

Phenomenology of Violations of Fundamental Human Rights by the Actions of Authoritarian States in Cyberspace

Akbar Shoja

M.A. Graduate, Bukan Branch, Islamic Azad University, Bukan, Iran.

Ali Sabernejad Alavian*

Assistant Professor, Department of Law, Ghazali University, Qazvin, Iran.

Hatam Soltani

Department of Public Law, Islamic Azad University, Bukan Branch, Bukan, Iran

Saberi@ghazali.ac.ir

DOI: 10.30495/CYBERLAW.2023.703200

Keywords:

Cyber Space,
Authoritarianism,
Human Rights,
Troll Army,
Artificial
Intelligence,
Social Networks

Abstract

As an attractive, accessible and inclusive environment, the cyberspace has many capacities for the development and expansion of basic human rights and demands regarding them. But in reality and action, the mentioned space has become a tool to violate these rights, and the politicians of "authoritarian" States, with the help of the capacities of this space - especially social networks -, have violated the basic human rights including privacy, right to freedom of information and freedom of expression. The present article, employing the descriptive-analytical methods and with rational induction in the performance of some authoritarian States in the cyberspace, constitutes an attempt in finding cases of human rights violated by the "cyber authoritarianism" of the mentioned governments and the optimal understanding of the threats to the human rights using new technologies and artificial intelligence. The findings of the research indicate that cyber authoritarianism has fundamentally violated human rights by violating data privacy and security, denying free access to information, spreading false information and limiting the right to freedom of expression and that nowadays many states have been busy with establishing grounds in cyberspace for continuation of their authoritarianism by forming special malicious cyber groups such as "Keyboard Army" and using "Trolls" in the way of engineering public opinion and thought, hiding information and giving false information.



This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license:

(<http://creativecommons.org/licenses/by/4.0/>)

پدیدارشناسی نقض حقوق اساسی بشر توسط عملکرد دولت‌های اقتدارگرا در بستر فضای سایبر

اکبر شجاع

دانش آموخته مقطع کارشناسی ارشد حقوق عمومی، واحد بوکان، دانشگاه آزاد اسلامی، بوکان، ایران.

*علی صابر نژاد علویان

استادیار گروه حقوق، دانشگاه غزالی، قزوین، ایران.

حاتم سلطانی

مربی گروه حقوق عمومی، واحد بوکان، دانشگاه آزاد اسلامی، بوکان، ایران.

Saberি@ghazali.ac.ir

تاریخ پذیرش: ۲۳ خرداد ۱۴۰۲

تاریخ دریافت: ۰۶ اسفند ۱۴۰۱

چکیده

فضای سایبر به عنوان محیطی جذاب، در دسترس و فرآیند، ظرفیت‌های زیادی جهت بسط و گسترش حقوق اساسی بشر و مطالبه‌گری در خصوص آن دارد؛ اما در مرحله‌ی عمل فضای مذکور تبدیل به ابزاری جهت تجاوز به همین حقوق گردیده و سیاستمداران دولت‌های «اقتدارگرا» با یاری جستن از ظرفیت‌های این محیط - به طور ویژه شبکه‌های اجتماعی - دست به نقض حقوق اساسی بشری همچون حریم خصوصی، حق بر آزادی اطلاعات و آزادی بیان زده‌اند. مقاله‌ی حاضر با یاری جستن از روش توصیفی - تحلیلی و با استقراء منطقی در عملکرد برخی کشورهای اقتدارگرا در فضای سایبر، در راستای یافتن موارد حقوق بشری نقض شده توسط «اقتدارگرایی سایبری» این دولت‌ها و درک مطلوب تهدیدات حقوق بشر با استفاده از فناوری‌های نوین و هوش مصنوعی می‌باشد. یافته‌های پژوهش حکایت از آن دارد که اقتدارگرایی سایبری با تجاوز به امنیت و حریم داده‌های شخصی، محرومیت از دسترسی آزاد به اطلاعات، انتشار اطلاعات نادرست و محدود کردن حق بر آزادی بیان به صورت بنیادینی منجر به نقض حقوق بشر گردیده است و امروزه بسیاری از دولت‌ها با تشکیل گروه‌های سایبری مخرب خاص همچون «ارتش صفحه‌کلید» و استفاده از «ترول»‌ها در مسیر مهندسی افکار عمومی، پنهان‌کاری اطلاعات و دادن اطلاعات نادرست؛ سعی در بسترسازی سایبری برای تداوم عملکرد اقتدارگراییه خود دارند.

کلید واژگان: فضای سایبر، اقتدارگرایی، حقوق بشر، ارتش ترول، هوش مصنوعی، شبکه‌های اجتماعی.



مقدمه

تصویر کنید هر حرکتی که انجام می‌دهید توسط هزاران دوربین و ناظر الکترونیکی در اطراف شما (حتی در داخل خانه) تماشا می‌شود. می‌خواهید با خانواده و دوستان خود تماس بگیرید اما شبکه اینترنت قطع است. آنلاین می‌شوید تا اخبار مربوط به اتفاقات را بخوانید، اما روی صفحه‌نمایش اخطار «HTTP 404» نمایان می‌شود؛ یا در حساب رسانه‌های اجتماعی پست می‌کنید اما پست انجام نمی‌شود؛ چند ساعت بعد مأموران امنیتی در خانه شما را می‌زنند تا شمارا ببرند. درحالی‌که به نظر می‌رسد این وضعیت از یک فیلم علمی تخیلی و آینده‌نگر روایت می‌شود ولی امروزه تقریباً در خیلی از کشورها اتفاق می‌افتد.

فناوری‌های جدید اطلاعات و ارتباطات توانسته‌اند با گشودن فرصت‌های اقتصادی جدید و کمک به رهایی میلیون‌ها نفر از فقر، افزایش دسترسی به اطلاعات لازم برای سیاست‌گذاری، تصمیم‌گیری بهتر و گسترش دسترسی به آموزش و سلامت، در رفع نابرابری‌های اجتماعی و اقتصادی مفید فایده باشند. راههای جدید کسب و تبادل اطلاعات و ارتباط با افراد دیگر، افق‌های نوینی را برای مشارکت سیاسی، اقتصادی و اجتماعی فراهم نموده و سازمان‌های مردم‌نهاد زیادی از این فناوری، به ویژه اینترنت، در تلاش برای حقوق بشر، دموکراسی و صلح حتی در بسته‌ترین کشورهای اقتدارگرا استفاده می‌نمایند؛ با این حال، همین فناوری اطلاعات و ارتباطات را باید به عنوان یک شمشیر دولبه نگریست. بازیگران سیاسی، به ویژه دولتها، پتانسیل فناوری اطلاعات و ارتباطات را می‌شناسند و بسیاری از رژیم‌های سرکوبگر در بستر همین فضا روش‌های جدیدی را برای محدود کردن حقوق بشر و دموکراسی ابداع نموده‌اند که می‌توان از آن به «ظهور اقتدارگرایی دیجیتال» تعبیر نمود (Freedom House, 2018).

از سوی دیگر استفاده از «هوش مصنوعی»^۱ در این فضا، وضعیت را بغرنج تر کرده است. تمرکز اصلی محققان در مورد هوش مصنوعی به اشکالات آن در حقوق بشر، مانند نقض حریم خصوصی اختصاص دارد. روندهای جدید تحقیقات بر دستورالعمل‌های اخلاقی، شفافیت، توضیح‌پذیری و پاسخگویی افراد درگیر در پروژه‌های اعمالی این هوش متمرکز است. در خصوص مسئولیت دولتها با استفاده از این فناوری باید بیان داشت که از نظریه مسئولیت جمعی و توزیعی افراد در رابطه با اشتباه آن، ازانجایی که هوش مصنوعی نمی‌تواند آزادانه تصمیم بگیرد یا عمل کند و به دلیل فقدان آزادی و آگاهی نیست، هیچ اراده یا قصدی برای اقدام یا تصمیم‌گیری ندارد و هوش مصنوعی ازانچه انجام می‌دهد آگاه نیست (Mirzazadeh, 2023: 7). بنابراین هر نوع نقض حقوق بشری متوجه دولت استفاده‌کننده از آن خواهد بود. از این‌رو، نوشتار حاضر با استقراء در عملکرد برخی کشورها به بررسی این موضوع می‌پردازد که چگونه «دولتها اقتدارگرایی»^۲ و سایر بازیگران دقیقاً از اقتدارگرایی دیجیتال و هوش مصنوعی برای محدود کردن حقوق بشر استفاده می‌نمایند. هدف این مقاله درک بهتر تهدیدات حقوق بشر با استفاده از فناوری اطلاعات و ارتباطات در فضای سایبر بوده و به دنبال شناسایی راههای مختلفی است که دولتها و سایر بازیگران ذی‌صلاح از فناوری اطلاعات و ارتباطات در بستر فضای سایبر برای محدود کردن دسترسی و تبادل اطلاعات و ارتباطات و نهایتاً برای سرکوب مخالفان استفاده می‌کنند.

۱. اقتدارگرایی در فضای سایبر

می‌توان ادعا نمود که عصر حاضر «چرخش جهانی به استبداد» را تجربه می‌کند (Murakami, 2017: 358). که این روند دستاوردهای جنبش‌های حقوق بشر در چند دهه اخیر را تهدید می‌نماید. مطالعه‌ی چگونگی تأثیر استبداد، در همه اشکال آن بر حقوق بشر، برای دفاع بهتر از آن در مقابل دولت مستبد حائز اهمیت است. در اندیشه ادبیات حقوق سیاسی جهان مطلوب‌ترین مفهوم از اقتدارگرایی را دانشمند علوم سیاسی اسپانیایی «خوان لینز»^۳ ارائه نموده است که آن را یک نظام سیاسی دارای کثرت‌گرایی محدود، فاقد ایدئولوژی راهنمای، با مشارکت حداقلی مردم و قدرت نامتناهی حاکمان آن می‌داند (Linz, 2000: 159).

^۱ Artificial Intelligence

^۲ Authoritarianism

^۳ Juan Linz

بسیاری از نظریسین‌های مدرنیزاسیون، طرفدار پیش‌شرط اقتصادی در گذار به دموکراسی باور داشتند توسعه اقتصادی پیش‌شرط دمکراتیزاسیون می‌تواند باشد ولی در چین با وجود موقوفیت‌های اقتصادی و اجتماعی گذار به دموکراسی بر بنای مدل موردنظر آنها رخ نداده است. اینکه چه عواملی باعث شده است که نظری مدرنیزاسیون در گذار به دموکراسی با پیش‌شرط اقتصادی در چین تحقق پیدا نکند، بایستی در موقعیت دولت و جامعه جستجو کرد (منقی و جباری، ۱۴۰۱: ۱۴۰). لذا تعجب آور نیست که بشنویم در دوران ریاست جمهوری «شی جین پینگ»^۴، چین خیلی بیشتر از قبل اقتدارگرا به نظر می‌رسد (Ang, 2018). با این حال، در کشورهای ظاهراً دموکراتیک که در آن انتخابات به‌طور منظم برگزار می‌شود و آزادی‌های مدنی و سیاسی ظاهرآ توسعه قانون تضمین شده است، مفسران بر این باورند که «هندي اقتدارگرا پدید آمده است» (Nilsen, 2018). و «فیلیپین به‌تازگی اقتدارگرایی شده است» (Santos, 2018). در این راستا برخی محققان حقوق سیاسی پیشنهاد می‌نمایند که به‌جای تمرکز بر رژیم‌ها یا رهبران استبدادی، باید بر شیوه‌های اقتدارگری متوجه شد؛ بنابراین باید تجزیه و تحلیل اقدامات بازیگران سیاسی پس از رسیدن به قدرت را مدنظر داشت (Glasius, 2018: 94). رویکرد اخیر فراتر از تحلیل‌های دولت‌محور یا تک‌بعدی از اقتدارگرایی است و به بررسی وضعیتی می‌پردازد که از مزهای دولت فراتر رفته و دخالت بازیگران دولتی و غیردولتی در گذارگرایی را شناسایی و بازنخواست می‌نماید؛ همچنین به این معنی است که عملکرد اقتدارگرایانه را می‌توان در کشورهای به‌اصطلاح دموکراتیک که در آن تعاریف کلاسیک اقتدارگرایی کاربرد ندارد، تحلیل نمود. این رویکرد ظرفیت بررسی چگونگی استفاده از فضای سایبر برای سرکوب حقوق و آزادی‌های اساسی از طریق نظارت خودسرانه، پنهان‌کاری، اطلاعات نادرست و نقض آزادی بیان را دارد (Glasius & Michaelsen, 2018: 3795).

از سویی دیگر فضای سایبر فرصت‌های جدیدی را برای پیشرفت حقوق بشر ارائه نموده است. برای مثال رسانه‌های اجتماعی و برنامه‌های پیام‌رسانی مانند «واتس‌اپ»^۵ برای بسیج مردم در دفاع از حقوق و منافع خود استفاده شده‌اند (Ruijgrok, 2016: 499). به‌طورکلی اینترنت نقش مهمی در کمک به سازمان‌های حقوق بشر برای جمع‌آوری و انتشار اطلاعات در مورد حقوق بشر به عموم مردم ایفا نموده (Halpin & Hick, 2000: 238). و سامانه‌های جدید، ذخیره‌سازی اطلاعات و انتقال آن را آسان‌تر کرده است؛ تا جایی که حتی تلفن هوشمند معمولی نیز می‌تواند ابزاری قدرتمند برای ثبت و مستندسازی نقض حقوق بشر باشد؛ اما همان‌گونه که بیان شد این ابزار یک شمشیر دو لبه بوده و شیوه‌های اقتدارگرایانه در این فضا برای محدود کردن و نقض حقوق بشر نیز استفاده گردیده است. به‌عنوان نمونه در این فضا حقوق اساسی بشری همچون «حریم خصوصی» زمانی مورد تجاوز قرار گرفته که اقدامات یک فرد به‌طور مدام توسط سیستم‌های نظارتی پیشرفت‌های نظارت‌شده یا داده‌های شخصی ذخیره شده در یک پایگاه داده در دسترس نیروهای امنیتی دولتی درزمانی مشخص قرار گرفته است (Lucas & Feng, 2018: 86). نکته‌ی جالب آن است برخلاف تصور عمومی که باید این تحظی‌ها در کشورهای جهان سوم صورت پذیرد، بیشتر در ممالک ظاهراً دموکراتیک حادث شده است و مطالعات بسیاری حکایت از استفاده فناوری اطلاعات و ارتباطات جهت نظارت و تأثیرگذاری بر شهروندان توسط دولتها در «غرب لیبرال» دارد (Hintz & Milan, 2018: 3940). که نمونه بارز آن استفاده از رسانه‌های اجتماعی برای مهندسی افکار عمومی از طریق ایجاد حساب‌های جعلی برای حمایت از نامزدی «دونالد ترامپ»^۶ در سال ۲۰۱۸ هست.

قبل از تلاش برای تعریف اقتدارگرایی دیجیتال به‌عنوان یک مفهوم، باید این نکته مد نظر قرار گیرد که تالی فاسد اقتدارگرایی اصولاً در دو زمینه نمایان می‌شود اولی «استقلال و حیثیت یک فرد» را نقض کرده و به موضوع حقوق بشر ارتباط دارد؛ از سوی دیگر، مورد دوم، مسئولیت‌پذیری را خراب می‌کند، درنتیجه فرآیندهای دموکراتیک را تهدید کرده و بنابراین یک چالشی اساسی برای دموکراسی است (Glasius & Michaelsen, 2018: 3797). البته باید یادآور شد که هر دو تالی فاسد را می‌توان در نقض حقوق بشر فروکاست. در همین راستا تهدیدات برای افراد در فضای سایبر را می‌توان به سه دسته طبقه‌بندی نمود:

۱. نظارت خودسرانه (نقض حریم خصوصی)

⁴ Xi Jinping

⁵ WhatsApp

⁶ Donald John Trump



۲. پنهان‌کاری و اطلاعات نادرست (نقض حق بر آزادی اطلاعات)

۳. نقض آزادی بیان

در حالی که نظارت خودسرانه (نقض حریم خصوصی) یک عمل غیر لیبرال و نقض حقوق بشر است، پنهان‌کاری و اطلاعات نادرست (نقض حق بر آزادی اطلاعات) عملی اقتدارگرایانه و تخطی به دمکراسی است؛ زیرا مسئولیت پاسخگویی رهبران در قبال رأی دهنگانشان را مخدوش می‌نماید و نقض حق بر آزادی بیان نیز تخلف از هر دو معیار حقوق بشر و دمکراسی است. البته همان‌گونه که نویسنده مقاله عقیده دارد هر سه مقوله فوق، موضوعات حقوق بشری بوده و منجر به نقض حقوق بشر در فضای سایبری هستند. هر یک از این سه دسته، حقوق بشر خاصی را که در میثاقین ذکر شده، نقض می‌کند. نظارت خودسرانه حق حفظ حریم خصوصی افراد را نقض می‌کند در حالی که رازداری و اطلاعات نادرست برخلاف حق بر آزادی اطلاعات است. دسته سوم که به عنوان نقض آزادی بیان ذکر شده است، در عین حال نقض حق مشارکت و حق دخالت در امور سیاسی و عمومی است.

با در نظر گرفتن این موضوع، ما اقتدارگرایی سایبری را به عنوان شیوه‌های استفاده از فناوری اطلاعات و ارتباطات تعریف می‌کنیم که برای تجاوز به حریم خصوصی، ممانعت از دسترسی آزاد به اطلاعات، انتشار اطلاعات نادرست، محدود کردن بیان و محدود کردن مشارکت سیاسی به کاربرده می‌شود؛ که هریک از این موارد در ادامه تحلیل می‌گردد.

۲. نظارت و سانسور (تجاوز به حریم خصوصی سایبری)

حمایت از داده‌ها^۷ و اطلاعات شخصی در فضای سایبر یکی از مهم‌ترین مباحث است. چراکه بدون وجود چنین حمایتی ورود به فضای مذکور و استقبال از فعالیت در آن به شدت کاهش می‌باید (پورقه‌مانی و صابر نژاد، ۱۳۹۴: ۴۴). برای مثال در تجارت الکترونیکی که اعتمادسازی به آن از مهم‌ترین اهداف فعالان این عرصه است، اگر مصرف‌کنندگان از امنیت اطلاعاتی برخوردار نباشند از تجارت الکترونیکی روی برخواهد گرداند (حیب زاده، ۱۳۹۰: ۴۶). در همین راستا مسئله امنیت نیز در این فضای مذکور بسیار حائز اهمیت هست، چراکه زمینه‌ساز فعالیت در این فضا وجود اطمینان و امنیت می‌باشد تا از ورود افسارگسیخته متخلفان به این عرصه اجتناب شود؛ و بالطبع مسئله‌ی حریم خصوصی در این فضا اهمیت شایانی دارد، در این محیط احتیاج به این است که از داده‌های اشخاص که نمود

حریم خصوصی در این فضا هستند محافظت‌ها و مراقبت‌های لازم به عمل آید (صابرنژاد و حسین‌پور، ۱۳۹۶: ۱۱۱).

در ده گذشته، دولتها از استراتژی‌های فنی و قانونی برای تنظیم محتواهای آنلاین استفاده کرده‌اند. تلاقي فناوری، علوم رفتاری و قدرت بازار، برای افزایش نظارت و سانسور اینترنت در بسیاری از کشورها استفاده شده است (Clark et al., 2017). بهترین مثال کشور چین است که در آن مقامات دسترسی شهر و ندان به اطلاعات، جستجوها و برنامه‌های کاربردی موجود در اینترنت را محدود نموده‌اند. از سال ۲۰۱۸، همه ارائه‌دهنده‌گان اینترنت و برنامه‌های کاربردی مانند «علی‌بابا»^۸، «بایدو»^۹، «بایت دنس»^{۱۰} و «تنسنت»^{۱۱}، ملزم به نگهداری گزارش با اطلاعاتی مانند فعالیت‌های کاربرانی خود در «وبلاگ‌ها»، «اتاق‌های گفتگو»^{۱۲}، «پلتفرم‌های ویدیویی کوتاه» و پخش‌های اینترنتی هستند که باید هر وقت دولت برخواهد به آن ارائه نمایند. در آوریل ۲۰۱۸، مقامات چینی به «بایت دنس» دستور دادند تا یک پلتفرم رسانه اجتماعی محبوب را که در آن کاربران اغلب جوک‌ها، ویدیوها و فایل‌های «گیف»^{۱۳} را به اشتراک می‌گذاشتند، که دولتها آن را به عنوان نمایش افکار عمومی نادرست می‌دانست، تعطیل کنند. بعداً، در دسامبر ۲۰۱۸، «رویترز» گزارش داد که چین ۱۱۰۰ حساب رسانه‌های

^۷ Data Protection

^۸ Alibaba Group Holding Limited

^۹ Baidu

^{۱۰} Byte Dance

^{۱۱} Tencent

^{۱۲} Chat Room

^{۱۳} Graphics Interchange Format (GIF)

اجتماعی و ۳۱ وبسایت را بسته است که آن‌ها را به فعالیت‌های غیرقانونی مانند «ترولینگ»^{۱۴} یا باج‌خواهی متهم کرده است (Mayer, 2018).

همه ارائه‌دهندگان اینترنت یا برنامه‌های کاربردی در چین شرکت‌های بومی هستند زیرا سایتها و برنامه‌های اینترنتی خارجی سانسور و مسدود شده‌اند. شرکت‌های چینی موظف هستند اطلاعاتی را برای نظارت مقامات در هر زمان ثبت کنند و به دولت قدرت مطلق برای نظارت بر فضای دیجیتال خود می‌دهند. چین اخیراً یک سیستم نظارتی جدید با فناوری پیشرفته ایجاد کرده است که به شهروندان خود امتیازی به نام «اعتبار اجتماعی»^{۱۵} می‌دهد؛ که این رتبه‌بندی اعتبار اجتماعی بر روی جمعیت عظیم چین نظارت می‌کند. سیستم اعتبار اجتماعی که برای اولین بار در سال ۲۰۱۴ ابداع و تاسال ۲۰۲۰ در سراسر کشور چین عملیاتی شده است، در حال حاضر برای میلیون‌ها نفر در سراسر کشور به صورت آزمایشی در حال اجرا است. امتیاز اجتماعی یک فرد بسته به رفتار او می‌تواند بالا و پایین شود، مانند رانندگی بد، سیگار کشیدن در مناطق ممنوعه، خرید بازی‌های ویدیویی زیاد و ارسال اخبار جعلی آنلاین (Ma, 2018).

نمره اجتماعی بالا به این معنی است که فرد می‌تواند از امتیازات مختلفی برخوردار گردد؛ علاوه بر این، ممکن است درمان بهتری در بیمارستان‌های چین دریافت کند (Marr, 2019). با این حال، به کسانی که امتیازات پایینی دارند، چین از قبل شروع به مجازات افراد با محدود کردن سفر آن‌ها کرده است. در ماه مارس ۲۰۱۸ گزارشی منتشر شد که نشان می‌داد بیش از نه میلیون نفر با امتیازات پایین از خرید بلیت برای پروازهای داخلی منع شده‌اند؛ علاوه بر این، دولت می‌تواند فرد مذکور یا فرزندانشان را از ثبت‌نام در بهترین مدارس منع کند؛ که این ممنوعیت شامل اشخاص امتناع کننده از سربازی اجباری نیز می‌شود (Xueying, 2018). این اشخاص همچنین از استخدام مدیریتی در شرکت‌های دولتی و بانک‌های بزرگ منع می‌شوند و به عنوان شهروندان بد نامیده می‌شوند. این رتبه‌بندی و نمرات حاصل توسط دوربین‌های نظارتی با فناوری بالا و با استفاده از فضای سایبر نظارت و مدیریت می‌شود؛ که در سراسر چین بیش از ۲۰۰ میلیون دوربین به امکاناتی برای تشخیص چهره، اسکن بدن و ردیابی جغرافیایی مججهز هستند تا رفتار شهروندان را پالایش نمایند.

باید مذکور شده که چین تنها کشوری نیست که از این سیستم نظارتی با فناوری پیشرفته استفاده می‌نماید؛ فناوری راه‌اندازی نظارت و امنیت چین با ارائه دوربین‌های پوششی با تکنولوژی تشخیص چهره مبتنی بر هوش مصنوعی برای سازمان‌های مجری قانون، به مالزی نیز نفوذ کرده است. علاوه بر این در ژانویه ۲۰۱۸، شرکت چینی «ییتو»^{۱۶} اولین دفتر خارج از کشور خود را در سنگاپور افتتاح کرد تا به آسیای جنوب شرقی، «هنگ‌کنگ»، «ماکائو» و اقیانوسیه خدمات دهد. فناوری این شرکت می‌تواند با دقیقه ۹۵ درصد، شخص را از پایگاه داده ۱,۸ میلیارد نفری خود در عرض سه ثانیه شناسایی کند. این فناوری در فضاهای عمومی مانند فرودگاه‌ها، بانک‌ها و بیمارستان‌ها در چین استفاده می‌شود (Tan, 2018). این سرمایه‌گذاری‌ها و بهره‌گیری از ظرفیت فضای سایبر و هوش مصنوعی در کشورهای مختلف به بهانه‌ی بهره‌برداری از فناوری‌های نوین برای مدیریت شهری، موجبات نگرانی‌هایی در مورد حریم خصوصی افراد و حقوق اساسی اولیه را ایجاد کرده است.

از سوی دیگر این حق تحت ماده ۱۲ اعلامیه جهانی حقوق بشر، میثاق بین‌المللی حقوق مدنی و سیاسی ۱۹۶۶ و ماده ۱۱ کنوانسیون آمریکایی حقوق بشر مورد تأکید و حمایت قرار گرفته؛ که نقض آن ممکن است به دلیل عملیات سایبری و یا بهره‌گیری از ظرفیت‌های فضای سایبر رخ دهد. مفهوم «ازندگی خصوصی»^{۱۷}، همان‌طور که در ماده ۸ کنوانسیون اروپایی در مورد حمایت از حقوق بشر و آزادی های اساسی تفسیر شده است، گسترده است و ممکن است به طور کامل تعریف نشود. مفهوم استقلال شخصی ممکن است جنبه‌های

^{۱۴} می‌توان «ترولینگ» (Trolling) را در مجموع، به معنای نقض آگاهانه قوانین، قواعد و مقررات، عرف و رویه‌های جاری در فضاهای مجازی با هدف تحریک احساسات کاربران و انجام هر نوع واکنش منجر به جدل، مناقشه و درگیری در تالارهای گفتگو، چت و... دانست. در دنیای واقعی، بیشتر آدم‌هایی که مرتکب کجروی می‌شوند و یا اینکه مباحث را جدی نمی‌گیرند، نوعاً خصیصه ذاتی خود را بروز می‌دهند اما در دنیای مجازی به دلیل پنهان ماندن هویت آدم‌ها، این موضوع ممکن است اندکی تقادیر داشته باشد؛ یعنی افرادی با خصایص ظاهری خوب، در نقش یک فرد کجرو یا قانون شکن ظاهر شده و به اصطلاح عمل «ترولینگ» را انجام می‌دهند.

^{۱۵} Social Credit

^{۱۶} Yitu

^{۱۷} Private Life

زیادی از هویت فیزیکی، اجتماعی و فردی فرد را در برگیرد و باید هدف اصلی از حفظ این حق بشری حمایت از یک فرد در برابر مداخله یا داوری مقامات دولتی باشد و دولت‌ها را موظف کند که از چنین دخالتی خودداری کنند. علاوه بر این تعهد منفی، تعهدات مثبت دیگری نیز ممکن است وجود داشته باشد که ذاتاً با احترام مؤثر به زندگی خصوصی، حتی در حوزه روابط بین افراد مرتبط است که همگی این موارد در رویه‌ی کشورهای مذکور نقض شده است. (Katarzyna Chałubińska, 2022: 7)

۴. پنهان‌کاری و اطلاعات نادرست (نقض آزادی اطلاعات)

امروزه در طلیعه‌ی افکار حقوق بشری، فضای حاکم بر فضای سایبر نیز رنگ و لعابی دیگر یافته است و این مسائل در فضای مذکور نیز مصدق یافته‌اند؛ اما دولت‌ها اکثراً جریان آزاد اطلاعات را به جهت حمایت از منافع خاص یعنی امنیت ملی یا نظم عمومی محدود می‌نمایند. این عملکرد طی سالیان اخیر توسط برخی از کشورها در شبکه اینترنت صورت پذیرفته است و آن به این خاطر است که کشورهای دیگر فضای مجازی را با اجازه دادن به نشر مطالب ناهنجار «همچون پرونگرافی و حمایت از بعضی افکار و توهین به ادیان» تبدیل به تهدیدی جدی علیه نظم عمومی کرده‌اند و در این راستا نیز حرکت‌هایی برای تقویت قواعد بین‌المللی در سطح جهان در این باب صورت گرفته است (حسین‌پور و صابرژاد، ۱۳۹۴: ۴۰). البته این محدودیت‌ها باید منجر به نقض این حق بشری برای آحاد مردم گردد و باید بسیار مضيق تفسیر شود. در ادامه‌ی بحث به نقض این حق با استفاده از فضای سایبر و در قامت دولت‌های اقتدارگرا پرداخته شده است.

۳.۱. اخبار جعلی و اطلاعات نادرست

اصل‌اولاً دولت‌ها برای ایجاد بانک‌های اطلاعاتی و ارائه آن وارد فضای سایبر می‌شوند، اما در بسیاری از موارد این اطلاعات واقعی را نمایش نمی‌دهند. به عنوان مثال، هند که در آن تعداد کاربران «فیسبوک»^{۱۸} از ۳۰۰ میلیون نفر فراتر رفته است، خشونت ناشی از دروغ ریایش کودکان، از طریق رسانه‌های اجتماعی گسترش یافت. «واتس اپ» و سایر شبکه‌های اجتماعی منجر به مرگ ۲۴ نفر براثر خشونت اوپاشه شدند (Fernandez, 2019). در اثنای این اخبار اشتباه و شایعه‌پراکنی متأسفانه موارد کودک ریایی افزایش یافت؛ بنابراین اخبار جعلی و اطلاعات نادرست در این مورد به قاچاقچیان واقعی کودک اجازه داد تا به دلیل عدم شناسایی آن‌ها به فعالیت‌های غیرقانونی خود ادامه دهند (Jain, 2018).

۳.۲. سخنان نژادپرستانه و ترویج تنفر و تبعیض

در سال ۲۰۱۴، «گروه بین‌المللی حقوق اقلیت‌ها»^{۱۹} وضعیت اقلیت‌ها و مردم بومی جهان را منتشر کرد که مطالعات موردی ۷۰ کشور در سراسر جهان را ارائه نموده بود. این گزارش اقلیت ساکن در کشورها را بر مبنای خطرات سخنان نفرت‌انگیز و تبعیض‌هایی که با آن مواجه هستند رتبه‌بندی کرده بود. سه کشور آسیایی «میانمار»، «افغانستان» و «پاکستان» در میان ده کشور اول قرار داشتند و حتی در حال حاضر و در سال ۲۰۲۳ نیز دولت میانمار، همچنان به انتشار اطلاعات نادرست درباره مسلمانان «روهینگیا»^{۲۰} ادامه می‌دهد. در این سال‌ها «فیسبوک» توسط دولت میانمار برای انتشار اطلاعات نادرست در مورد تنش بین شهروندانش، برای تحریک خشونت علیه مردم «روهینگیا» استفاده شده (Brown, 2019). و خشونت به سایر نقاط کشور گسترش یافته و کشتار مسلمانان توسط اوپاشه محلی یا گروه‌های Office for the Coordination of Humanitarian Affairs Rohingya, 2018 انجام گردیده است (Seiff, 2014).

و دولت حاکم بر این کشور به پاکسازی قومی متهم شده است.

«روهینگیایی‌ها» که اغلب تحت تعقیب‌ترین اقلیت جهان نامیده می‌شوند، در معرض نقض مداوم حقوق بشر، از جمله پاکسازی قومی، بی تابعیتی و احتمالاً حتی نسل‌کشی قرار گرفته‌اند (Khaled, 2021). که این موارد در بستر فضای سایبر رهبری می‌گردد. با ارائه

^{۱۸} Facebook

^{۱۹} Minority Rights Group International (MRG)

^{۲۰} Rohingya People

سیاست‌های تنیبیهی که در فضای سایبر بسط و گسترش یافته‌اند، «روهینگیاها» به طور قاطع‌انه از طیف وسیعی از حقوق اساسی توسط دولت میانمار محروم شده‌اند، از جمله آزادی رفت‌وآمد، حقوق آموزش، امکانات بهداشتی اولیه، داشتن خانواده، ازدواج و اشتغال (Uddin, 2020). پاکسازی قومی و آزار و اذیت روهینگیاها در میانمار و سلب تابعیت آن‌ها (بی تابعیت کردن آن‌ها) استراتژی سیاسی رژیم‌های نظامی متواتی بوده است که با استفاده از ظرفیت‌های این فضاهای همراهی شده و امروزه، اکثریت قریب به اتفاق نزدیک به سه میلیون «روهینگیا»، عمده‌تاً در کشورهای همسایه بنگلادش، مالزی، هند و تایلند و همچنین در مناطق مختلف اروپا، استرالیا و آمریکای شمالی آواره هستند.

در پاکستان مفهوم آزادی مذهب و عقیده حساس و پیچیده است. گروه‌های مذهبی اقلیت در پاکستان نه تنها از تبعیض نهادینه شده رنج می‌برند، بلکه از تعصی که از طریق فضای سایبر پخش می‌شود نیز در عذاب‌اند. در آوریل ۲۰۱۸، دولت پاکستان گزارشی در مورد افراد تحت تعقیب فرقه «اقلیت احمدی»^{۱۱} منتشر نمود؛ که نشان می‌داد چگونه اعضای این فرقه مذهبی به طور مداوم توسط دولت هدف قرار می‌گیرند. احمدی‌ها از اینکه خود را مسلمان بخوانند یا از نمادهای اسلامی در اعمال مذهبی خود استفاده کنند منع شده‌اند. این گزارش نشان می‌دهد که ۷۷ احمدی بر اساس قوانین مذهبی تبعیض آمیز در سال ۲۰۱۷ محاکوم شدند که ۹ نفر از آن‌ها در زندان محبوس هستند، در حالی که چهار نفر دیگر در جرائم ناشی از نفرت در سراسر کشور به قتل رسیده‌اند. همچنین، تحقیقات نشان می‌دهد که تا سال ۲۰۱۸ میلادی رسانه‌های پاکستان ۳۹۳۶ گزارش خبری و ۵۳۲ سرمهقاله را منتشر کردند که حاوی تبلیغات نفرت علیه احمدی‌ها بوده است (Ahmadi Pakistan's, 2018).

۴. نقض آزادی بیان، دستگیری و بازداشت خودسرانه

همان‌گونه که قبل از گردید فضای سایبر تیغ دو لبه‌ای است که از یکسو موجب ترویج حقوق بشر شده و از سوی دیگر عرصه‌ای است برای نقض حقوق بشر (ضیائی، ۱۳۹۶: ۷۹). در همین راستا یکی از این حقوق اساسی که توسط دولت‌های اقتدارگرا مورد تجاوز قرار می‌گیرد حق آزادی بیان سایبری است که تعرض بدان به انحصار گوناگون انجام می‌پذیرد.

استفاده از هوش مصنوعی در نظرات بر فضای سایبر، بر آزادی بیان تأثیر وحشتناکی دارد. نظرات شباهه‌روزی بر شهروندان، این احتمال را افزایش می‌دهد که مردم از حقوق اساسی اولیه خود محروم گردند. امروزه دشوار است که ربات‌های دیجیتال القاشه با هوش مصنوعی از کاربران واقعی تفکیک گردد و برای همین افراد از اینکه نظری را ابراز دارند خودداری می‌نمایند. در بسیاری از انتخابات اخیر در سرتاسر جهان، احزاب سیاسی از هوش مصنوعی برای ایجاد و انتشار اطلاعات نادرست در مورد رقبای سیاسی خود استفاده نموده‌اند و این امر دموکراسی را تهدید می‌کند.

۱.۴. مهندسی افکار عمومی

سریازان سایبری «ارتش ترول‌ها»^{۱۲}، استراتژی جدید دولت‌ها برای کنترل مردم از طریق شکل دادن به افکار عمومی آنان هستند برای نمونه دولت فیلیپین در زمان حاضر و تحت ریاست جمهوری «دوترته»^{۱۳} به عنوان یکی از کشورهایی شناخته می‌شود که از «ارتش صفحه کلید»^{۱۴} استفاده می‌کند (Palatino, 2017). «ارتش صفحه کلید» فیلیپین با سه روش درزمنهای مهندسی افکار عمومی و نقض آزادی بیان، عمل نموده است:

^{۱۱} Ahmadi Minority

^{۱۲} ارتش ترول (Troll Army) یا اویاش مجازی در گفتمان اینترنتی به افرادی گفته می‌شود که با رفتار مخرب در فضای وب به دنبال جلب نظر کاربران، ایجاد تشنج و بیان مطالب تحریک‌کننده و توهین‌آمیز هستند. یک ترول، فردی است که در اتفاق‌های گفتگو، تالارها، وب نوشتها یا تارنامه‌های کاربر-محور پیام‌هایی ارسال می‌کند که حاوی مطالب ناراحت‌کننده یا جنجال‌برانگیز است. در حالی که در یک جمع اینترنتی کاربرانی با حسن نیت بحثی را دنبال می‌کند، اویاش اینترنتی با تحریک سایرین و با پیش کشیدن بحث‌های نامریوط یا توهین‌آمیز، به دنبال مطرح کردن خود و متشنج کردن فضای گفتگو هستند. نگاه کنید به: <http://www.straightdope.com/columns/read/1764/what-is-a-troll>

^{۱۳} Rodrigo Roa Duterte

^{۱۴} keyboard Army



اول، این ارتشن در طول فرآیند انتخابات از «دوترته» حمایت نموده است. بسیاری از پلتفرم‌های خبری بیان می‌کنند که «دوترته» از «فیس بوک» به عنوان سلاحی برای حمایت از خود و آزار و اذیت مخالفانش استفاده کرده (Stevenson, 2019). که ارتشن موردنظر سایبری از ۴۰۰ تا ۵۰۰ نفر در طول مبارزات انتخاباتی ریاست جمهوری در سال ۲۰۱۶ تشکیل شده بود و با استفاده از حساب‌های واقعی و جعلی «فیس بوک» پیام‌هایی را برای کمپین ایجاد و توزیع می‌کرد. درنتیجه، «دوترته» یک ماه قبل از رأی‌گیری بر گفتگوهای سیاسی مسلط شده بود (Etter, 2017).

دوم، سیاست‌های جنگ مواد مخدّر که از سال ۲۰۱۶ تاکنون بیش از بیست هزار نفر را کشته داده است، توسط «ارتشن ترول‌ها» حمایت می‌شود. اخباری که ادعا می‌نمایند «پاپ فرانسیس»^{۲۵} سیاست جنگ مواد مخدّر را در اجلاس واتیکان اعلام نموده است، هزاران بار در فیس بوک توسط حساب‌های طرفدار «دوترته» به اشتراک گذاشته شده است (Etter, 2017). و از آنجایی که اکثریت جمعیت فیلیپین کاتولیک بوده و پاپ شدیداً مورد احترام است منجر به تبعیت افراد و کشت و کشتار گردیده، درحالی که پاپ هرگز به جنگ با مواد مخدّر اشاره‌ای نکرده است.

در نهایت، «ارتشن ترول‌ها» برای حمایت از «دوترته» اخبار نفرت تولید می‌کنند. یکی از نمونه‌ها دستگیری روزنامه‌نگار «ماریا رسما»^{۲۶} است که از دولت «دوترته» انتقاد کرده بود (Riley & Pradhan, 2018). از مارس سال ۲۰۱۹، این روزنامه‌نگار سه بار دستگیر شده است؛ اذعان داشته که حملات به او پس از اینکه «рапلر»^{۲۷} نحوه دست‌کاری طرفداران «دوترته» در فیس بوک را منتشر کرد، افزایش یافته است و دولت علناً اعلام کرد که «рапلر» یک رسانه خارجی است که قصد خرابکاری دارد و «ماریا رسما» یک بازیگر خارجی است (Buan, 2019).

۲.۴. قطع کردن ارتباطات

قطع کردن ارتباط و نتیجتاً محدود کردن آزادی بیان و مشارکت، حمایت از حقوق بشر را مختل می‌کند. در دسامبر ۲۰۱۸، دولت «بنگلادش»^{۲۸} «فیس بوک» و سایر رسانه‌های اجتماعی و همچنین سرویس داده تلفن همراه «نسل سوم»^{۲۹} و «نسل چهارم»^{۳۰} را در طول انتخابات غیرمعمول مجلس خود مسدود کرد (Taye, 2019). علاوه بر این، در همان زمان، دولت در جریان اعتراضات دانشجویی پهنه‌ای اتصال اینترنت را بسیار پایین آورده و «اسکایپ»^{۳۱} را مسدود نمود. در ۵ آگوست ۲۰۱۸، سایت «نت بلاک»^{۳۲} توبیت کرد که اختلال‌های اینترنت امروز در سراسر بنگلادش، به ویژه در «دакا»^{۳۳} و اطراف آن تشدید شده و داده‌ها نشان می‌دهند که مسدود کردن به موقع، هدفمند و موضوعی در پاسخ به اعتراض، تهدیدکننده آزادی مطبوعات و امنیت است (Netblocks, 2018). بی‌تردید چنین کاری و ارتباطات آهسته در فضای سایبر به طور غیرمستقیم مشارکت مردم را در روند دموکراسی سازی کاهش می‌دهد.

در نمونه‌ای دیگر از قطع نمودن اینترنت جهت اطلاع‌رسانی نادرست و فریبکاری در «سریلانکا»، چند ساعت پس از بمب‌گذاری سال ۲۰۱۹ در روز یکشنبه عید پاک که در آن ۳۰۰ نفر کشته و بسیاری زخمی شدند، دولت اینترنت، از جمله «فیس بوک»، «توییتر»^{۳۴} و «واایبر»^{۳۵} را قطع کرد؛ البته شکی نیست که بمب‌گذاری سریالی و حشت ایجاد کرد و فیس بوک نتوانست اطلاعات نادرست را پالایه کند. همچنین خانواده‌هایی که به دنبال اعضای خود بودند با مشکلاتی مواجه شدند. با این حال، برخی افراد از این استراتژی حمایت نموده

^{۲۵} Franciscus

^{۲۶} Maria Ressa

^{۲۷} Rappler

^{۲۸} 3G is the third generation of wireless mobile telecommunications technology

^{۲۹} 4G is the fourth generation of broadband cellular network technology

^{۳۰} Skype

^{۳۱} NetBlock.org

^{۳۲} Dhaka

^{۳۳} Twitter

^{۳۴} YouTube

^{۳۵} Viber Messenger

و یکی از مقامات ارشد دولت سریلانکا بیان داشت که «کاری که دولت سریلانکا انجام داده مستبدانه بود، اما احتمالاً همان کاری است که باید انجام می‌شد تا بعدازآن اتفاق رسانه‌های اجتماعی نتوانند وضعیت را بدتر نمایند» (Tortermvasana, 2018).

در اقدامی مشابه در ماه مه ۲۰۱۹، دولت «اندونزی» سرعت اینترنت و شبکه رسانه‌های اجتماعی را کاهش داد و ارسال تصاویر و ویدئوها را برای جلوگیری از گسترش اطلاعات دروغین درباره تظاهرات خشونت‌آمیز که در آن هشت نفر کشته شدند، محدود کرد. حامیان «پرابوو»^{۳۶}، نامزد ریاست جمهوری که در انتخابات شکست خورده بود، تظاهراتی برپا کرده بودند. کمیسیون ملی انتخابات «جوکووی»^{۳۷} را برندۀ اعلام کرده بود که منجر به اعتراض گروه‌های مخالف گردیده بود. در مورد اینکه چه کسی معتبرضان را کشته است، اختلاف نظر وجود داشت که درنتیجه مشخص نبود چه کسی باید مسئول شناخته شود (Amnesty International Indonesia, 2019). برای توقف تنش‌ها، دولت اینترنت را قطع کرد که از منظر محدود کردن آزادی اطلاعات نادرست بود. علاوه بر این، دولت نه گزارشی در مورد نقض حقوق بشر در رابطه با تظاهرات ارائه کرد و نه برای توجیه تعطیلی آن دلیلی آورد.

۳.۴. دستگیری و بازداشت

یکی دیگر از محدودیت‌های اعمال شده توسط دولت‌های اقتدارگرا برای آزادی بیان در فضای سایبر، دستگیری و بازداشت هست. محدودیت‌های قبلی تأثیر غیرمستقیم بر حقوق مشارکت مدافعان حقوق بشر از طریق حذف محتوا و سوءاستفاده از اطلاعات را تشريح می‌کند، اما این بخش تأثیر مستقیمی که توسط بازیگران دولتی و غیردولتی بر زندگی مدافعان حقوق بشر، روزنامه‌نگاران و متقدان رسانه‌ای از طریق دستگیری، بازداشت، بستن دهان یا قتل ایجاد می‌شود را موربدیت قرار می‌دهد.

پاکستان به عنوان چهارمین کشور خطرناک جهان برای خبرنگاران که از سال ۱۹۹۰ تا ۲۰۱۹، کشته شدن ۱۱۵ خبرنگار در آن گزارش شده (Baloch & Qammar, 2019). محدودیت بسیاری بر فضای سایبر اعمال می‌نماید که درنتیجه آن بسیاری از فعالان و خبرنگاران بازداشت، دستگیر و حتی ترور می‌شوند. در ژانویه ۲۰۱۷، دفتر «کمیسarıای عالی حقوق بشر»^{۳۸} گزارش داد که چهار فعال رسانه‌ای اجتماعی و حقوق بشر به نام‌های «وقاص گورایا»^{۳۹}، «عاصم سعید»^{۴۰}، «سلمان حیدر»^{۴۱} و «احمد رضا نصیر»^{۴۲} به جرم توهین به مقدسات متهم شده‌اند که مجازات بسیار سنگینی در پاکستان دارد (Kaye, 2017). اما درواقع این فعالان شبکه‌های اجتماعی به دلیل انتقاد از دولت پاکستان دستگیر شده بودند. در پی ناپدید شدن این فعالان و سایر موارد توهین آمیز در رسانه‌های آنلاین، اداره مخابرات پاکستان که اصلی‌ترین کanal ارتباطی در پاکستان است، شروع به ارسال پیام‌های هشداری با محتویات اینکه «آپلود و به اشتراک‌گذاری محتوا توھین آمیز در اینترنت یک جرم قابل مجازات است» (Human Rights Watch, 2018). به میلیون‌ها نفر از مشترکان تلفن همراه خود کرد و با یاری جستن از همین موضوع، محدودیت‌های مشارکت سیاسی را با راهاندازی کمپین‌های رسانه‌ای در مورد افرادی که جرئت ابراز هرگونه عقیده سیاسی یا مذهبی دارند را تشدید نمود (Digital Rights Foundation, 2018). بی‌تردید عملکرد دولت پاکستان به عنوان مصدقه بازی از یک دولت اقتدارگرا به نقض حق بر آزادی بیان در فضای سایبر انجامیده است، که در آن افراد نمی‌توانند آزادانه دیدگاه‌ها و نظرات خود را در مورد موضوعاتی که دولت معتقد است جرم هستند، بیان نمایند.

نمونه‌ی دیگری از عملکرد کشورهای اقتدارگرا در این زمینه، اقدام دولت «لائوس»^{۴۳} هست؛ در این کشور فعالان و متقدان دستگیر و بازداشت شده‌اند، اقلیتی تک‌حزبی کنترل مطلق بر رسانه‌ها را در دست دارد و در فهرست جهانی آزادی مطبوعات در سال ۲۰۱۹، رتبه بسیار پایین ۱۷۱ را دارد (Reporters Without Borders, 2019).

^{۳۶} Prabowo

^{۳۷} Jokowi

^{۳۸} Office of the United Nations High Commissioner for Human Rights(OHCHR)

^{۳۹} Waqas Goraya

^{۴۰} Asim Saeed

^{۴۱} Salman Haider

^{۴۲} Ahmed Raza Naseer

^{۴۳} Laos

حساب‌های رسانه‌های اجتماعی خود از طریق نظرات و پست‌های «فیسبوک» دستگیر شدند (Jha, 2016). در مرحله‌ی قانون‌گذاری نیز در کشور «لائوس» فرمان موسوم به «آزادی اینترنت»^{۴۴} در سال ۲۰۱۴ اشعار می‌دارد هرکسی که «نظر منفی»^{۴۵} علیه دولت در شبکه‌های اجتماعی ارائه دهد، می‌تواند دستگیر یا زندانی شود. در نمونه‌ای دیگر در کشور «کامبوج»^{۴۶}، یک کاربر جوان رسانه‌های اجتماعی به نام «هنگ لیخنا»^۷، در ژوئیه ۲۰۱۷ به دلیل اشتراک‌گذاری یک ویدیو در حساب «فیسبوک» خود دستگیر شد. این ویدئو حاکی از آن بود که «هون سن»^۸—نخست‌وزیر و خانواده‌اش در قتل یک تحلیلگر و محقق سیاسی برجسته به نام «کیم لی»^۹، در سال ۲۰۱۶ میلادی دست داشته‌اند (Radio Free Asia, 2017).

نتیجه‌گیری

با توجه به آنچه تحلیل آن گذشت می‌توان بیان داشت بسیاری از دولت‌های اقتدارگرا از فناوری‌های اطلاعات و ارتباطات در بستر فضای سایبر برای تجاوز به حریم خصوصی، نقض حق بر آزادی اطلاعات و انتشار اطلاعات نادرست، محدود کردن حق بر آزادی بیان و مشارکت سیاسی بهره می‌جویند و در این راستا از ابزارهای خاص فضای مذکور نیز استفاده می‌نمایند که نمونه بارز آن تمسک به «ارتشر ترول‌ها» می‌باشد؛ مانند مورد فیلیپین در زمان «دوتره» که جهت مهندسی افکار عمومی مردم و برای ایجاد محظای حمایت‌کننده از دولت و سرنوشت متقدان، از این ابزار استفاده شده است. ابزار دیگر دولت‌های اقتدارگرا در این زمینه استفاده از راهکار قطع ارتباط سایبری است که در کشورهایی همچون «سریلانکا» و «اندونزی» قطع شدن اینترنت برای جلوگیری از اطلاعات نادرست در مورد انتخابات نقش نامطلوبی بر حمایت از حقوق بشر ایفا نموده است. مسدود کردن و حذف محتوا به عنوان موانعی برای مدافعان حقوق بشر است در صورتی که دول اقتدارگرا در بستر فضای سایبر به کرات به آن اقدام می‌نمایند. از طرفی آن‌گونه که به صورت مورد کاوی مورداشارة قرار گرفت کشورهای «میانمار» و «پاکستان» از نظر گسترش سختان نفرت‌انگیز، نژادپرستی و تبعیض در فضای سایبر در رتبه‌های بالایی قرار دارند و متقدان، از جمله فعالان حقوق بشر و روزنامه‌نگاران، به دلیل عقایدشان در کشورهای آسیب‌دیده از تروریسم، مانند پاکستان، با دستگیری، بازداشت یا حتی قتل‌های فراقانونی مواجه می‌شوند. بی‌تردید می‌توان گفت تصور بیان‌شده در مقدمه‌ی مقاله حاضر که برداشتی از کتاب ۱۹۸۴ «جرج اورول»^۵ بود و ترسیم کننده وقایعی وحشتناک، تهدیدآمیز و ناپسند است؛ امروز پس از گذشت ۷۰ سال، به طور محسوسی به واقعیت تبدیل شده است. فناوری‌های جدید که می‌توانستند ابزار مغایدی در پیشبرد حقوق بشر باشند، در تملک برخی سیاستمداران تبدیل به تهدیدی جدید برای حقوق و آزادی‌های اساسی بشری شده‌اند.

از سوی دیگر بررسی موارد مطروحه در متن مقاله‌ی حاضر نشان می‌دهد که تشخیص مبنی بر هوش مصنوعی می‌تواند برای محدود کردن و ممانعت از مشارکت سیاسی، از جمله با شناسایی و دلسرد کردن گروههای خاصی از مردم استفاده شود. قدرت پیش‌بینی هوش مصنوعی که در حال حاضر برای پیش‌بینی و کمک به جلوگیری از درگیری‌های مسلحانه استفاده می‌شود، اگر همین رویکرد بتواند پیشگیرانه توسط دولتها برای پیش‌بینی و جلوگیری از تظاهرات یا اعتراضات عمومی قبل از وقوع آن‌ها استفاده شود، ضربه مهمی به حق اعتراض و مخالفت علیه دولت خواهد بود. از همین رو پیشنهاد می‌گردد که جامعه بین‌المللی با ظرفیت‌های موجود (به طور خاص سازمان ملل متحد)، در راستای انتظام به این موضوع در قالب معاهده‌ی بین‌المللی اقدام نماید.

^{۴۴} Internet Freedom

^{۴۵} Negatively Comment

^{۴۶} Cambodia

^۷ Heng Leakhena

^۸ Hun Sen

^۹ Kem Ley

^۵ اریک آرتور بلر (Eric Arthur Blair) با نام مستعار جرج اورول (George Orwell) داستان‌نویس، روزنامه‌نگار، متقد ادبی و شاعر انگلیسی بود (۱۹۰۳ تا ۱۹۵۰). او بیشتر برای دو رمان سرشناس و پرفروش «مزرعه حیوانات» که در ۱۹۴۵ منتشر شد و در اواخر دهه ۱۹۵۰ به شهرت رسید و نیز رمان «۱۹۸۴» شناخته می‌شود. این دو کتاب بر روی هم بیش از هر دو کتاب دیگری از یک نویسنده‌ی قرن بیستمی، فروش داشته‌اند (Rodden, 2007: 10).

منابع

- پورقهرمانی، بابک و صابر نژاد، علی. (۱۳۹۴). حریم خصوصی در فضای سایبر از منظر حقوق بین‌الملل، چاپ اول، تهران: انتشارات مجد.
- حبیب زاده، طاهر. (۱۳۹۰). حقوق فناوری اطلاعات مقدمه‌ای بر حقوق تجارت الکترونیک، چاپ اول، تهران: انتشارات مرکز پژوهش‌های مجلس.
- حسین‌پور، پری و صابر نژاد، علی. (۱۳۹۴). آزادی اطلاعات در فضای سایبر از منظر حقوق بین‌الملل، چاپ اول، تهران: انتشارات مجد.
- صابر نژاد، علی و حسین‌پور، پری. (۱۳۹۶). «تحلیل حقوقی گونه شناسی نقض حریم خصوصی در فضای سایبر»، فصلنامه جستارهای حقوق عمومی دوره ۱، شماره ۳.
- ضیائی، یاسر. (۱۳۹۶). «حمایت از حقوق بشر در فضای سایبر»، فصلنامه پژوهش‌های حقوقی، دوره ۱۶، شماره ۳۱.
- متقی، ابراهیم و جباری، محمدحسین. (۱۴۰۱). «دولت اقتدارگرا و گذار به دمکراسی در چین»، فصلنامه رهیافت‌های سیاسی و بین‌المللی، دوره ۱۳، شماره ۶۹.
- Ahmadi Pakistan's. (2018). ‘Ahmadi community faces persecution, hate crime: Report’ Hindustan Times 28 April, available at <https://www.hindustantimes.com/world-news/pakistan-s-ahmadi-community-faces-persecution-hate-crime-report/story-AuTwmNKaYA63pQwHqrX7oK.html>.[last visited: 20 may 2022]
- Amnesty International Indonesia. (2019). ‘Penjelasan polri terkait kekerasan 21-23 Mei mengecewakan keluarga korban tewas’ (Explanation from national police is disappointing the families’ victims of protest on 21-23 May), <https://www.amnestyindonesia.org/penjelasan-polri-terkait-kekerasan-21-23-mei-mengecewakan-keluarga-korban-tewas>.[last visited: 25 may 2022]
- Ang, Yuen Yuen. (2018). ‘Autocracy with Chinese characteristics’ Foreign Affairs May/June, available at <https://www.foreignaffairs.com/articles/asia/2018-04-16/autocracychinese-characteristics>.[last visited: 20 may 2022]
- Baloch, Hasnain & Qammar,Nassen. (2019). ‘A danger of digital surveillance. Bytes for all publications’ (nd), available at <https://content.bytesforall.pk/publication/dangers-digital-surveillance>> [last visited: 25 may 2022]
- Brown, Nicola & Liar, liar. (2019). platforms on fire: The rise of misinformation and what to do about it’ The SpinOff. InternetNZ, 4 February, available at <https://the spinoff.co.nz/partner/internetnz/04-02-2019/liar-liar-platforms-on-fire-the-riseof-misinformation-and-what-to-do-about-it/>.[last visited: 20 may 2022]
- Buan, Manila. (2019). ‘Maria Ressa arrested at NAIA over anti-dummy law’ Rappler.com 29 March, available at <https://www.rappler.com/nation/226880-maria-rezza-arrestednaia-anti-dummy-law-case-march-29-2019>.[last visited: 25 may 2022]
- Clark, Anthony, Mahesti Hasanah and Numfon K Jaiwon. (2017). ‘An uptake in communications encryption is tempered by increasing pressure on major platform providers; governments expand content restriction tactics’ The Shifting Landscape of Global Internet Censorship. Internet Monitor 29 June, available at <https://thenetmonitor.org/research/2017-globalinternet-censorship>.[last visited: 20 may 2022]
- Digital Rights Foundation. (2018). ‘Content regulation in Pakistan’s digital spaces’,Human Rights Council Report, Digital Rights Foundation, available at <https://digitalrightsfoundation.pk/wp-content/uploads/2017/12/DigitalRightsFoundationSubmissionSpecialRapporteurFreedomofExpression.pdf>.[last visited:25 may 2022]
- Etter Lauren. (2017). ‘What happens when the government uses Facebook as a weapon?’Bloomberg.com 7 December, available at <https://www.bloomberg.com/news/features/2017-12-07/how-rodrigo-duterte-turned-facebook-into-a-weaponwith-a-little-help-from-facebook>.[last visited: 25 may 2022]
- Fernandez Borja. (2019). ‘Fake news in Asian politics’ Global Risk Insights 1 April, available at <https://globalriskinsights.com/2019/04/fake-news-in-asian-politics/>.[last visited: 20 may 2022]
- Freedom House. (2018). ‘The rise of digital authoritarianism’ Freedom House, available at https://freedomhouse.org/sites/default/files/FOTN_2018_Final%20Booklet_11_1_2018.[last visited: 25 may 2022]
- Glasius, Marlies. (2018). ‘What authoritarianism is ... and is not: A practice perspective’, 94 International Affairs 515, available at <https://academic.oup.com/ia/article/94/3/515/4992409>.[last visited:25 may 2022]



- Glasius, Marlies & Michaelsen, M. (2018). Illiberal and Authoritarian Practices in the Digital Sphere: Prologue. International Journal of Communication: IJoC, 12, 3795–3813.
- Halpin, Erfel & Hick, Stiven. (2000). ‘Information: An essential tool for human rights work’ in Hick, EF Halpin & E Hoskins (eds) Human rights and the internet London: Macmillan Press
- Hintz, Arne & Milan, Stefania. (2018). ‘through a glass, darkly: Everyday acts of authoritarianism in the liberal West’, International Journal of Communication, No.12:3939–3959
- Human Rights Watch ‘Pakistan Events of 2017’. (2018). available at <https://www.hrw.org/world-report/2018/country-chapters/pakistan>.[last visited: 25 may 2022]
- Jain,Dwivedi. (2018). ‘The rising trend of child abductions in India’ Live Mint Online 11 July. Available at <https://www.livemint.com/Politics/Bv4TbeToCpVS9j4IX3hJjN/The-rising-trend-of-child-abductions-in-India.htm>.[last visited: 25 may 2022]
- Jha,Philip. (2016). ‘Laos cracks down on social media critics’ Al Jazeera 6 June, available at <https://www.aljazeera.com/news/2016/06/laos-cracks-social-media-critics> 160606092251543. [Last visited: 25 may 2022]
- Katarzyna Chałubińska. (2022). Operations in Cyberspace vs Human Rights and Freedoms, Polish Political science Yearbook, vol. 5
- Khaled, Afkham. (2021). Do no harm in refugee humanitarian aid: the case of the Rohingya humanitarian response. *J Int Humanit Action* 6(1)
- Kaye, Donald. (2017). ‘UN expert urges Pakistan to locate and return home four disappeared rights and social media activists’ OHCHR News 11 January, available at <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21074>.[last visited:25 may 2022]
- Linz, Joe. (2000). Totalitarianism and authoritarianism Boulder: Lynne Rienner,Publishers Inc
- Lucas,Licol & Feng, Xiang. (2018). ‘Inside China’s surveillance state’ Financial Times 20 July, available at <https://www.ft.com/content/2182eebe-8a17-11e8-bf9e-8771d5404543>.[last visited:25 may 2022]
- Ma, Ayo. (2018). ‘China has started ranking citizens with a creepy “social credit” system:Here's what you can do wrong, and the embarrassing, demeaning ways they can punish you’ Business Insider 29 October, available at <https://www.businessinsider.com/china-social-credit-system-punishments-and-rewardsexplained-2018-4>.[last visited:20 may 2022]
- Marr, Bhupati. (2019). ‘Chinese social credit score: Utopian big data bliss or black mirror on steroids?’ Forbes Online 21 January, available at <https://www.forbes.com/sites/bernardmarr/2019/01/21/chinese-social-credit-score-utopian-big-data-blissor-black-mirror-on-steroids/#741c3a2>.[last visited: 20 may 2022]
- Mayer, Snowden. (2018). ‘China steps up internet surveillance by recording user activities’ CPO Magazine Online News 19 December, available at <https://www.cpomagazine.com/data-privacy/china-steps-up-internet-surveillance-by-recording-useractivities/>.[last visited: 25 may 2022]
- Mirzazadeh,Iman. (2023), Artificial Intelligence (AI) and Violation of Human Rights, Stockholm University
- Murakami Wood, D. (2017). Editorial: The Global Turn toAuthoritarianism and after. *Surveillance & Society*15 (3/4): 357-370.
- Net blocks. (2018).‘Mobile internet speeds restricted in Bangladesh amid student protest’ Netblocks.org 4 August, available at <https://netblocks.org/reports/bangladesh-internet-shutdown-student-protests-jDA37KAW>.[last visited: 25 may 2022]
- Nilsen, Alf Gunvald. (2018). ‘An authoritarian India is beginning to emerge’ The Wire 31 August, available at <https://thewire.in/politics/an-authoritarian-india-is-beginningto-emerge>.[last visited: 25 may 2022]
- Office for the Coordination of Humanitarian Affairs Rohingya refugee crisis United Nations Office for the Coordination of Humanitarian Affairs 29 August. (2018). available at <https://www.unocha.org/rohingya-refugee-crisis>.[last visited:20 may 2022]
- Palatino, Rodrigo. (2017). ‘Beware Duterte’s troll army in the Philippines’ Thediplomat.com18 November, available at <https://thediplomat.com/2017/11/beware-dutertes-troll-army-in-the-philippines/>.[last visited: 25 may 2022]



- Radio Free Asia. (2017). ‘Young Cambodian arrested for derogatory comments about Hun Sen on social media’ Radio Free Asia 13 July, available at <https://www.refworld.org/topic,50ffbce582,50ffbce58e,5a0f01d64,0,KHM.html>.[last visited: 22 may 2022]
- Reporters without Borders. (2019). ‘Laos: No light under the tunnel’ Reporters without Borders for Freedom of Information, available at <https://rsf.org/en/laos>.[last visited: 25 may 2022]
- Riley, Michael & Pradhan, Boe. (2018). ‘A global guide to state-sponsored trolling’ Bloomberg.com 19 July, available at <https://www.bloomberg.com/features/2018-government-sponsored-cyber-militia-cookbook/>.[last visited: 25 may 2022]
- Rodden, John. (2007). *The Cambridge companion to George Orwell*. Cambridge University Press
- Ruijgrok, Koen. (2016). ‘From the web to the streets: Internet and protests under authoritarian regimes’, *Democratization*, No.24:3, 498-520
- Santos, Vonywer. (2018). ‘The Philippines just became more authoritarian, thanks to the people’ *The New York Times* 24 May, available at <https://www.nytimes.com/2019/05/24/opinion/philippines-duterte-election-senate.html>.[last visited: 24 may 2022]
- Seiff, Abby. (2014). ‘Hate crime, racism on the rise in Southeast Asia’ UCA News.com 3 July, available at <https://www.ucanews.com/news/hate-crime-racism-on-the-rise-in-southeast-asia/71321>.[last visited: 24 may 2022]
- Stevenson, Ashly(2019). ‘Maria Ressa, journalist critical of Duterte, is arrested again in Philippines’ *The New York Times* 28 March, available at <https://www.nytimes.com/2019/03/28/business/media/maria-rezza-arrestedphilippinesrappler.html>.[last visited: 23 ma y 2022]
- Tan, Cika. (2018). ‘Malaysian police adopt Chinese AI surveillance technology’ *Nikkei Asian Review* 18 April, available at <https://asia.nikkei.com/Business/Companies/Chinas-startup-supplies-AI-backed-wearable-cameras-to-Malaysian-police>.[last visited: 23 may 2022]
- Taye, Berhan. (2019). ‘Sudan, Bangladesh, DRC, Gabon start 2019 with major digital rights violations’ Accesnow.org 10 January, available at <https://www.accessnow.org/sudan-bangladesh-drc-gabon-start-2019-with-major-digital-rightsviolations/>.[last visited:23 may 2022]
- Tortermvasana K. (2018). ‘Cybersecurity ASEAN course set for June’ Bangkok Post 30 March, available at <https://www.bangkokpost.com/world/1437530/cybersecurity-asean-course-set-for-june>.[last visited:23 may 2022]
- Uddin, Nasir. (2020) *The Rohingya an ethnography of ‘Subhuman’ Life*. Oxford University Press, New Delhi
- Xueying, Neao. (2018). ‘Many people refused to accept military service into the blacklist of credit information’ Beijing News 19 March, available at <http://www.bjnews.com.cn/news/2018/03/19/479533.html>.[last visited: 23 may 2022]