامات آمریکایی نسبت به دسترسی خارجی به داده‌های کاربران آمریکایی «پروژه تگزاس» کلید خورد؛ براین‌اساس، از ژوئن ۲۰۲۲، صد در صد ترافیک کاربران ایالات‌متحده به زیرساخت ابری اوراکل[1] در ایالات‌متحده هدایت می‌شود و داده‌های کاربران آمریکایی نسبت به دسترسی خارجی مهروموم می‌شود. بنابراین، داده‌های آمریکایی در یک شرکت آمریکایی در خاک ایالات‌متحده و تحت نظر کارکنان آمریکایی ذخیره گردید. (Hendrix,2023)

نتیجه‌گیری

با گسترش اینترنت و بالأخص همه‌گیری شبکه‌های اجتماعی هرچند سرعت انتقال اطلاعات و تغذیه محتوای آن از سوی کاربران تغییرات چشم‌گیری داشته است، لکن به همان نسبت تشویق به خشونت، انتشار سخنان نفرت‌انگیز نژادی، سیاسی و مذهبی، افشای غیرمجاز اطلاعات شخصی، کلاه‌برداری‌های اقتصادی و....چالش‌های امنیتی، اخلاقی، اجتماعی، اقتصادی، قضایی متعددی را برای دولت‌ها ایجاد نموده که موجب گردید در تمامی کشورها بحث نظارت بر شبکه‌های اجتماعی بیش‌ازپیش اهمیت یابد. لذا در عرصه ملی با توجه به اختیارات اعطاشده از ناحیه کنوانسیون‌های حقوق بشری در برخورد با محتوای غیرمجاز شبکه‌های اجتماعی، دولت‌ها اقدام به تصویب قوانین و مجازات کیفری و نیز قواعد مدنی در جهت کنترل این شبکه‌ها نمودند. به عبارتی دقیق‌تر استانداردهای حقوق بشری مندرج در کنوانسیون‌های بین‌المللی از یک‌سو بر امنیت ملی، نظم عمومی، بهداشت و سلامت عمومی دولت‌ها توجه دارند و از سوی دیگر استانداردهای حقوق بشری مربوط به شبکه‌های اجتماعی که همانا دسترسی آزاد به این شبکه‌ها و نیز صیانت از

1. Oracle Cloud Infrastructure

داده‌های شخصی کاربران می‌باشد را به رسمیت می‌شناسند. واقعیت هم آن است که بهترین مسیر جهت نظارت بر شبکه‌های اجتماعی مسئول نمودن صاحبان آن‌ها در قبال درخواست‌های دولت‌ها از طریق وضع قانون می‌باشد. به عبارتی دیگر دولتها از طریق قانون‌گذاری در جهت مسئول نمودن شبکه‌های اجتماعی، تکلف به معرفی نماینده از سوی شبکه‌های اجتماعی، ایجاد مکانیسمی جهت شکایت و اعمال مجازات از صاحبان پلتفرم‌ها ، الزام به انتقال محل ذخیره داده ها به داخل تکلیف خود به نظارت بر داده‌های کاربران رسانه‌های اجتماعی را افزایش دادند. لذا دولت‌ها از این طریق نه تنها صلاحیت قضایی خود را بر کاربران شبکه‌های مجازی بلکه بر پلتفرم‌های این شبکه‌ها درصورتی‌که مرز مربوط به جرائم مندرج در قانون آن کشور را رد نمایند، اعمال می‌کنند. با نگاهی به عملکرد دولت‌ها جهت نظارت بر شبکه‌های اجتماعی می‌توان ادعا نمود که دوره ماه‌عسل شبکه‌های اجتماعی به پایان رسیده است؛ تا جائی‌که می‌توان بیان داشت که پلتفرم‌های رسانه‌های اجتماعی در حال حاضر با «تورم نظارتی» جهانی روبرو هستند . به‌عبارتی‌دیگر اصول نوظهور حاکمیت اینترنت منعکس‌کننده اجماع فزاینده‌ای در موردنیاز به نظارت بر فعالیت‌های نهادهای بخش خصوصی درگیر در نگهداری اینترنت، یا به‌عنوان واسطه بین اینترنت و کاربران فردی است. با امعان نظر به مطالب مطروحه می‌توان استدلال نمود که اصولا تصویب قوانین نظارتی و صیانتی از کاربران در ایران نیز خلاف قواعد حقوق بین‌الملل نمی‌باشد. هرچند ضروری است در تصویب نهایی این قوانین از یک سو ابهامات و خلأهای این قانون همچون تعیین تکلیف کسب‌وکارهای اینترنتی ، اقناع جامعه هدف این طرح‌ها ، اطمینان از عدم نقض حریم خصوص افراد و... مرتفع گردند و از سویی دیگر مسئولین ذیربط به موازات تصویب قوانین نظارتی راهکارهای دیگری به مانند سرمایه‌گذاری بخش خصوصی در تولید و توسعه پلتفرم ، تخصیص بودجه جهت گسترش این نوع از پلتفرم‌ها، معافیت‌های مالیاتی را به عنوان مکمل طرح‌های نظارتی در دستور کار خود قرار دهند. واقعیت آن است با توجه به تحریم‌های بی سابقه علیه جمهوری اسلامی ایران عملاً امکان حضور بسیاری از پلتفرم‌های خارجی که اغلب مالکیتی آمریکایی دارند در ایران امکان‌پذیر نمی‌باشد لذا ارائه پلتفرم‌های داخلی باکیفیت و خصوصی و تضمین عدم نقض حریم خصوصی یا پردازش اطلاعات بدون رضایت کاربر، می‌توان عملاً همان اهداف قوانین نظارتی را دنبال نمود.

فهرست منابع

احمدی‌نژاد، مریم؛ امین الرعایا، یاسر(۱۳۹۵)، ماهیت حقوقی دکترین حاشیه مجاز تفسیر، فصلنامه سیاست خارجی، سال سی‌ام، شماره۲، تابستان۱۳۹۵

امین الرعایا، یاسر ، احمدی‌نژاد، مریم، متاجی، محسن، (۱۴۰۰) ، تحلیلی بر اصول، قواعد و رویه‌های بین‌المللی در قطع اینترنت در مواقع اضطراری و امنیتی ، نشریه علمی آفاق امنیت، سال چهاردهم ، شماره پنجاه و یکم تابستان

انصاری، باقر (۱۳۹۹). حق دسترسی به اینترنت؛ مبانی و محتوا، مجله حقوقی دادگستری، دوره ۸۴، ش ۱۱۲

جباری، منصور، حاتمی، فاطمه (۱۳۹۳). نقش اتحادیه بین‌المللی مخابرات در تدوین و توسعه حقوق بین‌الملل فضای ماورای جو ، فصلنامه پژوهش حقوق عمومی، سال پانزدهم، شماره۴۲،بهار

حبیب نژاد، سید احمد، عصاره، عبدالله (۱۳۹۰)، محدودیت‌های دسترسی به اطلاعات در اینترنت، مجله حقوق اسلامی، سال هشتم، شماره ۲۸

رستم علی زاده، سعید، حاجی ملامیرزایی ، حامد(۱۳۹۹). نظام حقوقی حاکم بر فیلترینگ اینترنت در ایالات متحدهٔ آمریکا، فصلنامهٔ مطالعات حقوق عمومی، دورهٔ ۵۰ ، شمارهٔ ۴، زمستان

رسولی ، محمدرضا ، غفوریان تبریزی، آزاده (۱۳۹۵). بررسی نقش شبکه‌های اجتماعی در جنبش‌های اجتماعی جهان ، مجله علوم خبری ، سال چهارم بهار ، شماره۱۷

سخنرانی مقام معظم رهبری، سخنرانی نوروزی با مردم، ۱۴۰۰/۱/۱.

قانون راجع به تصویب اساسنامه و اصلاح مقاوله‌نامه (کنوانسیون) اتحادیه بین‌المللی مخابرات (ITU) منعقده در سیزدهمین اجلاس سران مختار کشورهای عضو ۱۹۸۹ (نیس) و اجازه مبادله اسناد مصوب آن‌ها، مصوب ۱۳۷۱/۱۲/۱۸ مجلس شورای اسلامی.

کریانساک کیتیچایسری (۱۴۰۰)، حقوق بین‌الملل عمومی در فضای سایبری، مترجم: حسین امین الرعایا، انتشارات مجد ، چاپ اول.

Act to Improve the Enforcement of Rights on Social Networks (NetzDG) ,Federal Government of Germany 1 June 2017

Al Jazeera (2016),Turkey to investigate massive leak of personal data, 6 Apr.

Big Brother Watch and Others v. United Kingdom(2018), European Court of Human Rights, Judgment of 13 September

Bird ,Robert C. , Smythe, Donald J. , (2012), Social Network Analysis and the Diffusion of the Strict Liability Rule for Manufacturing Defects, Law & Social Inquiry Vol. 37, No. 3

Christakis ,Theodore , Bouslimani ,Katia(2020). , 'National Security, Surveillance and Human Rights', SSRN,8 June

Cohen ,Julie E. (2017), 'Law for the Platform Economy, University of California, Vol. 51

de Sola Pool, I. (1983). *Technologies of Freedom*. Cambridge, MA: Harvard University Press.

Delfi AS v. Estonia(2015),European Court of Human Rights, Appl. no. 64569/09, Judgment of 16 June

European Court of Human Rights, Appl. no. 22947/13,Judgment of 2 February

Exec. Order No. 13942, TikTok Order Addressing the Threat Posed by TikTok, and Taking Additional Steps To Address the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain, 85 Fed. Reg. 48637 (Aug. 6, 2020)

Fagan, Frank (2018) Systemic Social Media Regulation, Duke Law & Technology Review, No. 1, Vol. 16

Flew, T., Martin, F., & Suzor N. (2019). Internet Regulation as Media Policy: Rethinking the Question of Digital Communication Platform Governance.Journal of Digital Media and Policy, 10(1)

Gaedtke ,Felix(2014), Can Iceland become the 'Switzerland of data?, Al Jazeera, 28 Dec

George ,C.E. and Scerri, J. (2007)., Web 2.0 and User-Generated Content: Legal Challenges in the New Frontier', 2 Journal of Information, Law andTechnology 1

Gillespie, T. (2017). Governance of and by Platforms. In J. Burgess, T. Poell, & A. Marwick (eds.), SAGE Handbook of Social Media (pp. 254–278). Los Angeles: Sage.

Hendrix, Justin, Transcript: TikTok CEO Testifies to Congress, Tech Plicy Press website, 2023. Available from: https://techpolicy.press/transcript-tiktok-ceo-testifies-to-congress/ .visited: 5/8/2023

IT Countrey Justice,(2014), "Internet Governance Theory – Collisions in the Digital Paradigm III" 13 Jul

Kaesling ,Katharina (2018), Privatising Law Enforcement in Social Networks: A Comparative Model Analysis, Erasmus Law Review ,Vol. 11, No. 3,

Kelion ,Leo(2015), 'Microsoft to open UK data centres', BBC, 10 Nov

Kelion, Leo(2015), Schools given Dropbox guidance after safe Harbour warning, BBC, 28 Oct

Kleinschmidt ,B. (2010), 'An International Comparison of ISP's Liabilities for Unlawful Third Party Content', 18 IJLIT 332

Költzow ,Sarah (September 2013) ,Monitoring and Evaluation of Peacebuilding: The Role of New Media, Geneva Peace Building Platform

Leventoff, J. (2023). ACLU Strongly Opposes House Bill that Would Ban TikTok and Threaten First Amendment Rights. American Civil Liberties Union website, available from:https://www.aclu.org/press-releases/aclu-strongly-opposes-house-bill-that-would-ban-tiktok-and-threaten-first-amendment-rights Visited at: 29/03/2023

Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt(MTE) v. Hungary,2016

Maximillian Schrems v. Data Protection Commissioner (Hogan J.), 18 Jun. 2014

Prosecutor v Mahmoud Mustafa Busayf Al-Werfalli,(2017) International Criminal Court (ICC), Warrant of Arrest ,15 August

Rodriguez M. Belén V. Google Inc ,Supreme Court (Argentina)(2014), Judgment , 28 October

Rosine ,Faucher (2019), Social Media and Change in International Humanitarian Law Dynamics , Inter Gentes Vol. 2 Issue 1

Sander ,Barrie(2021), Democratic Disruption in the Age of Social Media: Between Marketized and Structural Conceptions of Human Rights Law, The European Journal of International Law, Vol. 32 no. 1

Segall ,Laurie, (2015) ,An app called Telegram is the 'hot new things among Jihadists, CNN, 18 Nov

Stecklow ,S. (2018), Hatebook: Why Facebook Is Losing the War on Hate Speech in Myanmar', Reuters ,15 August

Taub ,A. , Fisher ,M(2018), Where Countries Are Tinderboxes and Facebook Is a Match', New York Times ,21 April.

Act on Responsibility for Electronic Bulletin Boards (EBB). Swedish Code of Statutes 1998
code of Conduct on countering illegal hate speech online 2016
commissioner for human rights(2012) 8, social media and human rights, CommDH, Strasbourg, February
Concluding Observations on the Fourth Periodic Report of the United States of America(2014), International Covenant on Civil and Political Rights ,United Nations ,UN,23 April
Directive 2000/31/EC of the European Parliament and of the Council, 8 June
Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995
European Commission Communication(2017) ,Tackling Illegal Content Online. Towards an enhanced responsibility of online platforms', COM 555 Final, 28 September
European Treaty Series - No. 108, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.I.1981
French Data Protection Authority(2019), Deliberation of the Restricted Committee , pronouncing a financial sanction against
General Comment no. 16 (1988) Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 Apr,UN Human Rights Committee (HRC), ICCPR
House of Commons(2017), Hate Crime: Abuse, Hate and Extremism Online, Fourteenth Report of Session 2016-17
Iqbal, Mansoor, TikTok Revenue and Usage Statistics, Available from: https://www.businessofapps.com/data/tik-tok-statistics/. Last visited: 5/8/2023
Joint Declaration of the Three Special Rapporteurs for Freedom of Expression (2011)
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such
Report on the intelligence relating to the murder of Fusilier Lee Rigby (2014), Intelligence and Security Committee of Parliament, 25 Nov
the International Telecommunication Union (ITU)
The New York Times, (2023). Why Countries Are Trying to Ban TikTok, Available from: https://www.nytimes.com/article/tiktok-ban.html Visited at: 29/03/2023
The Turkish Internet Law: Full Translation of the Law , 2020 , no. 5651
"Internet Enemies" Archived 2014-03-12 at the Wayback Machine, Enemies of the Internet 2014: Entities at the heart of censorship and surveillance, Reporters Without Borders (Paris), 11 March 2014. Retrieved 24 June 2014.
Federal Law No. 242-FZ of July 21, 2014 on Amending Some Legislative Acts of the Russian Federation in as Much as It Concerns Updating the Procedure for Personal Data Processing in Information-Telecommunication Networks
Commission Recommendation of (1 March 2018),on measures to effectively tackle illegal content online
European Commission, Daily News 7 May 2018, MEX/18/3723.
Digital Global Statshot Report, Apr 2022 ,v01
Cybersecurity Law of the People's Republic of China, November 7, 2016

پایگاه خبری تحلیلی انتخاب ، واکنش وزیر ارتباطات به طرح مجلس درباره فضای مجازی: حکمرانی سایبری باید برای بهره‌گیری باشد نه انسداد ،حذف دولت از فرایند تصمیم‌گیری، حکمرانی سایبری را مبهم‌تر می‌کند ،۱۴۰۰/۴/۷.

پایگاه خبری تحلیلی سلام نو ، واکنش سیدمحمد خاتمی به طرح صیانت مجلس / نه کارساز است و نه مفید، ۱۴۰۰/۵/۹.

خبر آنلاین ، طرح صیانت از فضای مجازی چطور کاربران را محدود می‌کند؟، ۷ /۱۴۰۰/۵.

خبرگزاری بی‌بی‌سی، ۶ دی ۱۴۰۰.

خبرگزاری جمهوری اسلامی ایران (ایسنا).

دویچه وله فارسی، طرح صیانت از حقوق کاربران یا حذف مردم ایران از دهکده جهانی؟، ۷ مردادماه ۱۴۰۰

دیوار بلاگ- بیانیه دیوار درباره محکومیت اشکان میرآرمندهی ، ۱۴۰۰/۹/۶

رادیو فردا، لاری، سیما سادات، گزارشگران بدون مرز: طرح صیانت از فضای مجازی برگرفته از روش «سانسور در چین» است، .۲۰۲۱/۷/۰۸.