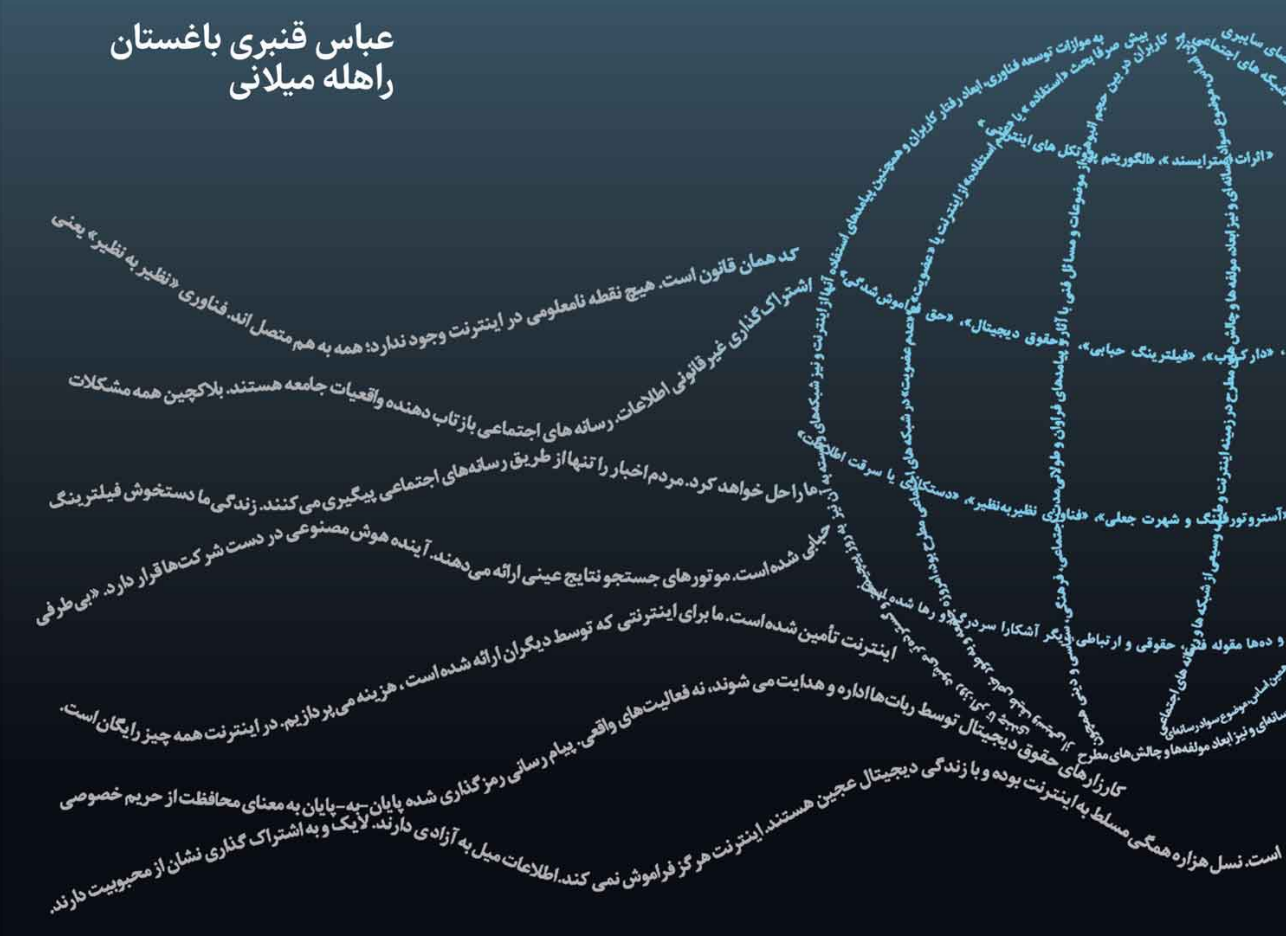
مرکز ملی فضای مجازی
انتشارات پژوهشگاه فضای مجازی

سواد رسانه‌ای و نگاه انتقادی

حقیقت دربارهٔ ۵۰ اسطورهٔ اینترنت

مترجمان
عباس قنبری باغستان
راهله میلانی



سواد رسانه‌ای و نگاه انتقادی

حقیقت درباره ۵۰ اسطوره اینترنت

ویراستارها

ماتیاس سی. کتمان و استفان درِیِر

مترجمان

عباس قنبری باغستان (عضو هیات علمی دانشگاه تهران)

راهله میلانی

بهار ۱۴۰۱

عنوان و نام پدیدآور	:	سواد رسانه ای و نگاه انتقادی: حقیقت درباره ۵۰ اسطوره اینترنت/ ویراستارها ماتیاس سی. کتمان و استفان دریر ؛ مترجمان عباس قنبری باغستان، راهله میلانی ؛ ویراستار مینا راستی.
مشخصات نشر	:	تهران : پژوهشگاه فضای مجازی، ۱۴۰۰
مشخصات ظاهری	:	۱۴۶ صفحه.
شابک	:	۹۷۸-۶۲۲-۹۷۷۰۰-۷-۸
وضعیت فهرست‌نویسی	:	فیپا
یاداشت	:	عنوان اصلی: . Busted! The truth about the 50 most common internet myths, ۲۰۱۹
عنوان دیگر	:	حقیقت درباره ۵۰ اسطوره اینترنت.
موضوع	:	اینترنت Internet اینترنت -- تدابیر ایمنی Internet -- Security measures فضای مجازی Cyberspace هوش مصنوعی Artificial intelligence داده‌کاوی Data mining شبکه های اجتماعی پیوسته Online social networks سواد رسانه ای Media literacy
شناسه افزوده	:	کتمان، ماتیاس سی ،. ویراستار
شناسه افزوده	:	Kettemann, Matthias C.
شناسه افزوده	:	درایر، اشتفان، ویراستار
شناسه افزوده	:	Dreyer, Stephan
شناسه افزوده	:	قنبری باغستان، عباس، ۱۳۵۷ - ، مترجم
شناسه افزوده	:	میلانی، راهله، ۱۳۶۲ - ، مترجم
شناسه افزوده	:	پژوهشگاه فضای مجازی
رده‌بندی کنگره	:	TK ۵۱۰۵/۸۷۵
رده‌بندی دیویی	:	۰۰۴/۶۷۸
شماره کتابشناسی ملی	:	۸۷۶۵۱۳۷
اطلاعات رکورد کتابشناسی	:	فیپا

مشخصات :

عنوان: سواد رسانه‌ای و نگاه انتقادی: حقیقت درباره ۵۰ اسطوره اینترنت

گردآورندگان: ماتیاس سی.کتمان، استفان دریر

مترجمان: دکتر عباس قنبری باغستان (عضو هیات علمی دانشگاه تهران)، راهله میلانی

ویراستار: مینا راستی

ناشر: انتشارات پژوهشگاه فضای مجازی

صفحه آرایی: مرضیه مرادیان

طراح جلد: مهراوه تقی‌زاده و محمدرضا قرقانی

سال و نوبت چاپ: ۱۴۰۱- اول

شابک: ۹۷۸-۶۲۲-۹۷۷۰۰-۷-۸

قیمت: ۷۰۰۰۰۰ ریال

فهرست مطالب

فصل ۳: گنجایش و ادغام

فصل ۴: زیرساخت و نوآوری

فصل ۵: داده و آشفتگی در آن

پیشگفتار ویراستاران

فرود بر ماه هرگز اتفاق نیفتاد و دروغی بیش نبود. زمین صاف است. واکسن‌ها مضر هستند. اینها اسطوره‌هایی هستند که در اینترنت با آنها مواجه می‌شویم. اما در این کتاب به بیان حقیقت درباره این قبیل اسطوره‌ها در اینترنت نخواهیم پرداخت؛ بلکه بیشتر با اسطوره‌های مرتبط با خودِ اینترنت سروکار داریم. در این راستا، به مفهوم گسترده‌ای از «اسطوره» تکیه خواهیم کرد که توسط رولان بارت[1]، نظریه‌پرداز فرهنگی تأثیرگذار فرانسوی مطرح شده است: اسطوره عبارت است از یک ساختار فرهنگی مشتمل بر حقایق جهانی که در قالب باور عمومی تجلی پیدا کرده است.

برای مثال، این‌که فعالیت‌های مردم در اینترنت قابل تنظیم و قانونمندی نمی‌باشد، اسطوره‌ای بیش نیست. این‌که پروتکل‌ها سیاسی نیستند، نیز یک اسطوره است. این ساختارهای قدرتمند واقعیت، چالش‌های حقیقی نظام‌مندسازی اینترنت را به بیراهه می‌کشانند. باوجوداینکه اینها تا حدودی حقیقت دارند (به‌طورمثال نظام‌مندسازی فعالیت‌های برخط در مقایسه با فعالیت‌های غیربرخط اغلب دشوارتر است و پروتکل‌ها در مقایسه با قوانین کمتر «سیاسی» هستند)، اما موضوع اصلی را بیش‌ازپیش مبهم می‌سازند. دقیقا به همین دلیل است که برخی از نیروها و ذی‌نفعان در حوزه سیاست‌گذاری اینترنت علاقه وافری به ترویج این اسطوره‌ها دارند.

---

1. Roland Barthes

دست‌های پنهان حوزه سیاست‌گذاری در زمینه نحوه حکمرانی اینترنت، در سایه اسطوره‌ها کمین می‌کنند. آنها همواره بر اساس اطلاعات نادرست سهوی و عمدی و همچنین باورهای غیرانتقادی گسترش می‌یابند. اعتماد به اطلاعات نادرست و باورهای غیرانتقادی به داستان‌هایی که برای خودمان تعریف می‌کنیم برای این است که دنیایی که ساخته‌ایم و فضایی که در آن زندگی می‌کنیم هر چه بیشتر برایمان قابل درک شود. از لحاظ روان‌شناختی، اسطوره‌ها به‌دلیل آنکه به نظر ملموس می‌آیند جذاب هستند. اسطوره‌ها در دوران‌های پیچیده و دشوارتر، نوعی ساده‌سازی مؤثر و کمک‌کننده در فهم مسائل به نظر می‌آیند. آنها این باور را تقویت می‌کنند که نیازی به تفکرات عمیق و پیچیده نیست، از زیر سؤال بردن وضعیت موجود دست بکشیم و فکرمان را مشغول چگونگی بهبود و توسعه درک خود نکنیم. به‌عنوان‌مثال چنانچه الگوریتم‌ها همیشه خنثی باشند، دیگر به ساختن ابزارهای هنجاری برای پاسخگو کردن شرکت‌ها و کمپانی‌های توسعه دهنده آنها نیازی نداریم. فکر نکردن، سؤال نکردن، بحث نکردن و توجه نداشتن به جزئیات همواره ساده‌تر از انجام دادن آن است.

اسطوره‌ها اغواکننده هستند. این خبر که مجرمان سایبری بدون هیچ مشکلی آزادانه به زندگی خود می‌پردازند را ممکن است جایی خوانده باشیم یا در نطق سیاست‌مداران به گوشمان خورده باشد. اما آیا واقعاً این‌طور است؟ یا شاید، آن اسطوره این حقیقت تلخ را پنهان می‌کند که مقابله با مجرمان سایبری نیازمند پیگیری‌های قانونی مناسب و عملیات پلیسی گسترده است تا ژست‌های سیاسی؟

در صورتی که موتورهای جستجو نتایج عینی ارائه دهند، دیگر به ایجاد گفتمان اجتماعی در خصوص وظایف آن دسته از اطلاعات ساختاری نیازی وجود ندارد. چنانچه مفهوم «حریم خصوصی» از بین رفته باشد، آیا باز هم لزومی دارد دغدغه نقض حریم خصوصی را داشته باشیم؟ اگر الگوریتم‌ها خنثی و بی‌طرف هستند، پس «سوگیری‌ها» و «جانبداری» دیگر معنایی ندارند.

البته در قلمرو {دولت} اینترنت همه چیز هم به‌خوبی پیش نمی‌رود. (که البته اینترنت یک قلمرو مستقل محسوب نمی‌شود، ولی همین که گفته می‌شود قوانین در فضای برخط اینترنت قابلیت تسری و اعمال ندارد نیز خود در اصل یک اسطوره بسیار قوی است.)

اسطوره‌ها نقش مهمی در فهم و درک امور دنیا دارند. بسیاری از این قبیل اسطوره‌های نوآورانه

ممکن است مفید باشند یا، تا حدودی صحیح یا حتی بر اساس باورهای دیرینه و مستحکم باشند. از نظر اقتصاد اندیشه[1]، اسطوره‌ها ممکن است به‌صورت‌جداگانه توجیه‌پذیر و قابل درک باشند. «اندیشیدن» کاری دشوار است، «اندیشیدن انتقادی» حتی دشوارتر نیز می‌باشد. اما از نظر اجتماعی، اسطوره‌ها بسیار خطرناک هستند.

بسیاری به‌طورآگاهانه اسطوره‌ها را به‌کار می‌گیرند. طبق گفته بارت[2]، «هر اسطوره وظیفه دارد توجیهی طبیعی برای یک هدف تاریخی مطرح کند و احتمال وقوع را امری جاودانه جلوه دهد». براین اساس، هر راه‌حل هنجاری برای هریک از مسائل مربوط به سیاست‌ها، خط‌ومشی‌ها و شیوه حکمرانی اینترنت[3] جهانی باید کاملاً عادی و طبیعی جلوه داده شود. در صورتی که منشأ اینترنت، حکمرانی اینترنت، نقش الگوریتم‌ها، ماهیت قانون، هنجارمندی دستورها، کثرت‌گرایی در فرهنگ‌ها و مفاهیم زندگی را دچار ابهام کنیم و به چالش بکشیم، قادر نخواهیم بود احتمالات تاریخی، وابستگی‌های فرهنگی و شرایط روابط اجتماعی را پیگیری و دنبال کنیم.

با چنین پیش‌زمینه‌ای، تصمیم گرفتیم در زمینه اسطوره‌های مربوط به اینترنت، فراخوان دهیم. مطالب زیادی به دستمان رسید و طی بررسی‌های صورت‌گرفته، ۵۰ مورد برتر را انتخاب کردیم. پر واضح است که اسطوره‌های مطرح شده در این کتاب تنها بخشی از اسطوره‌های موجود در گفتمان مربوط به «حکمرانی اینترنت» را تشکیل می‌دهند، باوجوداین، این نمونه‌ها بسیاری از مضامین کلیدی و طیف وسیعی از موضوعات گسترده مطرح شده در این حوزه را پوشش می‌دهند. همایش حکمرانی اینترنت در برلین در ۲۰۱۹، فرصتی مناسبی برای انتشار این کتاب فراهم آورد. (به‌عنوان یک اسطوره دیگر که می‌خواهیم باور داشته باشید، این همایش صرفاً محلی برای گفتگو و سخنرانی نیست.)

در واقع، با هدف تبیین و روشن ساختن گفتمان‌های مختلف در زمینه «حکمرانی اینترنت»، از میزبان همایش حکمرانی اینترنت در سال ۲۰۱۹ در برلین درخواست کمک کردیم و حمایت مالی مسئولان همایش از این ایده شایان تقدیر است.

باوجوداین، مسئولیت انتخاب و ویرایش اسطوره‌های این کتاب بر عهده خودمان بوده است.

---

1. Economy Of Thought
2. Barthes
3. Internet Governance Forum

این مسئولیت را با کمال میل بر عهده می‌گیریم چراکه اطمینان داریم تیم نویسندگان متبحر ما از بنیان‌گذاران اینترنت گرفته تا پژوهشگران نوظهور، از پزشکان و استادان گرفته تا نظریه‌پردازان و متخصصان، وظیفه شفاف‌سازی و روشنگری در زمینه اینترنت را به نحو احسن انجام داده‌اند. هدف ما تهیه یک کتاب مرجع برای تمام افرادی که با آینده اینترنت سروکار دارند، توجیه عقلانی مسائل و ابعاد آن و همچنین از بین بردن باورها و فرضیات رایج درباره آن بود.

این کتاب شامل پنج فصل می‌باشد: ۱-حقوق و قوانین، ۲-امنیت و ایمنی، ۳- گنجاندن و ادغام[1]، ۴-زیرساخت و نوآوری و ۵-داده و آشفتگی در آن. این کتاب در اصل به زبان انگلیسی نوشته شده است و حاوی خلاصه‌هایی به زبان‌های عربی، چینی، فرانسوی، آلمانی، روسی و اسپانیایی است.

تعریف انسان حال و آینده یا همان‌طور که فیلسوف آلمانی، گونتر آندرس، شرح می‌دهد، مردم امروز و فردا، بر اساس فاصله بین گسترش روزافزون ظرفیت‌های فناوری از یکسو، و ناتوانی در درک و فهم پیامدهای این فناوری می‌باشند. اسطوره‌ها غالباً برای پُر کردن این شکاف به‌کار گرفته می‌شوند. اما همان‌طور که در قالب این ۵۰ اسطوره نشان داده شده است، اینها صرفاً ساختارهایی هستند که اغلب به واسطه منافع مشخص ترویج داده می‌شوند.

هانس جوناس[2] یکی دیگر از فیلسوفان پیشگام آلمانی حوزه فناوری، اظهار داشته که برای به خدمت گرفتن فناوری در راستای منافع انسان، به یک «Kompaß»[3]، یا یک مرجع نظارتی جدید نیازمندیم تا هنجارها و سیاست‌ها را جهت‌دهی کند. در اوایل دهه ۲۰۰۰ این مرجع تمام‌وکمال در قالب «اجلاس جهانی سران در ارتباط با جامعه اطلاعاتی»[4] ظهور پیدا کرد و می‌توانست ۱۵ سال اول حکمرانی اینترنت را تحت تأثیر قرار دهد. در اعلامیه اصول ژنو در سال ۲۰۰۳ [5]و تعهد تونس در سال ۲۰۰۵[6]، جامعه جهانی متعهد شد: «یک جامعه اطلاعاتی مردم‌محور، فراگیر و توسعه‌گرا ایجاد کند و به اعلامیه جهانی حقوق بشر[7] احترام بگذارد

1. Inclusion and Integration
2. Hans Jonas
۳. قطب نما
4. World Summit on the Information Society (WSIS)
5.2003 Geneva Declaration of Principles
6.2005 Tunis Commitment
7. Universal Declaration of Human Rights

و از آن حمایت نماید، به‌گونه‌ای‌که مردم نقاط مختلف بتوانند به گسترش اطلاعات و دانش پرداخته، به آن دسترسی داشته باشند، آن را مورد بهره‌برداری قرار دهند و به اشتراک بگذارند و در نتیجه توان بالقوه خود را به‌کار گیرند و به اهداف و مقاصد توسعه‌ای موردقبول در سطح بین‌المللی از جمله اهداف توسعه هزاره[1] دست یابند.»

در همایش برلین، همچون دفعات پیشین، ذی‌نفعان حکمرانی اینترنت نحوه دستیابی به این هدف را موردبحث و بررسی قرار می‌دهند. اسطوره‌هایی که سر راه این تعهد قرار گرفته‌اند، باید از میان برداشته شوند. این اتفاق در مورد ۵۰ اسطوره‌ای که در صفحات بعدی آمده‌اند، رخ می‌دهد.

ماتیاس سی. کتمان و استفان درینر
هامبورگ / برلین - سپتامبر ۲۰۱۹

1. Millennium Development Goals

مقدمه

سواد رسانه‌ای و ضرورت نگاه انتقادی

عباس قنبری باغستان[1]

«سواد رسانه‌ای» از جمله مهمترین و چالش برانگیزترین دغدغه کشورها در دو دهه اخیر در ارتباط با شیوه مواجهه کاربران با اینترنت و فناوری‌های وابسته به آن بوده است. وضعیت سواد رسانه‌ای در ایران هم به طور سلبی(غفلت‌های صورت گرفته و چالش‌های ناشی از فقدان آن) و هم به طور ایجابی(استفاده روزافزون از فناوری‌های نوین)، متمایز از تجربه بسیاری از کشورهای دیگر نیست.

در ادبیات و محاورات عمومی ایران، از استعاره «نِتوند»[2] به جای «شهروند» استفاده می‌شود که در ارتباط با موضوع سواد رسانه‌ای استعاره بسیار معناداری است. اینکه رفتار «نتوند» ایرانی در مواجهه با فضای سایبری و شبکه‌های اجتماعی «چگونه است؟» یا «چگونه باید باشد؟»،«آیا چالشی یا پیچیده است یا منعطف و خنثی» و ...، سؤالاتی است که باید از طریق انجام تحقیقات علمی و تجربی متناسب با بافت فرهنگی‌اجتماعی ایران به آن دست یافت.

به موازات توسعه فناوری، ابعاد رفتار کاربران و نیز پیامدهای استفاده آنها از اینترنت و نیز

---

۱. عضو هیئت علمی گروه ارتباطات دانشگاه تهران

2. Netizen

شبکه‌های وابسته به آن نیز روز به روز پیچیده‌تر و گسترده‌تر می‌شود. اگر تا چندی پیش صرفاً بحث «استفاده» یا «عدم استفاده» از اینترنت یا «عضویت» یا «عدم عضویت» در شبکه‌های اجتماعی مطرح بود، امروزه جامعه و به طور خاص طیف وسیعی از کاربران در بین حجم انبوهی از موضوعات و مسائل فنی با آثار و پیامدهای فراوان و طولانی مدت اجتماعی، فرهنگی، سیاسی و دینی همچون «اثرات استرایسند»، «الگوریتم پروتکل‌های اینترنتی»، «واقعیت رمزگذاری پایان-به-پایان»، «دارک وب»، «فیلترینگ حبابی»، «حقوق دیجیتال»، «حق فراموش شدگی»، «آستروتورفینگ و شهرت جعلی»، «فناوری نظیر به نظیر»، «دستکاری یا سرقت اطلاعات» و ده‌ها مقوله فنی، حقوقی و ارتباطی دیگر آشکارا سردرگم و رها شده است.

براین اساس، موضوع سواد رسانه‌ای و نیز ابعاد، مؤلفه‌ها و چالش‌های مطرح در زمینه اینترنت و طیف وسیعی از شبکه‌ها و رسانه‌های اجتماعی وابسته به آن حائز اهمیت است که باید به صورت ریشه ای واکاوی شود.

تاریخچه، تعاریف و نظریه‌های سواد رسانه‌ای:

بر اساس مطالعات انجام شده، موضوع سواد رسانه‌ای از دهه ۱۹۶۰ که یونسکو به این موضوع و اهمیت آن ورود پیدا کرد، یکی از اصلی‌ترین محورهای تحقیقات بین رشته‌ای در حوزه علوم اجتماعی و رفتاری در کشورهای پیشرفته غربی از جمله کانادا و آمریکا بوده است(**McWhirter, Hoffman-Goetz, & Clarke**, ۲۰۱۲). «سواد رسانه‌ای» که با پیداش فناوری‌های نوین ارتباطی به خصوص رسانه‌های دیجیتال و شبکه‌های اجتماعی عجین می‌باشد، موضوعی است که هم در محافل علمی و آکادمیک(**Fisher**, ۲۰۱۱) و هم در محافل سیاسی و تصمیم گیری(**Rubin**, ۱۹۹۸) دغدغه‌هایی جدی در ارتباط با کاربران و مصرف کنندگان فناوری‌های نوین ایجاد کرده است.

از زمان طرح موضوع «سواد رسانه‌ای» در اوایل نیمه دوم قرن بیستم، در مناطقی همچون کشورهای آمریکای شمالی و نیز دول اروپایی، محققان و پژوهشگران حوزه‌های مختلف به کنکاش علمی پیرامون مبانی هستی شناسانه، شناخت شناسانه و روش شناسانه آن پرداخته و

در قالب طرح‌های پژوهشی نظری و تجربی به طرح و تعریف ابعاد آن مبادرت ورزیدند. در نتیجه انجام این تحقیقات و با توجه به اهمیت آن، در کانادا سریعاً موضوع سواد رسانه‌ای به عنوان «واحد درسی» به مدارس راه یافت. در ژاپن، به عنوان اولین کشور آسیایی، موضوع سواد رسانه‌ای با رویکرد انتقادی به سرعت مورد توجه قرار گرفت. حتی در کشورهای کوچکتری همچون مونته نگرو در اروپای شرقی نیز از سال ۲۰۰۹، موضوع سواد رسانه‌ای به عنوان واحد درسی اختیاری در دسترس دانش‌آموزان مدارس قرار گرفت (Perovic, ۲۰۱۵).

به‌طور کلی «تعامل فناورانه» نقطه کانونی تمامی تعاریف، مطالعات و تحقیقات مربوط به سواد رسانه‌ای به خصوص با تأکید بر تأثیرات رفتاری، شناختی، اخلاقی، فیزیکی، فرهنگی، اجتماعی، روانی و احساسی این فناوری‌های نوین در زندگی روزمره انسان‌ها بوده است. به این اعتبار، «سواد رسانه‌ای» عبارت است از کمک به افراد که بتوانند در این مسیر «شهروندان پیچیده[1]»ای باشند تا «مصرف‌کنندگان پیچیده[2]». به عبارت دیگر، به اعتبار تعریف «سواد رسانه‌ای»، رسانه‌ها باید بیش از مجموعه‌ای از پیام‌ها و اخبار فهمیده شوند که نیازمند بازبینی و تحلیل می‌باشند تا بتوان بین آنها تفکیک قائل شد و یا از میان آنها دست به انتخاب زد (**Lewis & Jhally**, ۱۹۸۸).

هابس[3] در سال ۱۹۹۸، سواد رسانه‌ای را فرایند دستیابی و ارزیابی انتقادی پیام‌های رسانه‌ای و متعاقباً ایجاد پیام از طریق ابزارهای رسانه‌ای تعریف کرد. در این تعریف، هدف سواد رسانه‌ای ایجاد «اختیار/استقلال[4]» از طریق توسعه قدرت تحلیل، استدلال، ارتباطات و مهارت خوداظهاری تعریف شده است. وی که یکی از پیشگامان این حوزه در آمریکا محسوب می‌شود، متعاقباً هفت مبحث کلان[5] در این زمینه مطرح ساخت که در قالب سؤالات ذیل عبارتند از: ۱- آیا سواد رسانه‌ای از کودکان دفاع می‌کند؟ ۲- آیا سواد رسانه‌ای نیازمند این است که دانش‌آموزان فعالیت‌های مرتبط با تولید رسانه‌ای داشته باشند؟ ۳- آیا سواد رسانه‌ای باید جهت‌گیری[6] فرهنگ عامه پسند داشته باشد؟ ۴- آیا سواد رسانه‌ای باید جنبه‌های[7] ایدئولوژیکی قوی‌تری داشته باشد؟

1. Sophisticated Citizens
2. Sophisticated Consumers
3. Hobbs
4.Autonomy
5. Seven Great Debates
6. Bias
7. Agenda

۵-آیا سواد رسانه‌ای می‌تواند به سطح تعداد بیشتری از دانش آموزان مدارس آمریکایی برسد؟ ۶-آیا فعالیت‌ها و نوآوری‌های مربوط به سواد رسانه‌ای باید به لحاظ مالی از سوی سازمان‌های رسانه‌ای حمایت شود؟ ۷-آیا سواد رسانه‌ای در بهترین حالت ابزاری برای رسیدن به یک هدف است؟

از نظر هابس پاسخ «بلی» یا «خیر» به هریک از مباحث فوق که خود دارای استدلال و دلالت‌های قوی می‌باشند، مبنای اصول پایه‌ای «سواد رسانه‌ای» و هدایتگر تحقیقات نظری و تجربی این حوزه در سال‌های آتی خواهد بود (Hobbs, ۱۹۹۸).

در همان سال‌ها، براون، از دیگر متفکران این حوزه، چشم‌اندازهای «سواد رسانه‌ای» را مطرح و استدلال کرد که سواد رسانه‌ای شامل فرایند شناختی به کار رفته در تفکر انتقادی می‌شود به نحوی که هرگونه موفقیت در برنامه‌ها و پروژه‌های مربوط به «سواد رسانه‌ای» مستلزم همکاری و مشارکت مربیان، مجریان، مشارکت کنندگان و تمامی کسانی که به نحوی درگیر هستند، می‌باشند (Brown, ۱۹۹۸). جاستین لوئیس و همکارش سواد رسانه‌ای را فراتر از این؛ به معنای توسعه دموکراسی دانسته‌اند، جایی که شهروندان باید بتوانند ساختار و سازمان‌های رسانه‌ای را نیز به چالش بکشند. در این تعریف، سواد رسانه‌ای نه فقط مربوط به قدرت تحلیل پیام‌های رسانه‌ها، بلکه همچنین مرتبط با «اینکه چرا این پیام‌ها تولید شده است؟» نیز می‌باشد. به عبارت دیگر، «اینکه ما بدانیم پیام‌های رسانه‌ای تولید شده‌اند یا حتی اینکه به لحاظ فنی چگونه تولید شده اند، دیگر کافی نیست. بلکه ما دقیقاً باید بدانیم که این پیام‌ها چرا تولید شده‌اند، توسط چه کسانی و تحت چه شرایط و محدودیت‌هایی تولید شده‌اند» (Lewis & Jhally, ۱۹۹۸).

از زمان پیدایش اولین تحقیقات در زمینه «سواد رسانه‌ای»، مطالعات نظری و تجربی زیادی به خصوص در کشورهای پیشرفته آمریکایی و اروپایی انجام و به طور مثال، موضوعات متعددی همچون «تحلیل انتقادی محتوای رسانه‌ها»، «سواد دیجیتال و اطلاعاتی»، «سواد فیلم»، «سواد خوانش اخبار و اطلاعات»، «سواد اینترنت و امنیت آنلاین»، «سواد بازی‌های دیجیتال»، «سواد رسانه‌های ارتباطی» و ... مورد توجه و تمرکز بوده است (Petranova, Hossova, & Velicky, ۲۰۱۷). همچنین برخی از این تحقیقات به صورت تک رشته‌ای و برخی دیگر نیز به صورت میان

رشته‌ای انجام شده است. به طور مثال، هابس در مورد تاریخچه و ظهور سواد رسانه‌ای (Hobbs, ۱۹۹۸, ۲۰۰۴, ۲۰۱۱; Hobbs & Tuzel, ۲۰۱۷)، آلورمان و هاگود در زمینه مفهوم پردازی و نظریه‌پردازی در حوزه «سواد رسانه‌ای»(Alvermann & Hagood, ۲۰۰۰a, ۲۰۰۰b)، سوتو و ساکاماتو در زمینه «آموزش و سواد رسانه‌ای» (Suto & Sakamoto, ۲۰۱۴)، لبس و مالس در زمینه «جوانان و سواد رسانه‌ای» (Labas & Males, ۲۰۱۷)، ریچ در زمینه «سواد رسانه‌ای و مسئله سلامت» (Rich, ۲۰۰۴)، هرساروی و تایی در زمینه «سواد رسانه‌ای، آموزش و کودکان» (Hirsjarvi & Tayie, ۲۰۱۱) تحقیقاتی را به سرانجام رسانیده‌اند.

به موازات کشورهای پیشرفته غربی و متعاقب نمایان شدن پیامدهای بعضاً چالش‌برانگیز استفاده وسیع از فناوری‌های ارتباطی، کشورهای درحال توسعه در آسیا، آمریکای لاتین و حتی کشورهای آفریقایی نیز توجه خاصی به «سواد رسانه‌ای» مبذول داشته و سعی کرده‌اند تا با استفاده از تجربیات و ادبیات موجود، هرچند با تأخیر گام‌هایی در مسیر واکاوی موضوع «سواد رسانه‌ای»، چالش‌ها و چشم‌اندازهای آن و ... بردارند. یکی از طرح‌های برجسته در این زمینه، پروژه «شبکه بین‌المللی سواد رسانه‌ای» (موسوم به میدلیت[1]) است که با همکاری اراسموس پلاس اتحادیه اروپا[2] در سه کشور مالزی، تایلند و ویتنام طی سال‌های اخیر (۲۰۱۸-۲۰۱۶) انجام شد.

هدف از پروژه میدلیت ارتقای سطح سواد رسانه‌ای در کشورهای مالزی، تایلند و ویتنام و نیز ایجاد و راه‌اندازی دوره‌های آموزش آنلاین در زمینه سواد رسانه‌ای بر اساس مطالعات تجربی در کشورهای متبوع بود. نکته قابل تأمل در ارتباط با این پروژه مشارکت ۱۱ دانشگاه (۵ دانشگاه از کشورهای اروپایی، آلمان، هلند و اتریش و ۶ دانشگاه از کشورهای مالزی، تایلند و ویتنام) بود که مسئولیت اجرایی آن را بر عهده داشته و نتایج آن نیز در قالب یک سمینار بین‌المللی در کوالالامپور، پایتخت مالزی ارائه شد. در حال حاضر، دوره‌های آنلاین آموزش سواد رسانه‌ای که به عنوان یکی از خروجی‌های پروژه مدلیت طراحی، تنظیم و اجرایی شده برای عموم مردم این کشورها قابل دسترس است و در سطوح مختلف آموزشی اعم از متوسطه، دانشگاه و سایر مراکز آموزش محور تدریس می شود.

---

1. MIDLIT
2. Erasmus+ CBHE Program

روند تصاعدی پژوهش‌های علمی در حوزه سواد رسانه‌ای:

بر اساس داده‌های به‌دست‌آمده از پایگاه استنادی «وب.آو.ساینس»، در فاصله زمانی ۱۹۷۰ تا ۲۰۱۹، در مجموع ۱۶۷۱ سند علمی با موضوع «سواد رسانه‌ای» شناسایی شده است. آنچه در این میان بیش از همه قابل توجه است، سیر به شدت تصاعدی میزان تحقیقات در حوزه «سواد رسانه‌ای» است به‌طوری‌که تولیدات علمی در این زمینه با یک سند علمی در سال ۱۹۸۹ آغاز و تا سال ۲۰۱۶، به ۲۳۷ سند علمی در سال رسیده است. همچنین روند تولیدات علمی در این زمینه تا سال ۲۰۰۵ تقریباً یکسان بوده، اما از این سال به صورت تصاعدی روند رو به رشدی به خود گرفته است.

به لحاظ جغرافیای تولیدات علمی در زمینه سواد رسانه‌ای، ایالات متحده آمریکا با ۵۴۹ تولید علمی، اصلی‌ترین و مهمترین کشور تولیدکننده اسناد علمی در این زمینه بوده است. به عبارت دیگر، ایالات متحده آمریکا طی بازه زمانی ۱۹۷۰ تا ۲۰۱۹ به تنهایی ۳۲.۸ ٪ از تولیدات علمی در زمینه سواد رسانه‌ای را به خود اختصاص داده است. پس از آن اسپانیا با ۲۱۲ سند علمی، انگلستان با ۸۱ سند علمی، چین با ۷۸ سند علمی و استرالیا با ۷۷ سند علمی و روسیه با ۷۱ سند علمی در رده‌های بعدی قرار دارند.

توزیع جغرافیایی تولیدات علمی در زمینه «سواد رسانه‌ای» نشان می‌دهد که در مجموع ۶۹ کشور در بازه زمانی ۱۹۷۰ تا ۲۰۱۹ شناسایی شده‌اند که در زمینه «سواد رسانه‌ای» دارای سند علمی (حداقل یک سند علمی) بوده‌اند.

علاوه‌براین، یکی از مهمترین نکات آموزنده در خصوص این تحقیقات، تنوع حوزه‌های پژوهشی مربوط به «سواد رسانه‌ای» بود. حوزه «آموزش و تحقیق در آموزش» با ۶۷۰ سند علمی، بیشترین میزان تولید در زمینه «سواد رسانه‌ای» را به خود اختصاص داده است. پس از آن حوزه ارتباطات با ۴۸۴ سند علمی (۲۸.۹ درصد) و حوزه روانشناسی با ۱۷۸ سند علمی (۱۰.۶ درصد) در رده‌های بعدی قرار دارند.

در ارتباط با مفهوم‌پردازی‌های صورت گرفته در ارتباط با «سواد رسانه‌ای»، اگرچه محورهای عمده کانونی همچنان «آموزش»، «جوانان»، «تلویزیون» و... بوده است، اما با گذر زمان

حوزه‌های تخصصی‌تر و جزئی‌تر متناسب با پیامدهای متأخر فناوری‌های نوین همچون «سلامت»، «اینترنت»، «کامپیوتر»، «شناخت»، «عقاید» و... نیز به دامنه مفهوم‌پردازی‌ها در این حوزه اضافه شده است (قنبری باغستان، ۲۰۱۹).

چرا سواد رسانه‌ای مهم است؟

بر مبنای ادبیات موجود و تحقیقات تجربی مربوط به سواد رسانه‌ای در کشورهای پیشرفته، «سواد رسانه‌ای» پاسخی «نرم» به عمده مسائل و پیامدهای چالش‌برانگیز استفاده وسیع «نِتوند»ها از فناوری‌های نوین ارتباطی است. به این اعتبار، مواجهه سالم و مطمئن جامعه با مقولات و مؤلفه‌های فنی‌ای که در مقدمه این فصل به آن اشاره شد، جز از طریق ارتقای «سواد رسانه‌ای» عموم کاربران اینترنت، شبکه‌های اجتماعی و فضای سایبری امکان‌پذیر نیست.

در ایران نیز همانند بسیاری از کشورهای دیگر، موضوع «سواد رسانه‌ای» و اهمیت آن سال‌هاست که در محافل مختلف علمی، دانشگاهی و پژوهشی مطرح و به کرات در مورد اهمیت آن نظرورزی شده است. اما آنچه بیش از پیش عیان شده است، «پیش افتادگی» سیاستگذاری و «پس افتادگی» مجموعه اقدامات عملیاتی صورت گرفته در این زمینه با هدف مصون‌سازی و ایمن سازی کاربران ایرانی از انواع آسیب‌ها و پیامدهای استفاده وسیع از انواع رسانه‌ها و شبکه‌هایی است که در بافت حیات سیاسی، اجتماعی و فرهنگی جامعه تنیده شده است.

به بیان عینی تر، در ارتباط با «سواد رسانه‌ای» باید از لاک دفاعی و سیاست‌گذاری محض خارج و وارد فاز اجرایی سیاست‌های عملیاتی در حوزه‌های مختلف شد. در این راستا، آموزش و تربیت «نِتوندی» آگاه و قادر به تفکر انتقادی در ارتباط با محتوای حجم وسیعی از پیام‌هایی که در بستر تعاملات روزانه از کانال‌های مختلف دریافت می‌کند، مسلط به تحلیل «منبع» پیام و چرایی دریافت پیام‌های ارتباطی، قادر به تعامل و به چالش کشیدن ساختاری سازمان‌های رسانه‌ای مدرن و... وظیفه‌ای است که بر عهده نهادهای آموزشی و فرهنگی همچون آموزش و پرورش، دانشگاه‌ها، نهادها و مؤسسات فرهنگی، انجمن‌ها و مؤسسات غیر دولتی است. اینها مسائل و موضوعاتی است که باید هرچه سریع‌تر در چارچوب کلان‌تر «سواد رسانه‌ای» در سطوح شهری، استانی و حتی ملی و کشوری مورد توجه قرار گیرد.

درباره این کتاب:

کتابی که پیش رو دارید، ایده‌هایی برای اندیشیدن و انتقادی نگریستن به باورهای عامیانه‌ای است که در ارتباط با اینترنت، به عنوان بستر و پلتفرم مادر، و نیز تمامی فناوری‌ها و شبکه‌های رسانه‌های مبتنی بر آن است.

از منظر سواد رسانه‌ای، این کتاب به تعبیر جاستین لوئیس، با رویکری کاملاً انتقادی ساختار و سازمان رسانه‌ای اینترنت را به چالش کشیده و حقیقت مرتبط با ۵۰ باور نادرست (اسطوره) در ارتباط با ماهیت آن را افشا می‌کند. این اسطوره‌ها طیف وسیعی از باورها و انگاره‌هایی که به اشتباه در ذهن و باور کاربران عجین شده را پوشش می‌دهد و از زوایای مختلف به روشنگری در زمینه ابعاد آنها می‌پردازد.

این کتاب به لحاظ فنی دو ویژگی منحصر به فرد دارد: ۱-نویسندگان آن، طیف وسیعی از محققان، پژوهشگران و نظریه‌پردازان برجسته در کشورهای اروپایی و آمریکایی هستند که خود بعضاً از پایه‌گذاران اینترنت بوده و نقش مؤثری در نوآوری، تولید، انتشار و گسترش فناوری‌های نوین داشته‌اند. ۲-موضوعات، مؤلفه‌ها و ابعاد بسیار فنی و پیچیده هریک از اسطوره‌ها با ذکر مثال‌هایی از تجارب زیسته عموم کاربران اینترنت و شبکه های اجتماعی، به زبان ساده و قابل فهم بیان شده است.

اهمیت این کتاب، به خصوص برای دانشجویان، دانش‌آموزان، فرهنگیان، پژوهشگران و عموم کاربران اینترنت و شبکه‌های اجتماعی از این جهت است به رغم افزایش سواد عمومی جامعه، از یک طرف روز به روز بر حجم و میزان باورهای غلط در ارتباط با مباحثی همچون «آزادی در اینترنت»، «امنیت در اینترنت»، «بی‌طرفی اینترنت و شبکه‌های اجتماعی»، «وضعیت داده‌ها در اینترنت و شبکه‌های اجتماعی» و... افزوده می‌شود؛ و از سوی دیگر تعداد روزافزونی از کاربران ناآگاه از اهداف و برنامه‌ریزی‌های ساختاری و پیچیده ذی‌نفعان اصلی فناوری‌های نوین، قربانی مطامع عمدتاً اقتصادی، تجاری و ایدئولوژیک آنها می‌شوند. از این‌رو، تنها راه رهایی از این وضعیت، همان‌طور که در تمامی تحقیقات و پژوهش‌های پیشین به آن اشاره شده و در این کتاب نیز مورد تأکید قرار گرفته، رهایی از بند «ناآگاهی» و «اسطوره‌های» نادرستی است که عمداً و سهواً در باورهای عمومی کاربران اینترنت نهادینه شده است.

در این مسیر، ارتقای «سواد رسانه‌ای» عموم «نتوندان» از واقعیات و مسائل پشت پرده توسعه اینترنت و شبکه‌های اجتماعی و موبایلی وابسته به آن، مهترین و والاترین گامی است که می‌توان برداشت: اینکه چه کسانی اینترنت و فناوری‌های وابسته به آن را توسعه داده‌اند؟، حکمرانی آنها در دستان چه کسانی است؟ چه کسانی بیشترین بهره را از آنها می‌برند؟ جهت‌گیری الگوریتم‌ها و فناوری‌هایی همچون بلاکچین، نظیر به نظیر، پایان به پایان به چه نحو است؟ چه اتفاقات و جریاناتی از زمان ورود کاربر به اینترنت تا هنگام خروج از آن در ارتباط با وی به وقوع می‌پیوندد؟ رابطه تولیدکننده محتوا با پلتفرم چیست؟ چه پیامدها و آسیب‌هایی متوجه کاربران است؟ و ده‌ها سؤال دیگر؛ موضوعات و مسائلی است که تنها در چارچوب گفتمان «سواد رسانه‌ای» می‌توان پاسخ‌های وثیقی برای آنها یافت.

ردیف	عنوان اسطوره	ردیف	عنوان اسطوره
۱	امکان نظام‌مندسازی فعالیت‌های انسان در اینترنت وجود ندارد	۲۶	ما همگی اکنون خبرنگار و تولیدکننده خبر هستیم
۲	حقوق و قوانین بین‌الملل قابل اعمال در اینترنت نیست	۲۷	نسل هزاره همگی مسلط به اینترنت بوده و با زندگی دیجیتال عجین هستند
۳	کد همان قانون است	۲۸	اینترنت مانند آنچه که در بهار عربی اتفاق افتاد، باعث توسعهٔ دمکراسی می‌شود
۴	پروتکل‌ها، سیاسی‌کاری نیستند	۲۹	اینترنت ماهیت انتخابات را از بین برده است
۵	مجرمین سایبری آزادانه می‌چرخند	۳۰	کارزارهای حقوق دیجیتال توسط ربات‌ها اداره و هدایت می‌شوند، نه فعالیت‌های واقعی
۶	در فضای آنلاین شما می‌توانید هر چیزی را بیان کنید	۳۱	اینترنتِ بدون سازمان، امکان سازماندهی را فراهم می‌آورد
۷	پلتفرم‌های‌اینترنتی‌مسئولیتی‌درقبال‌محتوای تولید شده توسط کاربران ندارند	۳۲	محصولات دیجیتال غیر مادی هستند
۸	اینترنت همواره بر اساس رویکردهای چند ذی‌نفعی عمل کرده است	۳۳	فضای سایبری کاملاً از دنیای واقعی مجزا است(دو فضای متفاوت هستند)
۹	در اینترنت همه چیز رایگان است	۳۴	هیچ نقطه نامعلومی در اینترنت وجود ندارد؛ همه به هم متصل‌اند
۱۰	جنگ سایبری در راه است	۳۵	اینترنت یک نظام شبکه‌ای است

ردیف	عنوان اسطوره	ردیف	عنوان اسطوره
۱۱	نظارت بر تسلیحات در فضای سایبری امکان پذیر نیست	۳۶	ما برای اینترنتی که توسط دیگران ارئه شده است، هزینه می‌پردازیم
۱۲	بهترین رویکرد دفاعی سایبری درواقع همان رویکرد تهاجمی است	۳۷	اینترنت هم اکنون در ابرها است
۱۳	پیشرفت‌های چشمگیر در امنیت سایبری ضروری است	۳۸	نظام نام‌گذاری دامنه متضمن جهانی بودن اینترنت است
۱۴	تنها جنایتکاران به دنبال مخفی سازی هویت خود در فضای آن لاین هستند	۳۹	«بی طرفی شبکه» در کل اینترنت تأمین شده است
۱۵	پنتاگون اینترنت را برای نجات از یک حملهٔ هسته‌ای اختراع کرده بود	۴۰	اینترنت باعث دموکرات شدن نوآوری می‌شود
۱۶	پیام‌رسانی رمزگذاری شده پایان-به-پایان به معنای محافظت از حریم خصوصی است	۴۱	بر تأثیرات شبکه نمی‌توان چیره شد
۱۷	دارک وب بهشتی برای خلافکاران است	۴۲	الگوریتم‌ها همواره بی طرف هستند
۱۸	اینترنت ابزاری رهایی بخش جهت پایان بخشیدن به تمام تبعیض‌ها است	۴۳	هوش مصنوعی چاره مشکل است
۱۹	موتورهای جستجو نتایج عینی ارائه می‌دهند (در ارائه نتایج بی طرف هستند)	۴۴	آینده هوش مصنوعی در دست شرکت‌ها قرار دارد
۲۰	رسانه‌های اجتماعی بازتاب دهندهٔ واقعیات جامعه هستند	۴۵	حریم خصوصی به کلی از بین رفته است
۲۱	تمام کاربران تجربهٔ مشابهی از اینترنت دارند	۴۶	اینترنت هرگز فراموش نمی‌کند
۲۲	زندگی ما دستخوش فیلترینگ حبابی شده است	۴۷	قوانین «حفاظت از اطلاعات» مرتبط با کنترل اطلاعات است
۲۳	مردم اخبار را تنها از طریق رسانه‌های اجتماعی پیگیری می‌کنند	۴۸	اطلاعات میل به آزادی دارند
۲۴	لایک و به اشتراک‌گذاری نشان از محبوبیت دارند	۴۹	فناوری« نظیر به نظیر» یعنی اشتراک‌گذاری غیر قانونی اطلاعات
۲۵	مشکل اصلی اخبار جعلی است	۵۰	بلاکچین همه مشکلات ما را حل خواهد کرد

منابع

1. Alvermann, D. E., & Hagood, M. C. (2000a). Critical media literacy: Research, theory, and practice in «new times». Journal of Educational Research, 205-193 ,(3)93. doi:00220670009598707/10.1080

2. Alvermann, D. E., & Hagood, M. C. (2000b). Fandom and critical media literacy. Journal of Adolescent & Adult Literacy, 446-436 ,(5)43.

3. Brown, J. A. (1998). Media literacy perspectives. Journal of Communication, 57-44 ,(1)48. doi:10.1111/j.2466.1998-1460.tb02736.x

4. Fisher, H. (2011). Handbook of Research on New Media Literacy at the K12- Level: Issues and Challenges. Australian Library Journal, 176-176 ,(2)60. doi:00049670.2011.1/10.1080 0722599

5. Hirsjarvi, I., & Tayie, S. (2011). Children and New Media: Youth Media Participation. A Case Study of Egypt and Finland. Comunicar(107-99 ,(37. doi:10.3916/c01-03-2011-37

6. Hobbs, R. (1998). The seven great debates in the media literacy movement. Journal of Communication, 32-16 ,(1)48. doi:10.1111/j.2466.1998-1460.tb02734.x

7. Hobbs, R. (2004). A review of school-based initiatives in media literacy education. American Behavioral Scientist, 59-42 ,(1)48 doi:0002764204267250/10.1177

8. Hobbs, R. (2011). The State of Media Literacy: A Rejoinder. Journal of Broadcasting & Electronic Media, 604-601 ,(4)55. doi:08838151.2011.619399/10.1080

9. Hobbs, R., & Tuzel, S. (2017). Teacher motivations for digital and media literacy: An examination of Turkish educators. British Journal of Educational Technology, 22-7 ,(1)48. doi:10.1111/bjet.12326

10. Labas, D., & Males, D. (2017). Adolescent perception of electronic media ethical values in context of sociode-mographic characteristics and media literacy. Nova Prisutnost, ,(2)15 230-211.

11. Lewis, J., & Jhally, S. (1998). The struggle over media literacy. Journal of Communication, 120-109,(1)48. doi:10.1111/j.2466.1998-1460.tb02741.x

12. McWhirter, J. E., Hoffman-Goetz, L., & Clarke, J. N. (2012). Can you see what they are saying? Breast cancer images and text in canadian women›s and fashion magazines. Journal of Cancer Education, 391-383 ,(2)27. doi:10.1007/s0-0305-011-13187

13. Perovic, J. (2015). Media Literacy in Montenegro. Media and Communication, -91 ,(4)3 105. doi:10.17645/mac.v3i4.335

14. Petranova, D., Hossova, M., & Velicky, P. (2017). Current Development Trends of Media Literacy In European Union Countries. Communication Today, 64-52 ,(1)8.

15. Rich, M. (2004). Health literacy via media literacy - Video intervention/ prevention assessment. American Behavioral Scientist, 188-165 ,(2)48. doi:0002764204267261/10.1177

16. Rubin, A. M. (1998). Media literacy. Journal of Communication, 4-3 ,(1)48. doi:10.1111/j.2466.1998-1460.tb02732.x

17. Suto, H., & Sakamoto, M. (2014). Developing an Education Material for Robot Literacy. In S. Yamamoto (Ed.), Human Interface and the Management of Information: Information and Knowledge in Applications and Services, Pt Ii (Vol. 8522, pp. 108-99).

18. قنبری باغستان, ع. (2019). سواد رسانه‌ای: یک فراتحلیل علم شناسانه از اسناد و تولیدات علمی (1970-2019). مجله جهانی رسانه - نسخه فارسی, 14(1), 75-93. doi:10.22059/gmj.73577.2019

فصل اول
حقوق و قوانین

اسطوره اول: امکان نظام‌مندسازی[1] فعالیت‌های انسان در اینترنت وجود ندارد[2]

نیکولاس گوگنبرگر[3]

باور عمومی: نظام‌مند ساختن فعالیت انسان در اینترنت امری غیرممکن است. کاربران اینترنت در برابر کلیه مقررات یا دست‌کم مقررات محسوس مقاومت می‌کنند. قوانین یا اعمال نمی‌شوند یا در صورت اعمال و نقض شدن آنها، به سبب معماری زیرساخت‌ها و ماهیت ارتباطات برخط توسط دولت قابلیت پیگرد ندارند.

اصل موضوع: باوجود کلیه شواهدی که نادرستی تفکر فوق را ثابت می‌کنند، این باور عمومی که فعالیت‌های انسانی در اینترنت، فضای سایبری یا «بزرگراه اطلاعاتی» امری غیر قابل پیگیری قضایی است، به‌طور وسیعی گسترش یافته و هر بار نیز با ظاهری جدید طی چرخه‌های نوآوری و فناوری مدرن نمود پیدا می‌کند. این باور نادرست ناشی از سوءبرداشت از ماهیت تنظیم مقررات و عدم درک زیرساخت‌های شبکه و به‌طورکلی ویژگی‌های ارتباطات برخط می‌باشد. با وجود آنکه در ۳۰ سال گذشته تحقیقات، قانون‌گذاری‌ها و اقدامات اجرایی گوناگونی در راستای مردود شمردن

1. Regulated
2. Lawrence Lessig. (200.6). "Code". Version 2.0. Basic Books
3. Nikolas Guggenberger

این باور نادرست صورت گرفته است، با ظهور هر فناوری جدید از موتورهای جستجو گرفته تا رسانه‌های اجتماعی و فناوری بلاک چین[1]، این برداشت اشتباه مجدداً قوت می‌یابد.

بحث را با سوءبرداشت اول از ماهیت مقررات آغاز می‌کنیم. مقررات از اشخاص حقیقی یا حقوقی می‌خواهد که دقیق و صریح باشند. این مقررات به‌طورمستقیم به نظام‌مندسازی مواردی همچون شبکه‌ها، فضاها یا بزرگراه‌ها نمی‌پردازند، بلکه در بهترین حالت روابط بین افراد و بازیگران مختلف را قاعده‌مند می‌سازند. بنابراین، بحث در مورد قانونمندی اینترنت اساساً اشتباه است. در مقابل، پرسش درست این است که آیا می‌توان با افرادی که از طریق اینترنت با یکدیگر ارتباط برقرار و معامله می‌کنند، از طریق قوانین و مقررات برخورد نمود و دیگر این‌که آیا این چرخه به‌نوبهٔ خود پیکره اصلی اینترنت را شکل می‌دهد یا خیر؟ درحقیقت، می‌توانیم به این پرسش پاسخ مثبت بدهیم: اشخاص را می‌توان به‌دلیل تخلفات اینترنتی مجازات نمود، می‌توان آنها را در برابر نقض کپی‌رایت و انتشار محتوای غیرقانونی تحت پیگرد قضایی قرار داد. قراردادهای الکترونیکی همانند قراردادهای سنتی، از نظر قانونی الزام‌آور هستند. حقوق حمایت از مصرف‌کننده، تجارت الکترونیکی را شکل داده است و قانون حفاظت از داده‌های عمومی[2] و قوانین پیشین آن نیز مرزهای پردازش داده‌های شخصی را تعیین کرده‌اند.

در دومین سوءبرداشت، نواقص اجرایی در اعمال مقررات قانونی به‌طورکلی با قابلیت نظام‌مندسازی اشتباه گرفته می‌شود. بدون‌شک، دنیای دیجیتالی، دنیایی غیرمتمرکز و از برخی جهات ناشناخته است که سبب ترویج جرایم خاص می‌شود و با کاهش هزینه‌های معاملات، دور زدن قوانین محلی را تسهیل می‌کند. با این‌حال، هیچ‌یک از چالش‌های اجرایی قانون، اصل قابلیت نظام‌مندسازی فعالیت‌های انسان در اینترنت را تضعیف نمی‌کنند (ارجاع به اسطوره ۵). البته باید سه نکته را در نظر داشت: اول این‌که مقامات ذی‌صلاح رویکردهایی را در راستای تحقیق در زمینه جرایم و اجرای قوانین برخط توسعه داده‌اند. دوم این‌که، اینترنت به‌عنوان یک شبکه و واسطه به زیرساخت‌های فیزیکی (از جمله قلمرو حکومت‌ها) وابسته است که به‌راحتی می‌توانند هدف اقدامات و پیگردهای قانونی قرار گیرند. سوم، نظارت در اینترنت اساساً دشوارتر از محیط‌های دیگر نیست.

1. Blockchain
2. GDPR (General Data Protection Regulation)

حقیقت: رفتار در اینترنت دقیقاً مانند هر رفتار دیگری می‌تواند تحت نظارت و پیگرد قانونی قرار گیرد. هرگونه نقض قوانین و مقررات می‌تواند به اعمال اقداماتی (از جمله محاکمه، تحت پیگرد قرار گرفتن و ...) منجر بشود. با آنکه بی‌نام‌ونشان بودن، ماهیت برون‌مرزی قراردادها و جرائم، سرعت ارتباطات و قدرت فنی متخلفان اثربخشی اجرای قانون را به چالش می‌کشد، این حقیقت را که زندگی ما در هر دو صورت برخط و غیربرخط تحت نظارت و قانون قرار دارد را تغییر نمی‌دهد.

اسطوره دوم: حقوق و قوانین بین‌الملل قابل اعمال در اینترنت نیست[1]

ماتیاس سی. کتمان[2]

باور عمومی: به‌دلیل نبودن یک عهدنامه بین‌المللی در خصوص اینترنت، به‌عنوان‌مثال شبیه **توافق‌نامه اقلیمی پاریس**[3]، حقوق بین‌الملل در مورد موضوعات بین‌المللی و روابط اینترنتی آنها کاربرد ندارد. بنابراین دولت‌ها و کشورها می‌توانند هرکاری را که می‌خواهند، به‌صورت برخط انجام دهند.

اصل موضوع: فقدان عهدنامه بین‌المللی برای نظام‌مندسازی فضای مجازی کاملاً حقیقت دارد. اما حقوق بین‌الملل در اینترنت قابل اعمال می‌باشد و از امنیت، ثبات، استحکام، انعطاف‌پذیری و عملکرد اینترنت -یکپارچگی آن- به‌عنوان یک نفع مشترک پشتیبانی می‌کند. پیش‌تر، گزارش کارشناسان دولتی سازمان ملل متحد[4] در سال ۲۰۱۳، با تکیه بر اسناد ژنو و تونس {مصوب سران کشورها در دو اجلاس جهانی جامعه اطلاعاتی در ژنو (۲۰۰۳) و تونس (۲۰۰۵)} تأیید کرد که اعمال هنجارهای برگرفته از قوانین بین‌المللی موجود در خصوص

1. **Source:** Group of Governmental Experts Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/174/70 of 22 July 2015; Matthias C. Kettemann, The Common Interest in the Protection of the Internet: An International Legal Perspective, in Benedek/de Feyter/Kettemann/Voigt (eds.), The Common Interest in International Law (Antwerp: Intersentia, 2014)167-184.
2. Matthias C. Kettemann
3. Paris Agreement on Climate Change
4. UN Group of Governmental Experts

استفاده از فناوری اطلاعات و ارتباطات توسط کشورها «اقدامی ضروری در راستای کاهش خطرهایی است که صلح، امنیت و ثبات بین‌المللی را تهدید می‌کنند». در گزارش سال ۲۰۱۵، این گروه فراتر رفته است و تعهدات دولت‌ها دربرابر برخی اصول مهم منشور و سایر حقوق بین‌المللی را بسیار مهم خوانده که عبارتند از برابری حاکمیتی[1]، منع تهدید یا اعمال زور، احترام به حقوق بشر و آزادی‌های بنیادی و عدم مداخله در امور داخلی سایر کشورها.

جدا از حقوق بین‌الملل عرفی[2]، اصول کلی حقوق بین‌الملل نیز در تنظیمات اینترنتی و برخط اعمال می‌شود. این موارد شامل اصول «ارزیابی بایسته»[3]و «همسایگی خوب»[4] است که از طریق اقدامات اعتمادساز متقابل و نیز ظرفیت سازی به اجرا در می‌آیند.

در خصوص اعمال حقوق بین‌الملل در اینترنت یک استدلال هنجاری نیز وجود دارد: قوانین «الزام‌آور». «حقوق بین‌الملل» درواقع تنها بدنه قانونی است که می‌تواند به‌عنوان پایه و اساس قانونی هنجارهایی در نظر گرفته شود که در سطح بین‌المللی قابل اجرا می‌باشند، و از طریق آن می‌توان اقتدار عمومی بین‌المللی را مشروعیت بخشید و توزیع کالاها و حقوق را مورد بحث و بررسی قرار داد.

سرورها و هسته عمومی اینترنت[5] هر دو برای کارکرد صحیح اینترنت و زیرساخت‌های حیاتی (به‌عنوان‌مثال شبکه‌های برق) و همچنین زیرساخت‌های (اطلاعاتی) مهم داخل آنها ضروری هستند. حفظ یکپارچگی اینترنت (امنیت، ثبات، استحکام، انعطاف‌پذیری و عملکرد آن) به یکی از اهداف اساسی حقوق بین‌الملل تبدیل شده و تضمین آن تنها به واسطه حقوق بین‌الملل میسر است.

حقوق بین‌الملل اینترنت همچنین چارچوبی برای به اجرا درآمدن رویکردهای مرتبط با حکمرانی اینترنت[6]، یا به‌عبارتی «اعمال» قوانین بر اینترنت، فراهم می‌سازد (ارجاع به اسطوره ۱). اهمیت این قوانین ریشه در این واقعیت دارند که در اینترنت، مسئله قانونی یا

1. Sovereign Equality
2. Customary International Law
3. Due Diligence

ارزیابی بایسته یک اصطلاح حقوقی به‌معنای ارزیابی وجوه منفی و مخاطره آمیز یک موضوع قبل از پرداختن به آن است. به‌عنوان مثال، قبل از سرمایه‌گذاری یا قبل از امضای قرارداد لازم است تمامی وجود و ابعاد منفی، تهدیدات احتمالی، ریسک احتمالی و ... آن را در نظر گرفت.

4. Good Neighbourliness

یک اصل عمومی در حقوق بین‌الملل است که به‌معنای وفق دادن یا در نظر گرفتن حقوق و ملاحظات کشورهای همسایه در هرگونه اقدام به خصوص در زمینه محیط زیست می‌باشد.

5.Internet's Public Core
6. Internet Governance
7. Conceptualization

غیرقانونی بودن اساساً یک دوگانگی کاذب است. درحالی‌که قانون به‌طورسنتی به این دوگانگی می‌پردازد، هنجارهای حکمرانی امکان مفهوم‌پردازی[۷] و نقد نظام‌های «مسئولیت‌پذیری» و «پاسخگویی»[۱] را فراهم می‌آورند: قانونمند بودن در فضای برخط از تنوع زیادی برخوردار است. باتوجه‌به ماهیت پویای اینترنت، این تغییرپذیری هنجاری[۲] را می‌توان به‌عنوان یکی از ویژگی‌های اصلی تحول هنجاری[۳] در نظر گرفت.

حقیقت: مادامی که هیچ عهدنامه بین‌المللی‌ای در خصوص اینترنت وجود ندارد، حقوق بین‌الملل کاملاً قابلیت اعمال در آن را دارد. قوانین عُرفی[۴] و اصول کلی حقوق بین‌الملل میزان قدرت و محدودیت‌های بازیگران بین‌المللی را مشخص می‌کنند و همچون حقوق بین‌الملل، تقریباً کلیه کشورها به اکثر قوانین احترام می‌گذارند. هنگامی که حل‌وفصل مسائل سیاستی[۵] بیشتری ضرورت داشته باشد، رویکردهای حکمرانی اینترنت مکمل حقوق بین‌الملل خواهند بود.

اسطوره سوم: کد همان قانون است[۶]

ریکا کولو[۷]

باور عمومی: کد همان قانون است. کدهای نرم‌افزاری به ابزار کانونی یا حتی اساسی تنظیم رفتار انسان و تأکید بر کنترل اجتماعی وی بدل شده‌اند. اینترنت نیز مخالف مقررات دولتی است و به‌همین‌دلیل به راهکارهای جایگزین از قبیل «خود تنظیمی»[۸] و «تنظیم براساس کدها»[۹] احتیاج دارد.

---

1. Accountability
2. Variable Normativity
3. Normative Evolution
4 .Customary Rules
5. Policy-Oriented
6. **Source:** Mireille Hildebrandt, Legal and Technological Normativity: More (and Less) Than Twin Sisters ((2008 3)12) Techné: Journal of the Society for Philosophy and Technology (183-169 ,(2008, https://www. academia. edu/702733/Legal_and_Technological_Normativity_more_and_less_than_twin_sisters; Ronald Leenes: Framing Techno-Regulation: An Exploration of State and Non-State Regulation by Technology, Tilburg Law School Legal Studies Research Paper Series No. 2012/10, available at: http://ssrn.com/abstract=2182439.
7. Riikka Kuolu
8. Self-Regulation
9. Regulation By Code

اصل موضوع: این‌که محیط‌های رمزگذاری‌شده دارای یک بُعد هنجاری تأثیرگذار بر اقدامات احتمالی کاربران اینترنت هستند، انکار ناپذیر است. بااین‌حال، این بدان معنی نیست که ساختارهای اجتماعی و حقوقی موجود به‌طور خودکار کنار می‌رود یا در محیط‌های آنلاین (برخط) ناکارآمد می‌شوند؛ و درواقع استدلال اصلی لِسیگ[1]، دانشمند و فعال سیاسی آمریکایی، نیز این نبوده است. به گفته وی، زیرساخت فنی تنها یکی از اشکال مقررات فضای مجازی در کنار قانون، هنجارهای اجتماعی و بازار است. به نظر می‌رسد لسیگ موضع پدرسالاری سایبری[2] را طرح می‌کند چراکه نگرانی خود را از کنترل پنهان، غیرشفاف و توطئه‌آمیز کدها ابراز می‌کند، که از دیدگاه لسیگ می‌باید توسط قوانین و شفافیت مقررات برخط و غیربرخط برطرف و اصلاح شود.

درنهایت، عبارت کد همان قانون است. ساده‌سازی بیش از اندازه یک چشم‌انداز نظارتی بسیار پیچیده‌تر است که بی‌اعتقادی به توانایی دولت‌ها جهت قانونمندسازی فضای مجازی را منعکس می‌کند و اولین بار در اعلامیه استقلال فضای مجازی در سال ۱۹۹۶ [3]به‌کار برده شده و غالباً به اشتباه برای اهداف سیاسی عنوان می‌شود (ارجاع به اسطوره ۱). این رویکرد مبتنی‌بر «کد همان قانون است» در نظر نمی‌گیرد که قانون مدرن محدود به یک دولت نیست بلکه بین‌المللی و کثرت‌گرا[4] است (ارجاع به اسطوره ۲). ازاین‌رو، ماهیت فراملّی اینترنت به‌معنای این نیست که رفتار برخط از دسترس بازیگران غیربرخط دولتی و غیردولتی خارج است؛ به‌عنوان مثال، تلاش برای قانونمندسازی پلتفرم‌ها، حاکمیت داده‌ها و حمایت از مصرف‌کننده در تجارت الکترونیکی بیانگر این واقعیت است که آنها (بازیگران دولتی) همچنان به‌دنبال اعمال قوانین ملی بر اینترنت فراملّی است. مشاهدات لسیگ مبنی‌بر این‌که در فضای مجازی کنترل اجتماعی از طریق معماری فناوری صورت می‌گیرد، کاملاً صحیح است. همچنین بازتاب‌دهنده نگرش‌های قدیمی‌تر درباره فناوری‌های هنجاری متمرکز بر مهندسی اجتماعی از طریق معماری و مصنوعات فناورانه[5] می‌باشد. همان‌طور که لینز[6] توصیف می‌کند، «کد همان قانون است» همچون سایر «سازوکارهای کنترل مبتنی‌بر طراحی است [که] بسیار

1. Lessig
2. Cyberpaternalism
3.The 1996 Declaration of Independence Cyberspace
4. Pluralistic
5. Technological Artefacts
6. Leenes

قدرتمند می‌باشند، چراکه به‌جای آنکه پس از واقعه وارد عمل شوند، پیش از واقعه به آن می‌پردازند» و شامل تحریم‌ها به‌معنای عام نیستند (لینز ۲۰۱۲، ۱۴۷). زیرساخت‌های فنی به‌تنهایی کافی نیستند، چراکه قادر به حذف کامل درگیری‌ها و اختلافات نمی‌باشند. در نتیجه به قانون نیاز است که سازوکارهای حل اختلاف را ارائه می‌دهد.

هنجارمندی فناوری با هنجارمندی قانونی متفاوت است. هیلدبراندت[1] هنجارمندی فناوری را چنین توصیف می‌کند: «روشی که یک ابزار یا زیربنای فناورانهٔ به‌خصوص به واسطه آن اقدامات انسان را محدود می‌سازد، رفتار مشوق یا وادارکننده، بازدارنده یا منع‌کننده». بر خلاف هنجارمندی قانونی، معماری فناورانه به اقتدار دولت و انحصار خشونت متکی نیست و طی یک فرایند دموکراتیک به‌وجود نمی‌آید (هیلدبراندت ۲۰۰۸، ۱۷۶).

حقیقت: دانش اجتماعی-قانونی[2] رویکرد پیچیده‌تر و دقیق‌تری برای توصیف تداخل ظریف قواعد فنی، حقوقی و اجتماعی تعریف کننده رفتار انسانی در فضای برخط ارائه داده است. به‌عنوان‌مثال، مفاهیم کثرت گرایی حقوقی یا قانونمندسازی فناورانه[3] را می‌توان به‌منظور توصیف پیچیدگی قانونمندسازی اینترنت به‌کار برد که متشکل از بازیگران متعدد دولتی و غیر دولتی و لایه‌های مختلف مقررات قانونی، اجتماعی و فنی است.

اسطوره چهارم: پروتکل‌ها، سیاسی‌کاری نیستند[4]

کورین کث-اسپث[5]

باور عمومی: معیارها و پروتکل‌های فنی که اینترنت بر پایه آنها ساخته شده است، سیاسی‌کاری نیستند (سیاسی نیستند). آنها فناوری‌هایی خنثی هستند که توسط مهندسان بی‌طرفی

1. Hildebrandt
2. Socio-Legal Scholarship
3. Techno-Regulation
4. **Source:** Laura DeNardis, Protocol Politics: The Globalization of Internet Governance (Boston: MIT Press, 2013); Corinne Cath and Luciano Floridi, The Design of the Internet's Architecture by the Internet Engineering Task Force (IETF) and Human Rights, Science and Engineering Ethics 23 (2017)2, 449-468.
5. Corinne Cath-Speth
6 . Internetwork

که صرفاً به‌دنبال انتشار اطلاعات و همکاری[۶] بین شبکه‌ها می‌باشند، از طریق سازوکارهای اجماع غیرسیاسی توسعه داده می‌شوند.

اصل موضوع: پی بردن به سیاست‌هایی که در پَس پروتکل‌ها قرار دارد، باتوجه‌به کلمات اختصاری مبهم استانداردسازی اینترنت دشوار است. علاقه وافر پروتکل نویسان به استفاده از کلمات اختصاری، مانند سامانه نام‌گذاری دامنه (دی ان اس) بر روی پروتکل امنیتی لایه انتقال (تی ال اس)[۱] یا DoT، در این زمینه کمکی نمی‌کند.

پیشینه: اینترنت به واسطه مجموعه‌ای از استانداردها و پروتکل‌های فنی اداره می‌شود. اولین نسخه اینترنت به‌دنبال نیاز به برقراری ارتباط بین شبکه‌های متفاوت شکل گرفت (ارجاع به اسطوره ۱۵). پروتکل‌های اینترنت با ارائه یک روش استاندارد برای تبادل اطلاعات بین شبکه‌ها، «اینترنت تعاملی» را امکان‌پذیر کردند. این پروتکل‌ها توسط نهادهای استانداردسازی صنعتی، مانند کارگروه مهندسی اینترنت[۲] تهیه شده‌اند. بسیاری از عوامل این سازمان‌ها معتقدند که در این پروتکل‌ها سیاسی‌کاری وجود ندارد؛ این پروتکل‌ها فی‌نفسه خنثی تلقی می‌شوند، نحوه استفاده مردم از آنهاست که ممکن است آثار اخلاقی یا سیاسی به جای بگذارد. این یک باور نادرست است چراکه بر این پیش فرض، استوار است که این سازمان‌های فنی از بافت[۳] گسترده‌تر خود منفک هستند و پروتکل‌های خنثی می‌سازند. حال آنکه پروتکل‌ها ساخته دست انسان‌هایی هستند که ارزش‌ها، ایدئولوژی‌ها و فرضیات خود را رمزگذاری می‌کنند (ارجاع به اسطوره ۱۸ و ۴۲). بنابراین این پروتکل‌ها دارای بار معنایی سیاسی هستند. درواقع سؤال این است: این پروتکل‌ها متعلق به چه کسی؟ به‌عنوان‌مثال به «پروتکل رمزنگاری DoT» توجه کنید: طراحان آن حریم خصوصی کاربران را در برابر دسترسی تجاری یا دولتی به اطلاعات مربوط به وب‌سایت‌های مورد بازدید کاربران در اولویت قرار می‌دهند. این اولویت‌بندی به‌نوبهٔ خود بر کشمکش قدرت بین ذی‌نفعان مختلف (دولت‌ها، صنعت، جامعه مدنی) بر سر جریان اطلاعات برخط تأثیر می‌گذارد.

1. Domain Name System (DNS) over Transport Layer Secure (TLS)
2. Internet Engineering Task Force (IETF)
3. Context

«ماهیت سیاسی پروتکل‌ها» برای آن دسته از افرادی که تأثیرات آن را تجربه می‌کنند یا در آن حوزه به تحقیق و مطالعه پرداخته‌اند تعجب‌آور نیست. لنگدون وینر در مقاله مطرح خود در سال ۱۹۸۰، نشان داد که فناوری به لحاظ ارزشی خنثی نیست، چراکه نشانگر انتخاب‌های اخلاقی و سیاسی متمایزی می‌باشد. چندی پیش، لورا دناردیس[1] استدلال کرد که پروتکل‌ها دارای ساختار سیاسی هستند چراکه ارزش‌های اجتماعی و سیاسی شکل‌دهنده جامعه را از فیلتر فناوری عبور می‌دهند. به‌همین‌ترتیب، جوامع متأثر از طراحی پروتکل‌ها—که دغدغه حراست از قوانین مرتبط به عدم دسترسی به وب‌سایت یا مباحث مرتبط با حقوق بشر از جمله حریم خصوصی را دارند—ماهیت سیاسی پروتکل‌ها را مورد توجه بیشتری قرار داده‌اند. حال آنکه، این باور نادرست که پروتکل‌ها سیاسی نیستند همچنان در میان بسیاری از افراد جامعه فنی وجود دارد که بعضاً به زیان کاربران اینترنت منجر می‌شود.

حقیقت: تأکید بر این‌که «پروتکل‌ها سیاسی نیستند»، خود نوعی «سیاسی‌بازی» است، زیرا این نوع رفتار به منزله تعهد به شرایط موجود تلقی می‌شود-که غالباً هم‌سو با ارزش‌های جهان شمال[2] و منافع صنعتی آنها می‌باشد– که باعث استانداردسازی اینترنت می‌شود. این رفتار همچنین از نحوه روند استانداردسازی اینترنت در برخی شرایط فرهنگی، اقتصادی و سیاسی خاص چشم‌پوشی می‌کند. پروتکل‌ها، سیاسی‌کاری‌هایی دارند و تعامل انتقادی بیشتر با آنها با تمرکز بر پیامدهای این سیاسی‌کاری‌ها، ضروری است.

1. Laura DeNardis
2. Global North (منظور کشورهای پیشرفته موسوم به شمال شامل شمال آمریکا و اروپای غربی است)

اسطوره پنجم: مجرمان سایبری آزادانه می‌چرخند[1]

آمادئوس پیترز[2]

باور عمومی: ناشناس ماندن در اینترنت امری بسیار ارزشمند برای مجرمان می‌باشد. آنها برای مخفی‌سازی هویت خود از ابزارهای مخفی ساز مانند مرورگر Tor استفاده می‌کنند که به‌خودی‌خود امکان دسترسی آنها را به «دارک‌نت»[3] نیز فراهم می‌کند، و می‌توانند تعاملات مالی خود را از طریق ارزهای رمزگذاری شده[4] همچون بیت‌کوین انجام دهند. بنابراین شناسایی مجرمان سایبری توسط پلیس غیرممکن می‌شود.

اصل موضوع: باوجود ابزارهای بسیار پیشرفته برای پنهان‌سازی هویت افراد در اینترنت، نیروهای انتظامی کشورهای سراسر جهان توانسته‌اند تعداد زیادی از مجرمان سایبری سابقه‌دار یا تازه‌کار را به دام بیندازند. این واقعیت همچنین شامل حال مشتریان، بازاریاب‌ها و عاملان درگاه‌های فروش خدمات بازارهای دارک‌نت (ارجاع به اسطوره ۱۷) می‌شود که اقلامی مانند موادمخدر، پول تقلبی و اسلحه را می‌فروشند.

به‌عنوان یک نمونه بارز، می‌توان از عملیات بین‌المللی پلیس تحت عنوان «بایونت»[5] در سال ۲۰۱۷ نام برد. پلیس هلند گزارشی مبنی‌بر ارتباط یک شرکت با سروری که به‌طورآزمایشی خدمات ویژه دارک‌وب «هانزا»[6] را ارائه می‌داد، دریافت نمود. در آن زمان هانزا سومین درگاه فروش خدمات «دارک‌وب» در دنیا بود. پلیس هلند با پایش ارتباطات ایجاد شده با سرور به این مهم که سرور مذکور درواقع سرور میزبان «هانزا» است پی برد. بنابراین پلیس توانست به‌صورت مخفیانه نسخه‌ای از داده‌های ذخیره شده را تهیه کند و طی آن به تاریخچه مکالمات میان عاملان سایت با نام‌های واقعی آنها دست پیدا کند.

به دلایل نامعلوم، این وب‌سایت به‌سرعت به سرورهای ناشناخته جدیدی منتقل گردید. شرکت

---

1. **Source:** Y. Danny Huang et al., Tracking Ransomware End-to-end, IEEE Symposium on Security and Privacy (2018), https://ieeexplore.ieee.org/document/8418627; Jonathan Lusthaus, Industry of Anonymity (Cambridge, MA: Harvard University Press, 2018).
2. Amadeus Peters
3. Darknet
4. Cryptocurrencies
5. Bayonet
6. Hansa

تأمین‌کنندهٔ هاست جدید که در پی کشف اطلاعات ذخیره شده در سرور پیشین مشخص شده بود، در بستر «بیت‌کوین» تعاملات مالی داشت. ازآنجاکه تعاملات مالی در بلاکچین «بیت‌کوین» به‌صورت آشکار انجام می‌شود، پرداخت‌ها تا زمان تبدیل بیت‌کوین به یورو قابل پیگیری هستند. بنابراین مبادلات بیت‌کوین در نهایت هویت واقعی مشتریان که همان شرکت ارائه دهنده هاست جدید بود را به درخواست پلیس فاش کرد. پلیس آلمان مدیران سایت را دستگیر نمود و ازسوی‌دیگر پلیس هلند دسترسی به وب‌سایت هانزا را در اختیار گرفت که طی آن افسران پلیس خود را به‌عنوان سرپرستان سایت معرفی نمودند. پلیس هلند با اعمال تغییراتی در ارتباطات رمزگذاری‌شده بین مشتریان و فروشندگان آدرس ۱۰۰۰۰ محل تحویل را در اختیار آنها قرار داده است. ازسوی‌دیگر، با شبیه‌سازی مشکلات فنی، فروشندگان را وادار کرد تا کالاها را مجدداً بارگذاری کنند و در پی آن با دسترسی به اطلاعات ذخیره شده در فراداده[1] تصاویر اطلاعات ۵۰ فروشنده در اختیار پلیس قرار گرفت. علاوه‌براین، پلیس توانست با ترغیب ۶۴ فروشنده به باز کردن یک فایل، آدرس آی‌پی[2] واقعی آنها را مشخص کند. پس از جمع‌آوری این داده‌ها، وب‌سایت بسته شد و پلیس عملیات دستگیری فروشندگان و مشتریان را آغاز نمود. این مثال نشان می‌دهد که پلیس نه‌تنها می‌تواند به «هویت مخفی» افراد دست پیدا کند، بلکه از این ویژگی به نفع خود نیز بهره‌مند می‌شود. علاوه‌براین، برای دریافت کالاها یا پول رایج، آن فرد می‌بایست از دنیای مجازی خارج شود که این امر به‌خودی‌خود باعث از بین رفتن هرگونه پوشش هویتی یا مخفی‌کاری وی می‌شود.

حقیقت: باوجود گسترش و توسعه ابزارهای «مخفی‌سازی هویت» و به‌دلیل خطاهای انسانی و حوادث مختلف دیگر که به‌خودی‌خود اطلاعات مهمی در جهت شناسایی هویت واقعی تبهکاران در اختیار پلیس قرار می‌دهد، تبهکاران سایبری به دام می‌افتند. علاوه‌براین، بسیاری از ارزهای رمزنگاری شده تراکنش‌ها را مخفی‌سازی نمی‌نمایند، بلکه تنها نام مستعار به طرفین معامله اختصاص می‌دهند و بدین‌ترتیب امکان رصد و تحلیل جریان‌های مالی را ممکن می‌سازند. در نهایت مجموعه این تعاملات امکان تعقیب و دستگیری تبهکاران سایبری در دنیای واقعی را برای نیروهای انتظامی فراهم می‌سازد.

---

1. Metadata
2. IP address

اسطوره ششم:در فضای برخط شما می‌توانید هر چیزی را بیان کنید[1]

امیلی لیدلو[2]

باور عمومی: اینترنت فضایی رایگان و در دسترس عموم است که در آن نفرت‌پراکنی، افترا و سایر اشکال سوءاستفاده از ابزار کلامی بدون حدومرز یا عواقبی صورت می‌پذیرد. به‌عنوان‌مثال، اگر فردی محتوای زننده یا قابل سوءاستفاده‌ای را در شبکه‌های اجتماعی به اشتراک بگذارد، این عمل به‌خودی‌خود جرم محسوب نمی‌شود و امکان پیگرد و تعقیب آن از طریق مراجع قانونی وجود ندارد.

اصل موضوع: عوامل بسیاری در جهت محدودسازی «بیان» ما در دنیای مجازی وجود دارند: قوانین، هنجارها، معیارهای اجتماعی، ساختارهای حمایتی، هوش مصنوعی و بازار. مجموعه عوامل فوق‌الذکر نظام حکمرانی «بیان اینترنتی»[3] را شکل می‌دهند (ارجاع به اسطوره ۱ و ۲). در این ساختار، حقوق بشر به‌عنوان نقطه عطف نظری لحاظ می‌شود (باوجود اختلاف‌نظر در چگونگی تعریف و اعمال حقوق بشر در شرایط دشوار). قوانین حقوق بشر از حق آزادی بیان به‌عنوان جزء لاینفک مردم سالاری جهت ایجاد حس عزت نفس و کرامت انسانی و جستجوی حقیقت حمایت می‌کند. باوجوداین، این حقوق با وظایف و تعهداتی همراه است؛ از جمله عدم پایمال کردن حقوق، شهرت یا زندگی خصوصی دیگران ازیک‌سو و از بین بردن امنیت ملی یا نقض سلامت عمومی یا اخلاقیات ازسوی‌دیگر.

ایده آزادی بیان به‌عنوان یک حق و مسئولیت اجتماعی، لایه‌های مختلفی از ساختار حکمرانی برخط را شامل می‌شود. درواقع قوانین داخلی[4] نیز تمایل دارند آزادی بیان را این‌گونه تفسیر کنند. قوانین جزایی و مدنی اظهاراتی که به‌طورخاص باعث آسیب رساندن به جامعه می‌شوند از جمله نفرت‌پراکنی، ترویج نسل‌کشی، افترا یا سخنان تروریستی را ممنوع می‌شمارند. یکی از چالش‌های مهم دنیای مجازی دشوار بودن ردیابی متخلفان است (ارجاع به اسطوره ۵) که این مهم به‌دلیل

1. **Source:** Emily Laidlaw, Regulating Speech in Cyberspace: Gatekeepers, Human Rights and Corporate Responsibility (Cambridge University Press, 2015); David Kaye, Speech Police: the Global Struggle to Govern the Internet (Columbia Global Reports, 2019).

2. Emily Laidlaw

3. Governance Of Online Expression

۴. منظور قانون داخلی کشورها است.

قرار گرفتن آنها در خارج از حوزه قضایی کشورها (گرچه اغلب قابل شناسایی و پیگیری هستند) یا انتقال این «بیانات» از طریق کانال‌های خصوصی است. بنابراین، قوانین و راهکارهای سنتی نظارت و پایش «بیانات» در ساختارهای مجازی کم‌اثر می‌شود.

با این‌حال برخی دیگر از اشکال «مقررات گذاری» در مسیر پُر کردن این شکاف (ضعف) گام برداشته‌اند که برخی از آنها نوآورانه و برخی دیگر ناشیانه بوده‌اند. شرایط و سازوکارهای معمول در استفاده از شبکه‌های اجتماعی به‌خودی‌خود قوانین محدودکننده‌ای حول محور حق «آزادی بیان» از قبیل حق برهنگی یا اعمال خشونت‌بار ارائه می‌دهند. کاربرد هوش مصنوعی به‌طور فزاینده‌ای در جهت اعمال محدودیت‌ها و مشخص نمودن حریم فردی و به‌صورت حذف نمودن محتوای مجرمانه به‌کار گرفته می‌شود. در برخی از سایت‌ها، جامعه کاربران حدود قوانین مرتبط با آزادی بیان را مشخص می‌نماید که این خود با معرفی هنجارهای اجتماعی غیررسمی در قالب استفاده از قوانین مدیران متبلور می‌شود؛ البته ناگفته نماند که این مسئله خود باعث ظهور اشکال دیگری از سخنان آزاردهنده توسط مردم می‌شود. جامعه مدنی و اجتماعات با درخواست از پلتفرم‌ها برای حذف یا بازگرداندن محتوا یا گروه‌های خاص، کلام را قانونمند می‌سازد. ازسوی‌دیگر بازار نیز «آزادی بیان» را یا از طریق ارائه ساختارهای کلامی جایگزین به کاربران قانونمند می‌نماید یا با اعمال قدرت و تسلط فناورانه مانع از بروز آنها می‌شود.

حقیقت: اینترنت بهشتی برین برای آزادی بیان نیست که در آن هر سخنی بدون در نظر گرفتن تبعات می‌تواند بیان شود. در واقع، «بیان» در ساختار برخط از طریق یک نظام پیچیده حکمرانی شامل قوانین، هنجارها، معیارهای اجتماعی، قوانین حمایتی، هوش مصنوعی و بازار نظام‌مند می‌شود. این‌که آیا شما می‌توانید هرچه می‌خواهید در فضای برخط بیان کنید دغدغه اصلی نیست چراکه پاسخ آن مشخص است: خیر! نمی‌توانید. در عوض، پرسش اصلی این است که چطور می‌توان نظامی را در راستای مدیریت آزادی بیان ایجاد نمود که در برابر حفظ اصول حقوق بشر مؤثرتر و حساس‌تر باشد.

اسطوره هفتم: پلتفرم های اینترنتی مسئولیتی در قبال محتوای تولیدشده توسط کاربران ندارند[1]

آملی پیا هلد[2]

باور عمومی: پلتفرم‌های اینترنتی صرفاً به‌عنوان مجرایی[3] برای تولید محتوا توسط کاربر محسوب می‌شوند. به‌بیان‌دیگر، سایت‌ها به مثابه مجرایی برای انتقال محتوا می‌باشند که خود اطلاعی از محتوا ندارند، به‌همین‌دلیل است که آنها مسئولیت یا تعهدی در قبال محتوای غیرقانونی بارگذاری شده توسط کاربرانشان ندارند.

اصل موضوع: در ابتدا، پلتفرم‌های اینترنتی به‌عنوان توزیع کننده محتوا محسوب می‌شدند تا به‌عنوان عامل نشر: پلتفرم‌هایی با محتوای خنثی که این امکان را در اختیار کاربران خود قرار می‌دادند که مطالب را بدون بازبینی یا بررسی به اشتراک بگذارند. این اصل با عنایت به بند ۲۳۰ «قانون رفتار سالم در ارتباطات» ۱۹۹۶[4] (که از این پس با عنوان بند CDA ۲۳۰ از آن نام برده می‌شود) به یک قانون اینترنتی مهم در ایالات متحده تبدیل شد که براساس آن (به زبان ساده) هیچ نوع «خدمات رایانه‌ای تعاملی[5]» نمی‌تواند به‌عنوان عامل نشر و یا تشریح محتوا در نظر گرفته شود. ازاین‌رو، هیچ‌گونه مسئولیتی در قبال محتوای تولیدشده توسط کاربران[6] متوجه آنها نمی‌باشد. پلتفرم‌های اینترنتی تنها زمانی مسئولیت محتوای تولیدشده توسط کاربران را می‌بایست برعهده بگیرند که تحت قوانین کیفری فدرال و مالکیت معنوی در مظان اتهام قرار بگیرند و یا به‌عنوان ویراستار در محتوای تولیدشده نقش داشته باشند. منشأ این قانون را می‌توان تصمیم دیوان عالی کشور (اسمیت وی. کالیفرنیا[7]) در رابطه با مسئولیت صاحب یک کتاب‌فروشی در مقایسه با مسئولیت صاحب اثر دانست: این دادگاه اعلام نمود که به صرف در

1. **Source:** Daphne Keller, Toward a Clearer Conversation About Platform Liability, Knight First Amendment Institute's "Emerging Threats" Essay Series (2018), https://knightcolumbia.org/content/towardclearer-conversation-about-platform-liability; Aleksandra Kuczerawy, Intermediary Liability & Freedom of Expression: Recent Developments in the EU Notice & Action Initiative (2014), Computer Law and Security Review 31 (2015) 1, 46-56; CiTiP Working Paper 21/2015,https://ssrn.com/ abstract=2560257.
2. Amélie Pia Heldt
3. Conduit
4. 1996 Communications Decency Act
5. Interactive Computer Service
6. User Generated Content (UGC)
7. Smith v. California

اختیار داشتن یک کتاب حاوی تصاویر مستهجن، بدون این‌که فرد اطلاعی از محتوای مجرمانه آن داشته باشد، مسئولیتی (اتهامی) متوجه وی نمی‌شود. چنین اتهامی ذیل متمم اول قانون اساسی[1] مردود اعلام شده است، هرچند خود بیان و تصاویر مستهجن مورد حمایت قانون نیست. سایر کشورها قوانین مشابهی را تصویب کرده‌اند، از جمله بند ۷۹ قانون فناوری اطلاعات هند[2]، که مصونیت مشروط[3] برای واسطه‌ها (از جمله پلتفرم‌ها) ارائه می‌دهد یا ماده ۱۴ دستورالعمل تجارت الکترونیک اتحادیه اروپا به شماره ۳۱/۲۰۰۰/ای سی[4].

با این‌حال، طی پنج سال اخیر تغییر چشمگیری رخ داده است: ساختار قانون‌گذاری اتحادیه اروپا و قانون‌گذاران اروپایی به سمت اعمال قوانین سخت‌گیرانه‌تری در جهت مسئولیت‌پذیری هرچه بیشتر پلتفرم‌ها در قبال محتوای منتشر شده حرکت نموده‌اند. در مسیر معرفی تقسیم وظایف عادلانه‌تر، مصونیت واسطه‌ای[5] در قبال مواردی از جمله نفرت‌پراکنی، هراس‌افکنی یا نقض کپی‌رایت و قوانین مرتبط با بند ۱۷ (۳) دستورالعمل حق چاپ در اتحادیه اروپا در سال ۲۰۱۹ در بازار تک دیجیتال[6] به‌طور فزاینده‌ای محدود گردیده است. براساس همه این محدودیت‌های اعمال شده از سوی قانون‌گذاران اروپایی، پلتفرم‌ها به‌خاطر به اشتراک‌گذاری محتوای ناقض قانون کپی‌رایت و سایر موارد نقض قانون مسئول شناخته می‌شوند. بنا بر قانون اجرای شبکه آلمان (۲۰۱۷)[7]، پلتفرم‌ها می‌بایست از وجود ساختار کارآمد جهت ثبت شکایات راجع به محتوای مجرمانه[8] اطمینان حاصل نمایند. بر اساس برخی پیشنهادهای تصویب نشده اتحادیه اروپا، پلتفرم‌ها می‌بایست از اعمال فیلترهای پیشگیرانه (مثلاً با استفاده از هوش مصنوعی) روی محتوای ایجاد شده توسط کاربران در جهت جلوگیری از بارگذاری محتوای ناقض قانون کپی‌رایت و دیگر قوانین جلوگیری نمایند که البته این پیشنهادات محل اختلاف نظر شدید می‌باشد (ارجاع به اسطوره ۶). به‌طورکل، مسئول دانستن پلتفرم‌ها نمایانگر شیوه متفاوت قانون‌گذاری درایالات متحده و اتحادیه اروپا است.

---

1. First Amendment
2. Section 79 Of The Indian Information Technology Act
3. Qualified Immunity
4. Article 14 Of The Eu's E-Commerce Directive 2000/31/Ec
5. Intermediary Immunity
6. 2019 Eu Copyright Directive In The Digital Single Market
7. German Network Enforcement Act (2017)
8. Manifestly Unlawful Content

صرف‌نظر از محدودیت‌های تصویب شده توسط قانون‌گذاران، اصل این موضوع خودش بحث‌برانگیز است. اساس این مصونیت واسطه‌ای نسبی که همان بی‌طرفی آنها درباره محتوا می‌باشد، در بیشتر موارد یک خیال واهی بیش نیست. پلتفرم‌ها عامل طبقه‌بندی، اولویت‌بندی و مدیریت محتوی تولیدشده توسط کابران هستند. فناوری به آنها این امکان را می‌دهد تا به‌صورت گسترده‌ای محتوا را پیش از آنکه توسط کاربر به‌عنوان محتوای مجرمانه بررسی و گزارش شود، شناسایی و حذف نماید که در این شکل مثال پیشین راجع به بی‌اطلاعی صاحب کتاب‌فروشی از محتوای کتب موجود در قفسه کتابخانه را بی‌اثر می‌کند.

حقیقت: پلتفرم‌های اینترنتی را نمی‌توان صرفاً به‌عنوان عاملان توزیع محتوایی در نظر گرفت که هیچ اطلاعی از محتواها ندارند یا درخصوص این داده‌ها بی‌طرف هستند. اگرچه طی قوانین ایالات متحده مسئولیت‌پذیری پلتفرم‌ها به‌شدت محدود شده است، قوانین اروپایی ساختار مسئولیت‌پذیری شفاف‌تری دراین‌راستا برگزیده است؛ به‌خصوص با در نظر گرفتن قوانین مالکیت معنوی و محتوای کاملاً غیرقانونی و جرائم سنگین مانند ترویج تروریسم یا نژادپرستی.

اسطوره هشتم: اینترنت همواره بر اساس رویکردهای چندذی‌نفعی[1] عمل کرده است [2]

رکسانا رادو[3]

باور عمومی: ماهیت غیرمتمرکز اینترنت مستلزم تعامل گروه‌های ذی‌نفع مختلف از جمله دولت‌ها، صنعت و جامعه مدنی است. برخلاف سایر زمینه‌های سیاسی که رویکردهای بین دولتی در آنها حاکم است، اینترنت از ابتدای راه با مفهوم حاکمیت چندذی‌نفعی هم معنی بوده است و به این دلیل امکان استفاده یکسان به همه کاربران می‌دهد.

1. Multistakeholder
2. **Source:** Roxana Radu, Negotiating Internet Governance (Oxford: Oxford University Press, 2019); Mark Raymond and Laura DeNardis, Multistakeholderism: Anatomy of an Inchoate Global Institution, International Theory 572-616 7(2015)3.
3. Roxana Radu

اصل موضوع: اکثر خوانش‌های موجود از حکمرانی اینترنت ماهیت چنددی‌نفعی آن را یک دستاورد تلقی می‌کنند که طی آن امکان مشارکت در تصمیم‌گیری‌ها به دولت‌ها، مشاغل، جامعه فنی، دانشگاه‌ها و جامعه مدنی داده می‌شود؛ چه در نقش مشورتی و چه به‌عنوان بخشی از تلاش‌های مشترک در راستای ایجاد قانون. با این‌حال، تصمیماتی که منجر به تأمین بودجه، ایجاد و خصوصی‌سازی اینترنت گردیده‌اند نتیجه فرایندهای چنددی‌نفعی نیستند، بلکه به‌صورت یک‌جانبه توسط دولت ایالات متحده مطرح شده‌اند. در حال حاضر اینترنت که توسط بیش از ۳۰۰ سند نظارتی بین‌المللی و منطقه‌ای (و بسیاری دیگر در سطح ملی) اداره می‌شود، را می‌توان حاصل سازوکارهای مختلف دانست که بخش اعظم آنها ساختاری منحصراً دولتی یا صنعت‌محور دارند.

رویکرد چنددی‌نفعی اینترنت، در قیاس با مدل بین دولتی که بیشتر برای مدیریت و قانون‌گذاری ساختارهای ارتباطات از راه دور استفاده می‌شود، به‌عنوان بهترین روش برای اداره اینترنت مطرح می‌شود که در دوران ابتدایی شکل‌گیری اینترنت توسط جامعه فنی معرفی و پایه‌گذاری گردید. از زمان ظهور ساختار چنددی‌نفعی در اواسط دهه ۱۹۹۰، این ساختار در عمل به‌عنوان نوعی «لنگر اندازی اجتماع» تلقی می‌شود.

تعامل نمایندگان بخش‌های مختلف طی مذاکرات مربوط به مدیریت نظام نام‌گذاری دامنه[1]، کاملاً مشهود بود، فعالیتی که پیش از این به‌صورت یک‌جانبه توسط جامعه دانشگاهی دانشگاه استنفورد (جان پاستل)[2] اداره می‌شد. در سال ۱۹۹۸، بر اساس رهنمودهای از بالا به پایین[3] {یا بر اساس دستورهای} وزارت بازرگانی ایالات متحده از طریق مذاکرات چنددی‌نفعی، یک سازمان غیرانتفاعی جدید جهت اداره این امور به نام آیکان[4] شکل گرفت. به‌دنبال آن، بسیاری از سازمان‌های دیگر از ساختار چنددی‌نفعی استقبال کردند و در راستای بهره‌گیری حداکثری از منافع نهفته در این ساختار کوشیدند.

با گذشت زمان، ساختار چنددی‌نفعی قانونمندتر گردید و مدعی مکانیسمی بارز و منحصربه‌فرد در حکمرانی اینترنت شد. تعاملات فرابخشی[5] این ساختار با فعالیت‌های خاص اعضای میان دولتی و همچنین جوامع قانونگذار را می‌توان نقطه عطف این ساختار تلقی نمود. اشکال و فرم‌های مختلف

1. DNS
2. Stanford University (Jon Postel)
3. Top-down guidance
4. ICANN
5. Cross-sector integration

آن (ریموند و دناردیس ۲۰۱۵)[1] نیز در گذر زمان دچار تحول و به‌طورگسترده‌ای نهادینه شده‌اند.

با این‌حال و در پس این روایت، حکمرانی چندذی‌نفعی اینترنت کاملا ایدئولوژیک باقی ماند و نابرابری گسترده قدرت در بین گروه‌های ذی‌نفع را پنهان ساخت. وعده تعامل برابر ذی‌نفعان کاملاً با واقعیت عملیاتی که طی آن برخی از گروه‌ها را بهره‌مند می‌سازد و آنها را به عاملان کلیدی تصمیم‌گیری تبدیل می‌نماید در تضاد است. در اصل، ساختار فوق‌الذکر را می‌توان رویکردی مبتنی‌بر اصل «نقش‌ها و مسئولیت‌های مربوطه» تلقی نمود که به‌طوررسمی در اسناد اجلاس سال ۲۰۰۵ سازمان ملل متحد (اجلاس سران کشورها در تونس) در رابطه با جامعه اطلاعاتی[2] مورد تصویب قرار گرفت و در بازنگری ۱۰ ساله آن مجدداً تأیید شد[3]. سایر اجلاس‌های جهانی، مانند مجمع سالانه حکمرانی اینترنت یا نت‌موندیال سال ۲۰۱۴[4] تنها به ارائه الحاقیاتی در جهت بهبود ساختار فوق پرداخته‌اند.

حقیقت: ساختار چندذی‌نفعی را می‌توان به‌عنوان فعالیتی غالب که توسط جامعه حکمرانی اینترنت در دهه ۱۹۹۰ میلادی معرفی و پذیرفته شد تلقی نمود. با این‌حال، باوجودِ جذابیت گسترده آن، تصمیمات اصلی سیاست‌گذاری اینترنت در بخش‌های بین‌المللی، منطقه‌ای و ملی که منجر به تکامل آن شده‌اند، به‌ندرت محصول فرایندهای چندذی‌نفعی که از طریق تعامل دولت، صنعت و جامعه مدنی در شرایط برابر به‌دست می‌آید، می‌باشد.

اسطوره نهم: در اینترنت همه چیز رایگان است[5]

کورت ام. ساندرز[6]

باور عمومی: اگر چیزی در اینترنت قرار دارد، به‌معنای رایگان بودن و قابل دسترس بودن

1. Raymond and DeNardis 2015
2. UN Summit on Information Society
3. WSIS + 10
4 . 2014 NETMundial
5. **Source:** Understanding Copyright and Related Rights, World Intellectual Property Organization (2016), https://www.wipo.int/edocs/pubdocs/en/wipo_pub_909_2016.pdf; Kurt M. Saunders, Intellectual Property Law: Legal Aspects of Innovation and Competition (St. Paul, MN: West Academic, 2016).
6. Kurt M. Saunders

آن برای عموم است. بسیاری از کاربران به اشتباه باور دارند که رسانه و محتوای برخط از قانون کپی‌رایت تبعیت نمی‌کند. در دسته دیگری از کاربران این باور به‌صورت ناخودآگاه ایجاد شده که باعث می‌شود محتوای دیجیتال را نسخه‌برداری و بازنشر یا بدون کسب اجازه از مالک آن، از آن استفاده نمایند.

اصل موضوع: به نظر می‌رسد این باور که محتوای موجود در اینترنت رایگان است یا توسط قانون کپی‌رایت پوشش داده نمی‌شود، بر دو پایه استوار است که درواقع هر دوی این دلایل با یکدیگر مرتبط هستند. دلیل اول ریشه در فناوری دارد. اینترنت به‌طورگسترده‌ای هزینه نسخه‌برداری را کاهش می‌دهد و در نتیجه دسترسی، تکثیر، انتقال و تغییر محتوا را به امری آسان و کم‌هزینه تبدیل می‌نماید. کاربران می‌توانند نسخه‌های متعددی از یک محتوا را به گیرندگان بی‌شماری در سراسر دنیا در کوتاه‌ترین زمان ارسال نمایند. دلیل دوم ساختاری فلسفی دارد و ریشه در این نقل قول دارد که: «اطلاعات به رایگان بودن گرایش دارد» (ارجاع به اسطوره ۴۸). این نقل قول به استوارت برند[1] در اولین کنفرانس هکرها[2] در سال ۱۹۸۴ منتسب شده است که پس از آن به سرلوحه «جنبش سایبرپانک»[3] تبدیل گردید. به‌طورخلاصه، این برداشت برآن است تا محتوای موجود در اینترنت را مفهومی خارج از قوانین کپی‌رایت و سایر قوانین محدودکننده معرفی نماید. در سال ۱۹۹۶، جان پری بارلو[4]، یکی از پیشگامان اینترنت و بنیان‌گذار «بنیاد مرز الکترونیکی»[5]، برداشت فوق را در «بیانیه استقلال فضای مجازی»[6] با اعمال تغییراتی مجدداً به‌کار گرفت: «قوانین حقوقی شما در مورد اموال، بیان، هویت، جریان‌ها و محتوا شامل ما نمی‌شود زیرا این قوانین بر اساس ارجاع به ماده شکل گرفته‌اند. حال آنکه در فضای اینترنت ماده وجود ندارد».

با این‌حال، همانند سایر آثار فیزیکی موجود؛ هرآنچه در اینترنت یافت می‌شود نیز به‌عنوان اثری اصلی با مالکی مشخص تحت پوشش قانون کپی‌رایت قرار می‌گیرد.

این مهم شامل نرم‌افزار، تصاویر، متن، ویدیوها، موسیقی، جداول، نمودارها و همچنین پست‌های ارسال شده در رسانه‌های اجتماعی و وبلاگ‌ها می‌شود. هیچکدام از این موارد به‌صورت خودکار، تنها به‌دلیل این‌که در اینترنت به نمایش گذاشته شده‌اند یا ارسال گردیده‌اند، در عرصه‌عمومی

1. Stewart Brand
2. Hackers Conference
3. Cyberpunk Movement
4. John Perry Barlow
5. Electronic Frontier Foundation
6. Declaration of Independence in Cyberspace

و دسترسی آزاد قرار نمی‌گیرند. قانون کپی‌رایت شامل «بیان» از جمله برنامه‌های رایانه‌ای نیز می‌شود، اما ایده‌ها، رویه‌های اجرایی، عملکردها و یا مفاهیم ریاضی را در بر نمی‌گیرد.

باتوجه‌به جنبه‌های تجاری توافق‌نامه مالکیت معنوی[1]، که شامل کلیه کشورهای عضو سازمان تجارت جهانی می‌شود، حداقل زمان تحت پوشش قانون کپی‌رایت برابر است با طول عمر مالک یا صاحب اثر به‌علاوه حداقل ۵۰ سال پس از آن. البته ناگفته نماند بعضی اعضا، از جمله ایالات متحده و کشورهای اتحادیه اروپا، مدت زمان تحت پوشش قانون کپی‌رایت پس از فوت صاحب اثر را ۷۰ سال لحاظ می‌نمایند. پس از انقضای مدت زمان تحت پوشش قانون، حق نسخه‌برداری آن اثر وارد عرصه عمومی و دسترسی رایگان می‌گردد. ازطرف‌دیگر، برخی از صاحبان اثر، آثار خود را به عرصه عمومی و دسترسی رایگان اختصاص می‌دهند. این مهم به‌معنی خودداری از دریافت هرگونه مبلغ حاصل از فروش آن اثر می‌باشد. مدل‌های متفاوتی جهت تعامل با کاربران برای صاحبان اثر وجود دارد که طی آن می‌توانند از برخی از حقوق چشم‌پوشی نمایند یا اثرخود را با اعمال محدودیت‌های اندک در اختیار عموم قرار دهند، مانند قوانین تحت شبکه «مشترکات مبتکرانه»[2]و جریان منبع/متن باز[3] برای نرم‌افزارها.

حقیقت: اکثر محتوای موجود در اینترنت تحت پوشش قانون کپی‌رایت قرار دارد و بنابراین در دسترس عموم و جهت استفاده آزاد، کپی‌برداری، تطبیق یا نمایش عمومی، اجرا یا انتشار بدون کسب اجازه از صاحب آن، قرار ندارد. تنها زمانی اثر برای استفاده آزاد و بدون نیاز به کسب اجازه در دسترس عموم قرار می‌گیرد که صاحب اثر مشخصاً آن اثر را به عرصه عمومی[4] اختصاص داده باشد.

1. Trade-Related Aspects of Intellectual Property Agreement (TRIPS)
2. Creative Commons
3. Open Source
4. Public Domain

فصل دوم
امنیت و ایمنی

اسطوره دهم: جنگ سایبری در راه است[1]

ماتیاس شولز[2]

باور عمومی: جنگ‌های سایبری اجتناب‌ناپذیرند. اقتصادهای مدرن به‌شدت به رایانه‌ها که در برابر هک شدن آسیب‌پذیر هستند وابسته می‌باشند. یک حمله سایبری راهبردی علیه یک زیرساخت کلیدی مانند شبکه برق می‌تواند کل یک اقتصاد را فلج کند و به زانو درآورد و منجر به تلفات گسترده‌ای شود. مسئله اصلی امکان وقوع حمله نیست!، بلکه زمان وقوع آن است که اهمیت دارد.

اصل موضوع: در سال ۱۹۹۱، امکان وقوع نسخه دیجیتالی حادثه پرل هاربر[3]، یا به‌عبارتی حمله سایبری غافلگیرانه با هدف قرار دادن کارکردهای راهبردی یک دولت-ملت و در پس آن فلج کردن کل اقتصاد، برای نخستین‌بار در اذهان عمومی شکل گرفت. از آن زمان بود که جمله «جنگ سایبری در راه است!» را به کرّات شنیده‌ایم، زیرا ماهیت فراملّی میدان نبرد دیجیتال به مهاجمان اجازه می‌دهد از هر مکان و هر زمانی جهت حمله استفاده نمایند. موضوع احتمال وقوع حمله

1. **Source:** Thomas Rid, Cyber war will not take place (London: Hurst, 2013); Brandon Valeriano and Ryan C. Maness, Cyber War versus Cyber Realities (Oxford: OUP, 2015)
2. Matthias Schulze
3. Pearl Harbor

نیست، بلکه زمان چنین حمله سایبری مهلکی حائز اهمیت می‌باشد (آرکوئیلا و رانفلت،۱۹۹۳[1]). این سناریو آخرالزمانی سایبری به دفعات بازخوانی شده است و به‌همین‌دلیل در راهکارهای جهانی سایبری اعمال می‌گردد (ارجاع به اسطوره ۱۳). باوجود این‌که سالانه میلیون‌ها حالت مختلف از «حملات سایبری» رخ می‌دهد، تنها تعداد معدودی از آنها تأثیری قابل تأمل ایجاد کرده‌اند[2].تا به امروز، هیچ حادثه سایبری که مستقیماً به مرگ یک نفر منجر شود صورت نگرفته است. استاکس نت[3] که سانتریفیوژهای غنی‌سازی هسته‌ای ایران را در سال ۲۰۱۰ مورد هدف قرار داده بود را می‌توان به‌عنوان مخرب‌ترین مورد در نظر گرفت. دو مثال بارز دیگر که در اذهان عمومی ثبت شده‌اند مرتبط با غیرفعال‌سازی نیروگاه برق اوکراین در سال‌های ۲۰۱۶-۲۰۱۷ می‌باشند که تنها چند ساعت دوام داشته‌اند. مهاجمان سایبری که به نیروگاه‌ها حمله می‌کنند معمولاً سعی در مختل کردن روند فعالیت نیروگاه ندارند، بلکه با نصب و ایجاد درهای مخفی[4] در سامانه‌ها امکان دسترسی به آن سامانه را برای استفاده‌های آتی مهیا می‌سازند.

باور عمومی جنگ سایبری راهبردی، مبتنی‌بر سوءبرداشت از عملکرد جنگ و قابلیت‌های سایبری است. همان‌طور که وان کلاوزویز[5] می‌نویسند، «جنگ [...] عملی خشونت‌آمیز در جهت تشویق یا سوق دادن دشمن برای سرنهادن به قدرت و ارادهٔ ماست».

بیشتر حملات سایبری در چارچوب جنگ نمی‌گنجند، زیرا این حملات خشونت‌آمیز نیستند و غالباً ناشی از انگیزه‌های مالی و به‌دور از نیات سیاسی انجام می‌شوند. فعالیت‌های جاسوسی سایبری به‌صورت مکرر صورت می‌گیرند ولی عاری از هرگونه نیت تهدید و اجبار می‌باشند (رید[6]، ۲۰۱۳). ما همچنین امکان حمله سایبری استراتژیک را با احتمال آن اشتباه می‌گیریم: این سناریو ممکن است ولی محتمل نیست. دلیل این امر این است که دستاورد سیاسی خاصی از این قبیل حملات ناگهانی حاصل نمی‌شود مگر این‌که تأثیر آن حمله با تأثیر حملات فیزیکی در هم آمیزد. بیشتر حملات سایبری تأثیر کوتاه‌مدت مخرب دارند تا ماندگار و ویرانگر. به‌بیان‌دیگر، تأثیر این دسته از حملات در مغلوب کردن یا اجبار دشمن را نمی‌توان به اندازه حملات فیزیکی در نظر گرفت (گارتزکی[7]، ۲۰۱۳). به‌همین‌دلیل است که ظرفیت‌های سایبری را اغلب به‌عنوان مکمل

1. Arquilla and Ronfeldt
2. CFR Cyber Operations Tracker2019
3. Stuxnet
4. backdoors
5. Von Clausewitz
6. Rid
7. Gartzke

درگیری‌های فیزیکی و سنتی به‌کار می‌گیرند تا روشی مستقل. تنها در این بسترها ممکن است دستاوردی سیاسی به واسطه حملات سایبری حاصل شود-که درواقع عملکرد اصلی جنگ همان ادامهٔ سیاست‌های یک کشور می‌باشد.

حقیقت: بسیاری از راهبردپردازان سایبری درباره وقوع یک حادثه پرل هاربر دیجیتال {سایبری} یا به‌عبارت‌دیگر وقوع یک حمله سایبری راهبردی که می‌تواند با از بین بردن شبکه برق (نیرو) کل اقتصاد صنعتی را فلج کند، هشدار می‌دهند. باوجود این مهم که می‌توان یک نیروگاه برق را از راه دور از کار انداخت، این فعالیت دستاورد سیاسی خاصی به همراه ندارد مگر این‌که این حمله سایبری در چارچوب یک درگیری فیزیکی سنتی اتفاق بیفتد که طی آن تأثیر آن حمله به‌صورت ماندگار باقی بماند. بنابراین ممکن است از ظرفیت‌های سایبری به‌عنوان ابزاری در تعارضات و درگیری‌های فیزیکی استفاده شود، ولی یک جنگ سایبری راهبردی مستقل و صرفاً دیجیتالی به‌وقوع نخواهد پیوست.

اسطوره یازدهم: نظارت بر تسلیحات در فضای سایبری امکان‌پذیر نیست[1]

توماس رینهولد[2]

باور عمومی: نظارت بر تسلیحات به‌عنوان بخش مهمی از برقراری صلح و امنیت بین‌المللی در فضای سایبری امکان‌پذیر نیست. این فضا از قوانینی پیروی می‌کند که از قوانین حاکم بر سایر عرصه‌ها همچون هوا، دریا، زمین و فضا کاملاً متفاوت است. بنابراین، مفاهیم و ذهنیت‌های رایج درباره مفهوم امنیت بین‌المللی و همچنین تجربیات حاصل از سایر فناوری‌های نظامی را نمی‌توان به اینترنت تعمیم داد و براین‌اساس هرگونه تلاش در جهت ایجاد ساختاری قانونمند برای نظارت بر تسلیحات سایبری اصولاً محکوم به شکست است.

1. Source: Thomas Reinhold and Christian Reuter, Arms Control and its Applicability to Cyberspace, in Christian Reuter (ed.), Information Technology for Peace and Security (Wiesbaden: Springer, 2019) , 207-231
2. Thomas Reinhold

اصل موضوع: با ظهور بدافزار استاکس نت[1] که تأسیسات اتمی ایران را در سال ۲۰۱۰ شناسایی و مورد هدف قرار داد، جامعه بین‌المللی متوجه شد که برخی از کشورها فضای سایبری را به‌عنوان فصل بعدی روند پیگیری مناقشات نظامی و جمع‌آوری اطلاعات در نظر گرفته‌اند (ارجاع به اسطوره ۱۰). این مهم باعث بروز نگرانی‌هایی راجع به امکان استفاده کشورها از تسلیحات سایبری در جهت ایجاد اختلال یا نابودی ساختارهای فناوری اطلاعات یک کشور دیگر شد، نگرانی‌هایی که با ارائه گزارش سال ۲۰۱۳ مؤسسه تحقیقات خلع سلاح سازمان ملل[2] تأیید گردید.

سیاست‌گذاران بین‌المللی چگونگی استفاده و کاربرد قوانین کنترل تسلیحات را که طی دهه‌های گذشته در جهت محدودسازی تجارت و استفاده تسلیحات مخرب و دیگر فناوری‌های تسلیحاتی وضع شده بود و همچنین نحوه انطباق و تعمیم آن در فضای سایبری را به چالش کشیدند.

رویکردهای هنجاری اولیه مانند گروه کنترل سلاح های نظامی موسوم به واسنار[3]، که درواقع توافقی در جهت کنترل تجارت و صادرات می‌باشد را می‌توان به‌عنوان راهکارهایی در جهت اعتمادسازی بین‌المللی تلقی نمود؛ اما تأثیر آنها محدود به کاهش رقابت‌های تسلیحاتی و کاهش درگیری بین کشورهای در حال جنگ بود. فضای سایبری با ویژگی‌های متمایزی مانند فوریت، غیرمادی بودن و امکان نسخه‌برداری یکپارچه از اطلاعات و داده‌ها درواقع اثرگذاری رویکردهای فوق را به چالش می‌کشد. به‌عنوان‌مثال، مشاهده تعداد فزاینده تانک‌ها در مرزها امکان‌پذیرتر از رصد نمودن بدافزارهایی است که محققان حوزه رایانه و شرکت‌های تجاری همواره در حال توسعه رویکردهایی در جهت خنثی نمودن تسلیحات سایبری هستند که علیه آنها استفاده می‌شوند. به‌بیان‌دیگر، این رویکردها را می‌توان برای آرام کردن دریای مواج رقابت تسلیحات سایبری در نظر گرفت. به‌عنوان‌نمونه می‌توان به فایل‌های موسیقی پرداخت که یکی از سهل‌الوصول‌ترین موارد با قابلیت نسخه‌برداری آسان در فضای سایبری هستند. باوجوداین، شرکت‌ها روش‌های پایش حقوق مالکیت دیجیتال را

1. Stuxnet
2. UN Disarmament Research Institute
3. Wassenaar Arrangement

معرفی نموده‌اند. این رویکردها آن‌طور که انتظار می رفت تأثیرگذار نیستند، اما از آنها می‌توان در فرهنگ‌نامه نظارت تسلیحاتی با عنوان قوانین مربوط به «تکثیر»[1] یاد نمود. سایر نمونه‌ها عبارت‌اند از: سازوکارهای بلاک‌چین[2] برای ثبت گزارش‌های دیجیتال نفوذناپذیر راجع به اطلاعات خاص، ساختار IPv6 برای شناسایی دستگاه‌های موجود در کل فضای سایبری یا پروتکل «دروازه مرزی »[3] که امکان تبادل اطلاعات میان شبکه‌های ملی فناوری اطلاعات و شکل‌گیری مفهوم سنتی مرزها را فراهم می‌آورد. اکثر این رویکردها را می‌توان باتوجه‌به منطق استفاده دوگانه[4] در روش غیرسنتی در جهت پایش تسلیحات در فضای سایبری نیز به‌کار بست.

حقیقت: فضای سایبری یک حوزه ساخته شده توسط انسان است. با نبود قوانین یا توافق‌نامه‌های مرتبط با قانون‌گذاری تسلیحات موجود در فضای سایبری، روش‌های متعددی توسط کارشناسان علوم رایانه‌ای در جهت تضمین امنیت فضای سایبری و دفاع در برابر حملات سایبری در دنیای حقیقی شکل گرفته‌اند. کنترل تسلیحات سایبری امری ممکن است ولی برای انجام آن باید فراتر از رویکردهای هنجاری فعلی رفت و آنها را منطقاً اتخاذ و عملیاتی نمود.

اسطوره دوازدهم: بهترین رویکرد دفاعی سایبری درواقع همان رویکرد تهاجمی است[5]

اسون هرپیگ[6]

باور عمومی: به‌کارگیری ظرفیت‌های سایبری در شکل تهاجمی آن و در پاسخ به حملات سایبری دشمن (که بعضاً به آنها «هک‌بک[7]» گفته می‌شود) باعث فلج نمودن تحرک مجرمان و بزهکاران وابسته به دولت‌ها می‌شود و در نهایت باعث افزایش امنیت برای دولت، مشاغل،

1. Regulation of Proliferation
2. Blockchain
3. Border Gateway
4. Dual Use Logic
5. Source: Sven Herpig, Anti-War and the Cyber Triangle: Strategic Implications of Cyber Operations and Cyber Security for the State, PhD thesis, University of Hull (2015); Sven Herpig and Thomas Reinhold, Spotting the bear: credible attribution and Russian operations in cyberspace, Chaillot Paper 148 (2018) , 33-42
6. Sven Herpig
7. Hackbacks

زیرساخت‌های کلیدی و شهروندان می‌شود (بازدارندگی مبتنی‌بر مجازات).

اصل موضوع: ایالات متحده را می‌توان به‌عنوان یکی از پیشروترین کشورها با فعالیت‌های تهاجمی سایبری با نیت تأدیب دشمنان احتمالی سایبری تلقی نمود. استفاده تهاجمی از ظرفیت‌های سایبری یکی از رویکردهای متعددی است که می‌توان به‌عنوان پاسخ به فعالیت‌های سایبری سایر کشورها در نظر گرفت. همچنین مجازات‌های سیاسی، تحریم‌های اقتصادی، عملیات سرّی، عملیات نظامی، کیفرخواست‌های حقوقی و مجازات‌های مالی هدفمند علیه افراد را نیز می‌توان به‌عنوان روش‌های جایگزین ذکر نمود.

اگر رویکرد بازدارندگی مبتنی‌بر مجازات اثرگذار می‌بود، تاکنون می‌بایست شاهد کاهش چشمگیر عملیات سایبری علیه ایالات متحده می بودیم. حال آنکه، درزهای اطلاعاتی[1] گسترده و سایر عملیات مخرب سایبری (همچون نفوذ به ایمیل‌های حزب دموکرات، درز اسرار محرمانه جنگنده اف-۳۵، درز اطلاعات شخصی افسران دولتی ایالات متحده، هک آسان اطلاعات کارت‌های اعتباری مشتریان کمپانی بزرگ اکویفکس) همچنان ایالات متحده را به ستوه آورده است. به‌دلیل ناکارآمد بودن رویکرد فوق، دولت ایالات متحده در سیاست «پاسخ به حمله» تغییراتی ایجاد نمود که براساس آن، انجام عملیات سایبری بازدارنده (پیشگیرانه) علیه عملیات سایبری خصمانه قبل از وقوع آن، جایگزین مجازات عامل حمله شد. این رویکرد در آمریکا دکترین راهبردی «دفاع پیشگیرانه» و «درگیری پایدار» نامیده شد. علاوه‌بر شکست رویکرد بازدارندگی مبتنی‌بر مجازات، اقدامات تقابلی فوری در جهت مختل کردن بسامد حملات یا بازیابی اطلاعات «ربوده شده» یا به اصطلاح «هک‌بک[2]» با چالش‌های بزرگی روبرو هستند.

انتساب یک حمله و ارائه پاسخ به‌موقع و بدون هیچ‌گونه آمادگی قبلی (از جمله بررسی و پایش آسیب‌پذیری نظام‌ها) تقریباً غیرممکن است. بنابراین این راهبرد معمولاً منجر به ناامنی‌های بیشتر فناوری اطلاعات می‌شود زیرا این امرباعث می‌شود تا عوامل مرتبط مبادرت به جمع‌آوری فهرستی از نقاط آسیب‌پذیر و نیز ابزارهای هک نمایند، بدون آنکه تضمینی برای استفاده

1. Data Breaches
2. Hackbacks

موفقیت‌آمیز از آن وجود داشته باشد. به‌جز برخی موارد خاص، از جمله کارزار سایبری منتسب به آمریکا-اسرائیل علیه فعالیت‌های غنی‌سازی هسته‌ای ایران (استاکس‌نت)، عملیات‌های سایبری هنوز از یک آستانه مشخص فراتر نرفته است و بنابراین در حال حاضر ممکن است در پایین‌ترین حد خود یا حتی در انتهای چرخه درگیری قرار داشته باشد. سایر پاسخ‌ها، مانند تحریم‌ها و مجازات‌های حقوقی از احتمال تأثیرگذاری و تناسب بیشتری در تقابل با دشمنان برخوردار هستند و نتایج بهتری به ارمغان خواهند آورد. با این‌حال هنوز داده‌هایی مبنی‌بر تأثیرگذاری و ماندگاری بالای آثار هیچ‌یک از این رویکردها در دسترس نیست.

هیچ مدرکی دال بر کارآمد بودن رویکرد دفاع تهاجمی سایبری وجود ندارد. ایالات متحده به‌عنوان بازیگر اصلی، راهبرد خود را از بازدارندگی به عملیات سایبری پیشگیرانه تغییر داده است. انتساب عملیات سایبری همچنان به‌عنوان چالشی مهم و بزرگ باقی مانده است. تحلیل حقوقی حملات امری زمان بر است و عاملان حملات سایبری به‌طور فزاینده‌ای از نرم‌افزارهای مخربی بهره می‌جویند که بر اساس ادغام هسته‌های نرم‌افزاری متعلق به سایر عاملان در جهت انجام عملیات «پرچم دروغین»[1] تشکیل شده است (Vault7). در صورتی که امر شناسایی و انتساب همچنان دشوار باقی بماند، بازداشتن عاملان حملات از فعالیت‌های تهاجمی دور از ذهن به نظر می‌رسد، چراکه دشمنان مذکور از مخفی ماندن هویت خود مطمئن هستند.

حقیقت: کاربست و یا تهدید نمودن به انجام عملیات سایبری تهاجمی پیشگیرانه از وقوع حملات دشمنان به شما ممانعت نخواهد کرد. بهره‌گیری از فناوری اطلاعات امن‌تر و سازوکارهای پایدارتر نیز مانع آنها نخواهد شد («بازدارنگی مبتنی‌بر انکار[2]»)، بلکه تنها باعث کاهش احتمال موفقیت این حملات و درنتیجه افزایش امنیت دولت، مشاغل، زیرساخت‌های کلیدی و شهروندان خواهد شد.

1. False-Flag Operations
2. "Deterrence-By-Denial

اسطوره سیزدهم: پیشرفت‌های چشمگیر در امنیت سایبری ضروری است[1]

اندرو اودلیزکو[2]

باور عمومی: اینترنت و سایر ساختارهای اطلاعاتی آن می‌بایست در جهت ارائه امنیت بهتر و قوی‌تر از نو بازنویسی شوند (مهندسی مجدد شوند). عدم انجام این امر، جامعه را در معرض خسارات مالی فزاینده قرار می‌دهد و همچنین ازسویی‌دیگر، باعث ظهور ملموس‌تر نقض حریم خصوصی و شکل‌گیری محیط ویرانگر «پساواقعیت[3]» می‌شود. در نهایت این‌که می‌تواند به‌وقوع «پرل هابر دیجیتال» منجر شود که به‌خودی‌خود باعث توقف اقتصاد می‌شود.

اصل موضوع: خطرهای سایبری واقعی و روبه‌رشد هستند (ارجاع به اسطوره ۱۰). با این‌حال، آنها تفاوت چندانی با تهدیدات موجود در دنیای فیزیکی ندارند و همانند آنها قابل کنترل می‌باشند. آنها در گذشته مدیریت شده‌اند و تجربه زندگی با آنها و نیز تجربه وابستگی به نظام‌های آشکارا ناامن طی دهه‌های گذشته، درس‌آموخته‌های مفیدی برای آینده خواهد بود. ما آموخته‌ایم که نمی‌توانیم نظام‌های ایمن و پیچیده‌ای ایجاد کنیم. حتی اگر چنین چیزی امکان‌پذیر بود، آسیب‌پذیری انسان‌ها که از طریق فنونی از قبیل فیشینگ[4] مورد سوءاستفاده قرار می‌گیرند، همچنان به قوت خود باقی خواهند ماند. باوجوداین، در گذشته صدمات ناشی از فقدان امنیت سایبری قابل تحمل بوده و میزان این‌گونه صدمات به‌طورمعمول کمتر از دیگر اشکال جرم، بلایای طبیعی و خطاهای رایانه‌ای غیرعمد[5] یا خطاهای عملیاتی بوده است. همیشه مسئله اصلی دقیقاً مانند دنیای فیزیکی، مدیریت ریسک[6] بوده است و نه امنیت مطلق. این امر به این دلیل است که امنیت مهم‌ترین هدف نیست و برای آنکه افراد و سازمان‌ها بتوانند عملکرد خوبی داشته باشند و به شکوفایی برسند، تنها سطح مشخصی از آن مورد نیاز است.

احراز هویت دو عاملی[7] نمونه بارز آن است که در سه دهه گذشته به‌صورت تجاری شناخته شده و

---

1. **Source:** Andrew Odlyzko, Cybersecurity is not very important, ACM Ubiquity, June 2019 , 1-23, https://ubiquity.acm.org/article.cfm?id=3333611.
2. Andrew Odlyzko
3. "Post-Truth" Environment
4. Phishing
5. Innocent Bugs
6. Risk Management
7. Two-Factor Authentication

در دسترس بوده، اما امروزه به‌طورگسترده‌ای به‌کار گرفته شده است. بدیهی است که در گذشته سازمان‌ها به این نتیجه رسیده بودند که استفاده از آن مزیتی ندارد و اثبات نادرست بودن این تصمیم در گذشته امری دشوار می‌نماید.

یک نمونهٔ دیگر، رصد دقیق اقدامات امنیتی استاندارد (بهره‌برداری از به‌روزرسانی‌ها، استفاده از رمزهای عبور ایمن و مواردی از این قبیل) است. این‌گونه اقدامات استاندارد و در سطح جهانی مورد قبول می‌باشند، اما به‌ندرت رعایت می‌شوند. در صورت لزوم، با رعایت این استانداردها سطح امنیت ارتقا می‌یابد.

البته خطر حملات سایبری در مقیاس بزرگ همواره وجود دارد (ارجاع به اسطوره ۱۲). تجربه نشان داده است که چنین حملاتی درواقع تنها ممکن است توسط بازیگران بزرگ دولتی صورت گیرد. ازاین‌رو، سازمان‌های دولتی باید مانع آنها شوند و بدین‌ترتیب امیدوار باشند که ابعاد این‌گونه تهدیدات گسترده‌تر از طوفان‌های عظیم ژئومغناطیسی نخواهد بود.

برای بیشتر افراد و سازمان‌ها، تنها نگرانی جدی می‌بایست حملات بزهکارانه روزمره باشد. محافظت در برابر آنها را می‌توان به روش‌های مختلفی ارتقا بخشید که مهم‌ترین آنها تهیه نسخه‌های پشتیبان و سیستم‌های مهندسی ایمن برای بازیابی سریع اطلاعات است. این اقدامات همچنین می‌توانند در جلوگیری از حملات گسترده مؤثر واقع شوند.

حقیقت: ما با یک بحران امنیت سایبری مواجه نیستیم و نیازی به بازنگری اساسی (یا مهندسی مجدد) نظام‌های اطلاعاتی اینترنت نیست. تخلفات سایبری به‌صورت کنترل شده روبه‌افزایش هستند و در حال حاضر ابزارهای زیادی برای تقویت امنیت خود در اختیار داریم. ازاین‌رو، به احتمال زیاد می‌توانیم با انجام همان اقدامات گذشته از سطح امنیتی مناسبی برخوردار شویم و در صورت لزوم گام‌های کوچکی روبه‌جلو برداریم.

اسطوره چهاردهم: تنها جنایتکاران به دنبال مخفی‌سازی هویت خود در فضای برخط هستند[1]

تورستن تیل[2]

باور عمومی: ارتباطات دیجیتال باعث پیشبرد ارتباطات ناشناس می‌شود و همین نامشخص بودن هویت باعث سر زدن رفتار غیرمسئولانه از افراد می‌شود، اعتماد اجتماعی را از بین می‌برد و تأثیر نامطلوبی بر گفتمان عمومی می‌گذارد. مخفی نگاه داشتن هویت فرصتی ناعادلانه برای سوءاستفاده از دیگران، نفرت‌پراکنی یا ارتکاب جرم است. بنابراین، می‌بایست غیرقانونی اعلام شود.

اصل موضوع: اغلب این‌گونه تصور می‌شود که ظهور ارتباطات شبکه‌ای سبب ناشناخته‌تر شدن هر چه بیشتر دنیا شده است (ارجاع به اسطوره ۵). این باور نادرست است یا دست‌کم باید به‌طور توجه‌پذیری اصلاح شود. با وجود آنکه ارتباطات رایانه‌ای همیشه با استفاده از نام مستعار صورت می‌گیرند و در اکثر مواقع فرد به‌طور قطع می‌تواند هویت خود را از سایر کاربران اینترنت مخفی نماید، توانایی بازیگران کاردان[3] مانند کشورها و نهادهای شرکتی در شناسایی و ردیابی کاربران به میزان توجه‌پذیری افزایش یافته است. ارتباطات دیجیتالی قابل ضبط، ردیابی و تحلیل هستند و شناسایی مجدد افراد، هرچند به قیمت زیر پا گذاشتن حقوق اساسی تا حدود زیادی امکان‌پذیرتر شده است. اختفای هویت در محیطی مملو از اطلاعات امری مهم است که می‌باید همواره به آن توجه شود. بنابراین، مبحث آغازین این استدلال نادرست است.

ثانیاً، مخفی ماندن هویت تنها به سود مجرمان و تبهکاران نیست (اگرچه آنها نیز ممکن است از تکنیک‌های اختفای هویت استفاده کنند). ناشناس بودن برای بسیاری از افراد یا گروه‌های مختلف جامعه امری حیاتی است. اقلیت‌ها یا فعالان سیاسی نمونه اصلی این امر هستند چراکه اغلب برای شکل‌دهی به هویت خود و بررسی نحوه موضع‌گیری خود در برابر مسائل جامعه، به فضایی امن احتیاج

---

1. **Source:** Hans Asenbaum, Anonymity and Democracy: Absence as Presence in the Public Sphere, American Political Science Review112 (2018): 1-14; Gary T. Marx, What's in a Name? Some Reflections on the Sociology of Anonymity, The Information Society 15 (1999) , 99-112

2. Thorsten Thiel

3. Resourceful Actors

دارند (ارجاع به اسطوره ۱۸). همچنین گروه‌های حرفه‌ای زیادی در جامعه وجود دارند –از جمله روزنامه‌نگاران، فعالان سیاسی و غیره- که در زمینه‌هایی فعالیت دارند که مخفی ماندن هویت فرد سبب احساس امنیت بیشتر می‌شود و می‌باید حفظ شود. در آخر، حتی افراد خودشان نیز می‌توانند در یک ساختار اجتماعی که دارای ارتباطات ناشناس می‌باشد، از مخفی ماندن هویت خود بهره ببرند. داشتن هویت مخفی به شهروندان این امکان را می‌دهد که هویت‌های مختلف را امتحان کنند (و از این طریق، دیدگاه‌های دیگران را بشناسند)، به‌مرورزمان عقاید خود را تغییر دهند و نظرهای خود را به صراحت ابراز نمایند. ناشناخته ماندن امری مهم در یک جامعه لیبرال است -به دلایل حریم خصوصی و همچنین دموکراسی (ارجاع به اسطوره ۱۷).

علاوه‌براین، مخفی بودن هویت به‌خودی‌خود باعث بروز رفتار نادرست یا غیرمسئولانه نمی‌باشد. مطالعات تجربی تا به حال نشان نداده‌اند که رفتار افرادی که به‌صورت ناشناس ارتباط برقرار می‌کنند، نامناسب‌تر از افرادی است که هویت آنها قابل شناسایی می‌باشد. تا حد زیادی به بستر ارتباطی، عوامل فرهنگی و تمایلات افراد بستگی دارد. ناشناس ماندن هویت همچنین ممکن است سبب بروز یک رفتار آزادانه‌تر و خلاقانه‌تر شود، از تعصبات جلوگیری کند یا به‌جای مدیریت شهرت[1] سطحی و سازش‌پذیر، سبب شکل‌گیری یک گفتمان برابر شود.

حقیقت: ازآنجاکه احتمال شناسایی و فاش شده هویت زیاد می‌باشد، دیگر تنها ظاهر شدن با نام مستعار در فضای برخط کافی نیست. درعوض، باید راه‌هایی برای حصول اطمینان از عدم فاش شدن هویت واقعی در دنیای دیجیتال نیز بیابیم، یا به‌عبارتی دست‌کم در برخی از بسترهای مشخص اختفای هویت از نظر قانونی تضمین شود و فناوری نیز به کمکمان بیاید. یک گفتمان اجتماعی گسترده اما دقیق در خصوص مزایا و خطرهای ارتباطات ناشناس برای دستیابی به این مهم ضرورت دارد.

1. Reputation Management

اسطوره پانزدهم: پنتاگون اینترنت را برای نجات از یک حمله هسته‌ای اختراع کرده بود[۱]

ایان پیتر[۲]

باور عمومی: در اوایل دهه ۱۹۹۰ و به‌دنبال اولین نوشته‌های روبرت کرینژلی[۳]، ستون‌نویس شایعات دره سیلیکون، این باور عمومی که اینترنت در سال ۱۹۶۹ در پنتاگون اختراع شده و هدف آن نجات از یک حمله هسته‌ای بوده است رواج پیدا کرد. در حقیقت، این فرضیه به‌قدری گسترش پیدا کرده بود که می‌توان از آن به‌عنوان «نظریه بیگ‌بنگ پیدایش اینترنت[۴]» یاد کرد.

اصل موضوع: جای تعجب ندارد که عموم مردم باور کنند که یکی از برنامه‌های آژانس پژوهشی پیشرفته دفاعی[۵]، هدفی نظامی در قالب سناریوی جنگ سرد بوده است. اما این امر در مورد آرپانت[۶] حقیقت نداشت. آرپانت اساساً با این هدف راه‌اندازی شده بود که با استفاده از علم محاسبات کاربردی امکان برقراری ارتباط میان رایانه‌های اصلی (نظامی یا غیرنظامی) را فراهم آورد. انگیزه اصلی یافتن راهی برای به‌اشتراک‌گذاری داده‌ها و اطلاعات میان سیستم‌های مختلف بود.

حقایق مربوط به آرپانت برگرفته از باب تیلور[۷] است که مسئولیت این پروژه را از ابتدای تأسیس آن در سال ۱۹۶۶ تا اواخر سال ۱۹۶۹ به عهده داشت. وی در یکی از مکاتبات خود نوشته است که «در فوریه سال ۱۹۶۶، پروژه آرپانت را راه‌اندازی کردم. از اواخر سال ۶۵ تا انتهای سال ۶۹ مدیر دفتر تکنیک‌های پردازش اطلاعات آرپا[۸] بودم. تنها دو نفر در تصمیم‌گیری در خصوص راه‌اندازی آرپانت مشارکت داشتند: رئیسم چارلز هرزفلد[۹] که ریاست آرپا را به عهده داشت و خود من. انگیزه تأسیس آرپانت عاری از هرگونه ملاحظات جنگی بود. آرپانت با این هدف راه‌اندازی شد که افرادی که از علایق مشترکی بهره می‌برند بتوانند از طریق محاسبه تعاملی[۱۰] با یکدیگر ارتباط

---

1. **Source:** Robert Taylor and others (posted by Dave Farber), Dave Farber's Interesting People Mailing list (October 2004 archives), https://seclists.org/interesting-people/2004/Oct/index.html; Ian Peter, Internet History Site, https://www.nethistory.info.
2. Ian Peter
3. Robert Cringely
4. The Big Bang Theory of Internet Origins
5. Defence Advanced Research Projects Agency (Darpa)
6. Arpanet (سازمان پروژه‌های تحقیقاتی پیشرفته‌ی شبکه)
7. Bob Taylor
8. Arpa'S Information Processing Techniques Office (Ipto)
9. Charles Herzfeld
10. Interactive Computing

برقرار نمایند، حتی از پس فرسنگ‌ها فاصله». باوجود تبادلات برخط گسترده با دیگر افرادی که در حال تحقیق در مورد پروژه آرپانت هستند، اختلاف نظری دراین‌راستا وجود نداشته است. بنابراین در حقیقت آرپانت هیچ ارتباطی با جنگ هسته‌ای ندارد (مگر در این قالب که مهارت‌های رایانه‌ای بهتر سبب تقویت قابلیت‌های نظامی می‌شود). به‌بیان‌ساده، آرپانت در تلاش بود تا مشکل مشترک آن روزها را از میان بردارد –استفاده از رایانه‌هایی با سیستم عامل‌های متفاوت برای برقراری ارتباط با یکدیگر. تلاش‌های مشابهی در فرانسه (لوئیز پوزین و پروژه سیکلادس[۱]) و بریتانیا (دونالد دیویس، آزمایشگاه ملی فیزیک[۲]) نیز صورت گرفت. مفهوم سوئیچینگ بسته[۳]، که آرپانت در مرحلهٔ بعدی به‌عنوان راهی برای انتقال بسته‌های داده از یک رایانه به رایانه‌ای دیگر به‌کار برد، برگرفته از این منابع است.

بعدها، در سال ۱۹۷۳، معرفی پروتکل انتقال TCP / IP توسط وینت سرف و باب کان[۴] گامی مهم در این زمینه بود. فعالیت‌های اولیه مهم دیگری در آزمایشگاه‌های زیراکس پارک[۵] توسط جان شوچ و رابرت متکلف[۶] صورت گرفت. تمامی این پیشرفت‌ها مبانی فنی اولیه اینترنت را فراهم آوردند. البته تفسیرهای کارشناسان درباره اهمیت این تحولات و پیشرفت‌های مربوط و تعیین خاستگاه اصلی اینترنت (در صورت وجود) با یکدیگر متفاوت هستند.

حقیقت: هر نقشی را که در رابطه با خاستگاه اینترنت به آرپانت نسبت دهید، پر واضح است که انگیزه اولیه از راه‌اندازی اینترنت جلوگیری از جنگ هسته‌ای نبوده بلکه نیاز به پروتکل‌های فنی برای ارتباط رایانه‌ها (و کاربران آنها) با یکدیگر دلیل اصلی آن را تشکیل می‌دهد. آرپانت در درجه اول یک فعالیت علمی رایانه‌ای و فاقد اهداف نظامی بوده است.

1. Louis Pouzin and the Cyclades Project
2. Donald Davies, National Physics Laboratory
3. Packet Switching
4. Vint Cerf and Bob Kahn
5. Xerox Parc Laboratories
6. John Schoch and Robert Metcalfe

اسطوره شانزدهم: پیام‌رسانی رمزگذاری‌شده پایان-به-پایان[1] به‌معنای محافظت از حریم خصوصی است [2]

ایلجا اسپرلینگ[3]

باور عمومی: در عصری که حریم خصوصی همواره در معرض تهدیدات عوامل دولتی و غیردولتی قرار دارد، مردم به ارتباطات رمزگذاری‌شده پایان-به-پایان[4] متکی هستند. شبکه‌های اجتماعی متداول مانند واتساپ، آی‌مسیج یا تلگرام متعهد می‌شوند از حریم شخصی ما محافظت کنند و به ما اطمینان می‌دهند که تعاملات ما «به دست افراد نامربوط» نخواهد افتاد.

اصل موضوع: رمزگذاری پایان-به-پایان به کاربران حس قوی برخورداری از امنیت و رعایت حریم خصوصی می‌دهد. با این‌حال، درحالی‌که پیام رمزگذاری‌شده پایان-به-پایان به‌خودی‌خود یک الگوی امنیتی عالی است، احتمالاً برای کاربران واضح و روشن نیست که انتقال پیام‌های رمزگذاری‌شده تنها بخشی از مسئلهٔ حریم خصوصی می‌باشد. درحالی‌که سازمان‌ها یا شرکت‌های حقوقی مانند گروه ان.اس.او[5] به‌طورفعال به‌دنبال سوءاستفاده از آسیب‌پذیری‌های کاربران هستند، حریم خصوصی با بی‌احتیاطی‌های کاربر (به‌عنوان‌مثال دستگاه‌های محافظت‌نشده؛ پشتیبان گیری بدون رمزگذاری) و طراحی نامناسب برنامه‌ها (یعنی ذخیره پیام‌های رمزگشایی شده) تضعیف می‌شود (ارجاع به اسطوره ۴۵). در اینجا به یک نمونه از تهدید غیرمستقیم می‌پردازیم: آیا تاکنون از واتساپ، تلگرام یا آی‌مسیج برای به‌اشتراک‌گذاری یک مقاله خبری اینترنتی، یک مطلب در فیس‌بوک یا به‌طورکلی لینک‌های وب‌سایت استفاده کرده‌اید؟ آیا تاکنون درباره «پیش‌نمایش» محتوایی که به اشتراک می‌گذارید فکر کرده‌اید؟ این پیش‌نمایش معمولاً بسیار ساده و متشکل از یک عنوان، یک تیزر تبلیغاتی، نشانی وب[6] و یک تصویر بندانگشتی[7] می‌باشد.

---

1. End-to-End Encrypted Messaging
2. **Source:** Justin Seitz, How To Blow Your Online Cover With URL Previews, Bellingcat (2019), https://www.bellingcat.com/resources/how-tos/2019/01/04/how-to-blow-your-online-cover-with-url-previews; Justin Wu and Daniel Zappala, When is a Tree Really a Truck? Exploring Mental Models of Encryption, Fourteenth Symposium on Usable Privacy and Security, SOUPS (2018), https://www.usenix.org/ conference/soups2018/presentation/wu.
3. Ilja Sperling
4. End-to-End Encryption (E2EE)
5. NSO Group
6. URL
7. Thumbnail

این پیش‌نمایش در واقع، یک محتوای خارجی است و برنامه پیام‌رسان شما تنها آن را از یک سرور راه دور دریافت کرده است- معمولاً بدون کسب مجوز از شما، بدون اختفای هویت شما از شخص ثالث و بدون آنکه فرصت انصراف را در اختیار شما قرار دهد.

باوجود آنکه «پیش نمایش» پیوند ممکن است کاملاً بی‌خطر به نظر برسد، یک تهدید قابل‌تأمل برای حریم خصوصی شما و همچنین حریم خصوصی دریافت‌کننده پیام رمزگذاری شده شما محسوب می‌شود.

اساسی‌ترین تهدید این است که این پیوند «پیش‌نمایش» آی پی (آدرس عمومی) شما و نماینده کاربر (یوزر ایجنت) برنامه شما را برای شخص ثالث (میزبان محتوا) به نمایش می‌گذارد. درحالی‌که کلاینت‌های ایمیل دسک‌تاپ معمولاً هنگام ارسال محتوای از راه دور به شما هشدار می‌دهند، برنامه‌های پیام‌رسان موبایل در کمال تعجب این‌گونه عمل نمی‌کنند. چنانچه شما تنها یکی از میلیون‌ها بازدید کننده یک وب‌سایت هستید، این امر ممکن است باعث آزارتان نشود. حال آنکه، یک روزنامه‌نگار محقق یا یک فعال اجتماعی که مورد هدف یک برنامه فیشینگ قرار دارد، ممکن است به این نتیجه برسد که حریم شخصی‌اش نقض شده و توسط آن برنامه پیام‌رسان به‌طرزنامحسوسی در معرض خطر قرار گرفته است.

یک بازیگر با دسترسی به سوابق یک سرور یا یک نظام اقتدارگرا که امکان نظارت بر ترافیک شبکه را دارد، از روش‌های مختلف می‌تواند پیش‌نمایش پیوند را به ابزاری برای نظارت هدفمند تبدیل سازد. جاستین سیزت[1] (۲۰۱۹) که روند کار برنامه‌های پیام‌رسان مختلفی را برای پلتفرم تحقیقاتی بلینگ کت[2] مطالعه و ثبت کرده است، نحوه انجام چنین کاری را به‌خوبی نشان داده است.

حقیقت: ویژگی پیش‌نمایش پیوند در برنامه‌های پیام‌رسان رمزگذاری‌شده پایان-به-پایان مانند واتساپ، تلگرام یا آی‌مسیج هویت شما و طرف مقابلتان را برای شخص ثالث فاش می‌کند. در مورد ابزارهای پیام‌رسان فاقد رمزگذاری پایان-به-پایان از جمله اینستاگرام یا اسلک[3] این مشکل حادتر نیز می‌باشد. عوامل مخرب می‌توانند این نقض حریم خصوصی را به ابزاری برای نظارت و ردیابی تبدیل کنند.

1. Justin Seitz
2. Bellingcat
3. Slack

اسطوره هفدهم: دارک‌وب بهشتی برای خلافکاران است[1]

سوزت لیل[2]

باور عمومی: دارک‌وب (وب تاریک) عبارت‌است از یک سرزمین رؤیایی پهناور، غیرقابل‌نفوذ، نامرئی و غیراخلاقی برای کودک‌آزاری، سازمان‌های تروریستی، سرقت داده‌ها و معاملات مواد قاچاق از طریق رمزارز یا دیگر سازوکارهای رمزنگاری شده است. دارک‌وب همچنین در مرکز تهدیدات سایبری‌اقتصادی قرار دارد، جایی که ابزارهای هک کردن برای حمله به سازمان‌های تجاری یا اشخاص مورد معامله قرار می‌گیرند. در اصل، دارک‌وب منبع هرگونه بزهکاری در فضای دیجیتالی است.

اصل موضوع: باوجود آنکه در دارک‌وب می‌توان از مزایای اختفای هویت و فقدان سانسور بهره برد، اما آن بهشت برین اینترنتی‌ای نیست که تبهکاران بتوانند در آن آزادانه فعالیت کنند (ارجاع به اسطوره ۱۴). اول این‌که، دارک‌وب مطمئناً غیرقابل نفوذ نیست و حذف محتوای مشکوک نیز غیرممکن نمی‌باشد. اگرچه نظارت بر محتوای دارک‌وب چالش‌برانگیزتر است، عامل اعتماد موردنیاز برای عملکرد هر شبکه باعث تضعیف دارک‌وب در زمینه شناسایی مجرمان و محتوای غیرقانونی می‌شود. دراین‌راستا، بخش توجه‌پذیری از دارک‌وب قابل مشاهده است و ارتباط با آن از طریق انجمن‌ها و وب‌سایت‌های ویکی نسبتاً آسان است. دارک‌وب همچنین آن کوه یخ عظیم ناشناخته‌ای که تصور می‌شود نیست –رفتارهای مشکوکی که بخش اعظم فعالیت‌های اینترنتی را تشکیل می‌دهند. درواقع، در مقایسه با ترافیک ظاهری وب، فعالیت در دارک‌وب کمینه است.

شاید مهم‌ترین سوءبرداشت در خصوص دارک‌وب به این فرض عمومی مربوط باشد که ذاتاً به‌طرزخطرناکی فسادانگیز و مخرب است. تروریسم و کودک‌آزاری بخش کوچکی از فعالیت‌های دارک‌وب را به خود اختصاص داده است. علاوه‌براین، باوجود آنکه شکی نیست که دارک‌وب محلی

1. **Source:** Mihnea Mirea, Victoria Wang and Jeyong Jung. The Not So Dark Side of the Darknet: A Qualitative Study. Security Journal, 32 (2) (2018), 102-118; Georgia Avarikioti, Roman Brunner, Aggelos Kiayias, Roger Wattenhofer and Dionysis Zindros. Structure and Content of the Visible Darknet, ArXiv(2018), 1811 .01348 (2)1-27.
2. Suzette Leal

برای فعالیت‌های غیرقانونی مانند قاچاق انسان، کلاهبرداری و معاملات موادمخدر است، نباید نقش اینترنت معمولی را در چنین فعالیت‌هایی دست‌کم گرفت. به‌دنبال دست بالا گرفتن یا حتی اغراق در قدرت و ماهیت رمزآلود دارک‌وب، ترس از اعمال فتنه‌انگیز ممکن است به اتخاذ سیاست‌های دولتی نادرست منجر شود –سیاست‌هایی که از فعالیت‌های غیرقانونی آشکار چشم‌پوشی می‌کنند.

در حقیقت، تقریباً نیمی از دارک‌وب شامل فعالیت‌های مشروع است -محتواهایی مانند منابع نرم‌افزاری و یا فعالیت‌های مربوط به وبلاگ‌ها یا وب‌سایت‌ها. برای تعداد توجه‌پذیری از کاربران دارک‌وب اختفای هویت، حفظ حریم خصوصی و محافظت شدن امری بسیار ضروری است. در کشورهایی که استفاده از اینترنت با محدودیت‌هایی همراه است و نظارت و کنترل می‌شود، اقلیت‌های به‌حاشیه رانده‌شده و منزوی اغلب از دارک‌وب برای برقراری ارتباط، به‌اشتراک‌گذاری نظرها و ابراز عقاید استفاده می‌کنند. روزنامه‌نگاران برای محافظت از منابع خود از دارک‌وب بهره‌برداری می‌کنند و سازمان‌های رسانه‌ای از صندوق‌های ایمن[1] در دارک‌وب برای تضمین ایمنی و گمنامی در برابر افشاگران استفاده می‌کنند. در حقیقت، آزادی بیان غالباً دلیل اصلی تعامل در دارک‌وب است که کاربران آن بدون نیت آسیب رساندن به دیگران در آنجا فعالیت می‌کنند.

در اصل، این میزان ناشناس ماندن لزوماً یا به‌طورخودکار سبب انحراف و سوءرفتار نمی‌شود. دارک‌وب امکان اختفای هویت را فراهم می‌آورد، و متأسفانه علاوه‌بر نیت خیر، در عمل شر نیز از این ویژگی بهره‌برداری می‌شود. با این‌حال نباید «بی‌اخلاقی» را صرفاً منسوب به دارک‌وب دانست.

حقیقت: دارک‌وب شامل کلیه فعالیت‌هایی است که امکان جستجوی آنها با استفاده از موتورهای جستجوگر استاندارد وجود ندارد. اگرچه هویت مخفی و آزادی در دارک‌وب انجام فعالیت‌های جنایتکارانه را تسهیل می‌کند، دارک‌وب تنها نمادی از رفتارهای مرموز، مشکوک و غیرقانونی نیست. در حقیقت، بخش توجه‌پذیری از فعالیت‌های دارک‌وب به محافظت از افرادی که به حریم خصوصی احتیاج دارند و همچنین فراهم آوردن امکان برقراری ارتباط برای آن دسته از افرادی که در معرض تهدید قرار دارند، اختصاص یافته است.

1. Lockboxes

فصل سوم
گنجایش و ادغام

اسطوره هجدهم: اینترنت ابزاری رهایی‌بخش برای پایان‌بخشیدن به تمام تبعیض‌ها است[1]

کاترینا موسن[2]

باور عمومی: اینترنت و فناوری‌های اطلاعات و ارتباطات ابزارهایی خنثی هستند. این ابزارهای خنثی فضاهای عمومی‌ای را ایجاد می‌کنند که امکان مشارکت آسان و مؤثر برای همه فراهم و مسائل مربوط به اقلیت‌ها را به بخشی از یک گفتمان اجتماعی بزرگ‌تر تبدیل می‌کنند؛ بدین‌ترتیب باعث تقویت همه‌گیری و غلبه بر اختلافات قدرت می‌شوند که در رسانه‌های سنتی و خطی چالش‌برانگیز هستند.

اصل موضوع: پایان جنسیت‌زدگی، نژادپرستی، تواناگرایی[4]؟ برای مدت طولانی، اینترنت اصلی‌ترین ابزار رهایی‌بخش برای غلبه بر همه نظام‌های محرومیت محسوب می‌شد (ارجاع به اسطوره ۲۸ و ۴۲). اگرچه اینترنت فضایی برای خود شکوفایی ارتباطی بسیاری از گروه‌های اجتماعی حاشیه‌ای[5] ارائه می‌دهد، این گروه‌ها حتی در دنیای دیجیتال هم همواره تحت تأثیر

1. **Source:** Nicole Shephard: What is sexual surveillance and why does it matter?, genderit.org (2017), https://www.genderit.org/feminist-talk/what-sexual-surveillance-and-why-does-it-matter; Rachel E. Dubrofsky, Shoshana Amielle Magnet, Feminist Surveillance Studies (Durham: Duke University Press, 2015).
2. Katharina Mosene
3. Ableism
4. Ableism
5. #metoo, #metwo, #schauhin, #ThingsDisabledPeopleKnow

تبعیض قرار دارند. خشونت دیجیتالی، اقدامات محروم کننده و نفرت‌پراکنی هنوز در فضای اینترنت حاکم هستند. علاوه‌براین، عضویت در بیش از یک گروه مورد هدف در فضای مجازی، خطر تبدیل شدن به قربانی خشونت دیجیتال را افزایش می‌دهد.

همان‌طور که سازمان عفو بین‌الملل در سال ۲۰۱۸ تأیید کرد: زنان سیاه‌پوست، زنان اقلیت‌های مذهبی یا قومیتی، زنان معلول یا افراد فاقد هویت جنسی که در قالب هنجارهای جنسیتی سنتی مردان و زنان نمی‌گنجند، اغلب سوءاستفاده‌هایی را تجربه می‌کنند که آنها را به روشی منحصربه‌فرد هدف قرار می‌دهند. این امر بسیار خطرناک است. چنانچه گروه‌های مورد تبعیض قرار گرفته در اجتماع خشونت بیشتری را در فضای مجازی تجربه کنند و به‌همین‌دلیل از مشارکت در این محیط انصراف دهند، بر عقلانیت فرایندهای گفتمان اجتماعی-سیاسی به واسطه فناوری تأثیر منفی خواهد گذاشت.

تبعیض در فضاهای دیجیتالی به اشکال خشونت دیجیتال محدود نمی‌شود. بلکه، اینترنت از بسیاری جهات به‌عنوان آینه جامعه عمل و انواع تبعیض‌های موجود در جامعه را منعکس می‌کند. این فناوری هرگز خنثی نیست. در دنیای واقعی، کلیشه‌های تبعیض در قوانین نمود پیدا می‌کنند و با استفاده از داده‌های آموزشی جانبدارانه به سازوکارهای یادگیری منتقل می‌شوند. هنجارمندسازی و استانداردسازی اعضای بدن و سبک زندگی انسان به‌طورضمنی در قوانین درج شده است. در دنیای اینترنت نیز مشابه این تبعیض‌ها عیناً نمود یافته‌اند. نظام تشخیص چهره بیومتریک[1] قادر به شناسایی افراد رنگین‌پوست نمی‌باشد چراکه معمولاً بر اساس داده‌های مربوط به رنگ پوست سفید عمل می‌کند. در موردی مشابه، در مجموعه داده‌های آموزشی هوش مصنوعی وسایل نقلیه خودران، اطلاعات افرادی که دارای ناتوانی‌های جسمی هستند، از جمله آنهایی که از صندلی چرخدار استفاده می‌کنند، لحاظ نشده است.

تمام فناوری‌هایی که دنیای دیجیتال را ایجاد، سازماندهی و گسترش می‌دهند خنثی یا بی‌طرف نیستند بلکه ساختارهای اجتماعی‌ای هستند که همواره با روابط قدرت، سلطه و تبعیض دنیای واقعی درآمیخته‌اند. دراین‌راستا، با رفتارهای استعماری که طی آنها مجموعه داده‌های

1. Biometric Facial Recognition

اجتماعی پیشاپیش از ایجاد یک ساختار قدرت مردسالار حمایت می‌کند، پیوند می‌خورند. فناوری دیجیتالی به هیچ وجه ما را به یک جامعه برابر تبدیل نمی‌کند. به غیر از برخی تأثیرات مثبت، مانند حمایت از جنبش‌ها با استفاده از هشتگ و امکان ارتقای سریع سطح آگاهی در سطح جهانی، اینترنت نظام‌های قدرت و محرومیت موجود را تقویت می‌کند. به‌همین‌دلیل، نوآوری دیجیتال باید همواره به‌طورگسترده و دقیق مورد انتقاد قرار گیرد.

حقیقت: اینترنت یک بستر خنثی برای توانمندسازی جهانی نیست. بلکه فناوری‌های اطلاعاتی و ارتباطی ساختارهای قدرت و سلطه اجتماعی جوامع را منعکس می‌کنند. آنها از نظام‌های تبعیض و محرومیت اشباع شده‌اند. چنانچه این اوضاع کنترل نشود، گروه‌های آسیب‌پذیر در فضای مجازی نیز به حاشیه رانده می‌شوند و تعصب و اعمال تبعیض‌آمیز نیز به جزئی از دنیای دیجیتال تبدیل شده و تشدید می‌شوند.

اسطوره نوزدهم: موتورهای جستجو نتایج عینی[1] ارائه می‌دهند (در ارائه نتایج بی‌طرف هستند)[2]

استرید میجر[3]

باور عمومی: باور اولیه برگرفته از موتور جستجوگر مطرح و پیشرو در دنیای غرب، یعنی گوگل، این است که نتایج حاصل از موتورهای جستجو عینی می‌باشند و این موتورها در این زمینه بی‌طرف عمل می‌کنند. ۲۰ سال بعد هم این باور اولیه همواره در فلسفه شرکت گوگل به چشم می‌خورد. مهم‌تر از همه، این‌که این باور نادرست در اذهان عمومی نیز جا افتاده است. بسیاری از کاربران بدون اطلاع از نحوه عملکرد موتورهای جستجوگر، معتقدند که بهترین

1. Objective Results
2. **Source:** Sergey Brin and Lawrence Page, The anatomy of a large-scale hypertextual Web search engine, Computer Networks and ISDN Systems 30: 107-117 (1998); Astrid Mager, Defining Algorithmic Ideology: Using Ideology Critique to Scrutinize Corporate Search Engines, tripleC 12 (1) :28-39 (2014).
3. Astrid Mager

وب‌سایت‌ها در بالای صفحه و در صدر فهرست قرار دارند.

اصل موضوع: در سال ۱۹۹۸، سال تأسیس شرکت گوگل، سرگئی برین و لری پیج[1] هدف اصلی موتور جستجوگر خود را این‌گونه توصیف کردند: «هدف اصلی ارائه نتایج جستجوی باکیفیت در شبکه جهانی وب می‌باشد که به‌سرعت در حال گسترش است.» (برین و پیج، ۱۹۹۸: ۱۱۵). براین‌اساس، مفاهیم «کیفیت» و «کیفیت جستجو» بیش از ۳۰ بار در مقاله تحقیقاتی آنها آمده است. این نویسندگان الگوریتم رتبه‌بندی صفحات وب[2] را اصلی‌ترین مزیت رقابتی خود مطرح می‌کنند- باتوجه‌به این‌که تعداد و کیفیت هایپرلینک‌های یک وب‌سایت، متن لنگر (اَنکرتکست[3]) و میزان همبندی (پراکسیمیتی)، کیفیت یک وب‌سایت را تعیین می‌کنند و رتبه بندی آن را نیز بر همین اساس انجام می‌دهند. آنها الگوریتم را به‌عنوان «معیار عینی»[4] مطابق با «ایده ذهنی افراد از اهمیت» توصیف می‌کنند (برین و پیج، ۱۹۹۸: ۱۰۹). نکته جالب توجه این است که درواقع چنین چیزی صورت می‌گیرد. در یک پروژه دکتری، از مردم سؤال شد چرا برای جستجوی اطلاعات برخط در زمینه سلامت از گوگل استفاده می‌کنند و پاسخ‌ها حاکی از آن بود که گوگل بهترین نتایج جستجو را ارائه می‌دهد؛ به‌عبارتی از این موتور جستجو به‌عنوان ابزاری برای اطمینان از کیفیت نتایج استفاده می‌کنند. بنابراین بدون آگاهی از نحوه عملکرد این موتور جستجوگر یا حتی اندیشیدن در این باره، باور نادرست اولیه در مورد گوگل در اذهان مردم بازتولید شده است.

حال آنکه این تنها یک اسطوره و باور نادرست است. موتورهای جستجو فناوری‌های خنثی و بی‌طرف نیستند، بلکه کاملاً با هنجارها، ارزش‌ها و ایدئولوژی‌های اجتماعی، که ایدئولوژی سرمایه‌داری در رأس آنها قرار دارد، در هم تنیده شده‌اند. طی دهه‌های گذشته، ایدئولوژی «فناورانه-بنیادگرایانه[5]» گوگل در مورد رتبه‌بندی بی‌طرفانه با ملاحظات غیرعینی مطابقت داشته و تحت‌الشعاع آن قرار گرفته است. محققان رسانه‌های جدید بلافاصله پس از ورود موفقیت‌آمیز این موتور جستجوگر در بازار، شروع به بازسازی ذهنیت مردم و به چالش کشیدن

1. Sergey Brin and Larry Page
2. PageRank Algorithm
3. Anchor Text
4. Objective Measure
5. Techno-Fundamentalist

باور عمومی در مورد «بی‌طرفی» آن کردند. در ابتدا، آنها الگوریتم رتبه‌بندی صفحات وب را با این استدلال به چالش کشیدند که با ترجیح وب‌سایت‌های بزرگ، بانفوذ و غالباً تجاری به قیمت از بین رفتن وب‌سایت‌های کوچکتر، کمال مطلوب دموکراتیک وب[1] را تهدید می‌کند (ارجاع به اسطوره ۲۸). این محققان سپس، مدل‌های تجاری موتورهای جستجو را بر اساس تبلیغات هدفمند برای کاربران و تجاری‌سازی نتایج موتورهای جستجو و مسائل مربوط به حریم خصوصی ناشی از آنها به چالش کشیدند. انتقاد عمده دیگر دراین‌راستا در زمینه «جمع‌آوری اطلاعات مشتری[2]» می‌باشد که توسط گوگل و سایت‌های دیگر مانند بینگ[3] انجام می‌شود و این امکان را برای موتورهای جستجو فراهم می‌آورد که تبلیغات را بنا به علایق فردی کاربران تنظیم کنند (ارجاع به اسطوره ۲۱ و۲۲).

باتوجه به حجم روزافزون داده‌های کاربران جمع‌آوری شده توسط این شرکت‌ها، الگوریتم جستجو و نتایج جستجوی «ارگانیک» نیز تغییر کردند. علاوه‌بر هایپرلینک‌ها، فاکتورهای دیگری در سنجش کیفیت وب‌سایت به‌کار گرفته می‌شوند، از جمله پروفایل کاربران و به‌ویژه میزان کلیک‌ها، و همچنین ساختار یک وب‌سایت، زمان‌مندبودن، و میزان کلمات کلیدی و محتوای آن. براین‌اساس، محققان رسانه‌های جدید و به‌طور فزاینده‌ای روزنامه‌نگاران، شخصی‌سازی شدید نتایج موتور جستجو، سوگیری و تبعیض موتور جستجوگر را مورد انتقاد قرار دادند. این امر نشان می‌دهد که الگوریتم‌های جستجو کاملاً با الگوهای تجاری مورد اعتماد شرکت‌هایشان در هم تنیده‌اند. ایدئولوژی سرمایه‌داری در موتورهای جستجو نهادینه شده و «از طریق منطق الگوریتمی و نظام‌های محاسباتی عمل می‌کند» (میجر[4]، ۲۰۱۴: ۳۲).

حقیقت: باید در نظر داشته باشید که موتورهای جستجو و الگوریتم‌های آن‌ها فناوری‌هایی خنثی نیستند، بلکه ارزش‌ها و ایدئولوژی‌های اجتماعی که ایدئولوژی‌های سرمایه‌داری در رأس آن‌ها قرار دارد، در آن‌ها گنجانده شده است. تنها در این صورت می‌توانیم الگوهای حاکمیتی آینده‌نگرپایبند به مقررات داخلی و بازتاب‌دهنده حقوق بشر را ارائه دهیم (خصوصاً در اروپا که

1. The Democratic Ideal of the Web
2. Consumer Profiling
3. Bing
4. Mager

حفاظت از داده‌ها یکی از حقوق اساسی محسوب می‌شود).

اسطوره بیستم: رسانه‌های اجتماعی بازتاب‌دهنده واقعیات جامعه هستند[1]

ژوزف میچال مینتال[2]

باور عمومی: رسانه‌های اجتماعی جریان‌های اجتماعی و افکار عمومی را به اندازه کافی منعکس می‌کنند. ازآنجاکه امروزه عموم مردم در رسانه‌های اجتماعی فعالیت دارند، می‌توان نگرش‌های کلی یک جامعه را باتوجه‌به مطالب به اشتراک گذاشته شده در فضای مجازی شناسایی نمود.

اصل موضوع: دست‌کم دو فرضیه کاملاً نادرست در رابطه با این باور عمومی وجود دارد. اول، این تصور که امروزه تمام مردم در رسانه‌های اجتماعی حضور دارند. باوجود افزایش چشمگیر نفوذ اینترنت و میزان به‌کارگیری رسانه‌های اجتماعی در دهه گذشته، همواره اختلاف زیادی در میزان به‌کارگیری اینترنت و رسانه‌های اجتماعی در سراسر جهان وجود دارد، چراکه در برخی از کشورها این میزان تنها ۱۰ درصد می‌باشد. حال آنکه کاربران رسانه‌های اجتماعی در کشورهایی که میزان استفاده از اینترنت در آنجا بالا می‌باشد نیز بازتاب دهنده کل جامعه نمی‌باشند.

جنسیت، درآمد، سن و اختلافاتی از این قبیل همگی مؤثر هستند (بلنک/لوتز[3] ۲۰۱۷). اقلیت‌ها، از جمله اقلیت‌های زبانی، نیز تمایل به حضور کم‌رنگ‌تری در رسانه‌های اجتماعی دارند. اما عوامل دیگری نیز وجود دارند که مانع استنباط و دریافت نگرش کلی یک جامعه تنها باتوجه‌به مطالب به‌اشتراک گذاشته شده و لایک شده در شبکه‌های اجتماعی می‌شوند (ارجاع به اسطوره ۲۴).

در رسانه‌های اجتماعی، همواره آن دسته از افرادی که تصور می‌کنیم شباهت بیشتری به خودمان دارند، ما را جلب می‌کنند (ارجاع به اسطوره ۲۱ و ۲۲). این امر سبب می‌شود که

1. **Source:** Grant Blank and Christoph Lutz, Representativeness of Social Media in Great Britain: Investigating Facebook, LinkedIn, Twitter, Pinterest, Google+, and Instagram, American Behavioral Scientist 61 (2017) 7, 741-756; Stefan Wojcik and Adam Hughes, Sizing Up Twitter Users, Pew Research Center (2019), https://www.pewInternet.org/2019/04/24/sizing-up-twitter-users.

2. Jozef Michal Mintal

3. Blank/Lutz

عمدتاً در معرض اعتقادات و نگرش‌هایی از جنس اعتقادات و نگرش‌های خودمان قرار بگیریم که این پایه و اساس کاملاً نادرستی برای شناسایی طرز تفکر و علایق اکثریت مردم می‌باشد. علاوه‌براین، به نظر می‌رسد فعالیت کاربران در پلتفرم‌های مختلف رسانه‌های اجتماعی از اصل «توزیع قانون توان تقریبی»[1] پیروی می‌کند (ارجاع به اسطوره ۴۱). این بدان معنی است که تعداد کمی از کاربران بخش بزرگی از محتوای کلی را تولید می‌کنند.

به‌عنوان‌مثال، اخیراً یک مطالعه توییتری نشان داده است که ۱۰٪ از کاربران فعال ایالات متحده، مسئولیت ۸۰٪ از محتوای رسانه‌های اجتماعی را به عهده دارند (وُچیک/هیوز ۲۰۱۹[2]). بنابراین، نظرهای تعداد کمی کاربر که فعالیت زیادی دارند به‌صورت اغراق‌آمیز و به دور از واقعیت، متداول و همه‌گیر به نظر می‌رسد.

عوامل تعیین کننده دیگری نیز وجود دارد، از قبیل پارادوکس توهم اکثریت، سوگیری الگوریتمی، ایجاد شخصیت‌های جعلی برای رسانه‌های اجتماعی و غیره. بنابراین، باید درباره آنچه در فضای مجازی می‌بینیم بسیار حساس باشیم و به خاطر داشته باشیم که با نگاه به رسانه‌های اجتماعی نمی‌توان به درک دقیق و درستی از یک جامعه دست یافت.

حقیقت: رسانه‌های اجتماعی تصویری بسیار جانبدارانه و نادرست از کل جامعه به نمایش می‌گذارند. اگرچه میزان به‌کارگیری رسانه‌های اجتماعی رو به افزایش است، پلتفرم‌های رسانه‌های اجتماعی هنوز با بازتاب دادن نظرها و سبک زندگی عموم جامعه فاصله زیادی دارند. با وجود عواملی مانند کاربران بسیار فعال رسانه‌ها، سوگیری الگوریتمی و تمایل به جذب شدن به افراد هم‌عقیده با ما و همچنین به مطالبی که در راستای تفکرات و نظرهایمان قرار دارند، قادر به تعیین نگرش کلی یک جامعه تنها از طریق مطالب پُست شده یا به اشتراک گذاشته شده در فضای برخط توسط کاربران، نخواهیم بود.

1. Approximate Power Law Distribution
2. Wojcik/Hughes

اسطوره بیست‌ویکم: تمام کاربران تجربه مشابهی از اینترنت دارند[1]

دیوید شولز[2]

باور عمومی: اینترنت برای همه یکسان است. برخی دولت‌ها ممکن است دسترسی به محتوای خارجی را در داخل کشور مسدود کنند و برخی مطالب نیز در راستای رعایت قانون کپی‌رایت محافظت یا حذف شوند. اما در کل، چنانچه در کشوری با اینترنت آزاد زندگی می‌کنیم و دسترسی به وب‌سایت‌ها برایمان نامحدود است، ما همگی شهروندان برابر[3] اینترنت هستیم و به‌طور یکسان از اینترنت بهره‌مند خواهیم بود.

اصل موضوع: بیشتر کاربران این واقعیت را پذیرفته‌اند که محتوایی که در یوتیوب تماشا می‌کنند، در گوگل جستجو می‌کنند (ارجاع به اسطوره ۱۹) یا در سایت آمازون به آنها پیشنهاد می‌شود، شخصی‌سازی شده است (ارجاع به اسطوره ۲۲). تبلیغات اینترنتی هدفمندی که معمولاً با استفاده از تبلیغات گوگل و فیس‌بوک[4] در سایت‌های اینترنتی به نمایش گذاشته می‌شوند، کمتر مورد استقبال قرار می‌گیرند و اغلب از آنها انتقاد می‌شود. اما دولت‌ها و شرکت‌ها ظرفیت‌هایی از قبیل تغییر مسیر ترافیک، استفاده از فیلترها و الگوریتم‌ها را توسعه داده‌اند که می‌توانند تأثیری عمیق اما نامحسوس بر نحوه تجربه ما در استفاده از اینترنت داشته باشند.

به‌عنوان‌نمونه، فایروال بزرگ[5]، برنامه دولت چین برای کنترل اینترنت را در نظر بگیرید. درحالی‌که به ظاهر تنها دسترسی وب‌سایت‌های خارجی به‌خصوصی مانند اکونومیست و لِموند[6] را مسدود کرده است، مطالعاتی مانند مطالعه انجام شده توسط آزمایشگاه سیتیزن[7] در دانشگاه تورنتو حاکی از ساختار پیچیده‌ای است که می‌تواند سرعت اینترنت را نیز کاهش دهد و درخواست‌های دسترسی را به وب‌سایت‌های چینی و خارجی تغییر مسیر دهد، و از آن برای

1. **Source:** Roya Ensafi, Philipp Winter, Abdullah Mueen, Jedidiah R. Crandall, Analyzing the Great Firewall of China Over Space and Time, Proceedings on Privacy Enhancing Technologies, 1 (2015), 61-76, doi: https://doi.org/10.1515/popets-2015-0005; Greg Goth, ISP Traffic Management: Will Innovation or Regulation Ensure Fairness?, IEEE Distributed Systems Online, 9 (2008) 9, https://ieeexplore.ieee.org/ abstract/document/4659261.
2. David Schulze
3. Equal Citizens
4. Google Ads and Facebook
5. Great Firewall
6. The Economist and Le Monde
7. Citizen Lab

اهداف تهاجمی در حملات دی.او.اس[۱] (حمله از کاراندازی سرویس توزیع شده[۲]) استفاده کند. سانسور معمولاً منجر به ناامیدی و اعتراض می‌شود، اما همچنین می‌تواند به‌طور ناخودآگاه رفتار را تغییر دهد. مباحث و گفتمان‌های انتقادی آشکارا تحت سانسور شدید مسکوت مانده است. اما در صورت پائین بودن سرعت بالا آمدن (لود کردن) برخی از صفحات، ممکن است بی‌آنکه آن را به سانسور نسبت دهیم، از بازدید آنها صرف‌نظر کنیم. حال آنکه چنانچه درخواست ما تغییر مسیر داده شود، یا به بخشی از یک حمله دی.او.اس تبدیل گردد، ممکن است هرگز متوجه آن تغییر مسیر نشویم.

نمونه‌ای دیگر: شرکت‌ها از سخت‌افزارها و نرم‌افزارها برای اصلاح تجربیات کاربران به دلایل تجاری یا حتی سیاسی استفاده می‌کنند. الگوریتم‌هایی که ممکن است داستان‌های آشنا را در رسانه‌های اجتماعی یا نتایج جستجوهای ما نمایش دهند نیز بخشی از وب‌سایت‌های دیگر مانند گوگل اسکالر[۳] هستند. به‌دنبال بازرسی بسته‌های عمیق[۴] که جریان داده‌ها به سرویس‌های داخلی را از جریان داده‌ها به سرویس‌های رقیب تشخیص داده و در نتیجه تنظیم سرعت دسترسی را ممکن می‌سازند، ارائه‌دهندگان خدمات اینترنتی مانند کام کست[۵] (ایالات متحده) و بل کانادا[۶] به ممانعت غیرقانونی از ترافیک اینترنتی متهم شدند (ارجاع به اسطوره ۳۹). تولیدکنندگان تلفن‌های هوشمند نحوه استفاده مشتریان از اپلیکیشن‌ها –و از این طریق اینترنت– را با دشوارتر کردن دسترسی به برخی از آنها یا حتی ناسازگار ساختن آن اپلیکیشن‌ها با سیستم عامل‌هایشان کنترل می‌کنند. شرکت‌ها همچنین با مسدودسازی پیشگیرانه محتوای غیرقانونی تولیدشده توسط کاربران یا مسدود ساختن دسترسی به اعتراضات کارمندانشان راجع به شرایط کاری، متهم به سانسور کردن می‌شوند.

درحال‌حاضر، با وجود وقفه‌هایی که‌نه‌تنها بین کشورها، بلکه بین دستگاه‌های کاربران[۷] و وب‌سایت‌ها نیز رخ می‌دهد، ما شاهد یک اینترنت ازهم‌گسیخته هستیم. اولین گام به سمت یکپارچه‌سازی آن افزایش آگاهی است.

---

1. DDoS Attacks (Distributed Denial-of-Service)

۲. این حملات با ارسال تقاضاهای بسیار بالا به سرور صورت می‌پذیرد و با استفاده بیش از حد از منابع سرور باعث اختلال در عملکرد سرور می‌شود.

3. Google Scholar
4. Deep Packet Inspection (DPI)
5. Comcast
6. Bell Canada
7. User's Devices

حقیقت: ارائه‌دهندگان خدمات اینترنتی، دولت‌ها، شرکت‌های خدمات ابری[1] سخت‌افزاری و نرم‌افزاری، وال‌ها، والد گاردن‌ها[2]، شکاف‌ها و حباب‌هایی را ایجاد کرده‌اند که می‌توانند تجربه برخط ما، نحوه تعامل ما با سایر کاربران و چگونگی افزایش اطلاعات ما در مورد جهان را عمیقاً شکل دهند. این موانع انعطاف‌پذیر، در حال تحول و اغلب مخفی هستند. آنها باعث می‌شوند بخش‌های متفاوت اینترنت را به طرق مختلف تجربه کنیم. تنها آگاهی از این موانع می‌تواند ما را در غلبه بر ازهم‌گسیختگی زندگی دیجیتال کمک کند.

اسطوره بیست‌ودوم: زندگی ما دستخوش فیلترینگ حبابی[3] شده است[4]

سباستین راندراث[5]

باور عمومی: فیلترینگ حبابی تمام زندگی ما را در برگرفته است. مشکلات سیاسی، اجتماعی و اقتصادی مانند ظهور پوپولیسم، نفرت‌پراکنی، اخبار جعلی، سرمایه‌داری روبه‌رشد و حتی افسردگی ناشی از شخصی‌سازی موتورهای جستجو و بسترهای رسانه‌های اجتماعی و همچنین هدف‌گیری‌های خُرد[6] است. فیلترینگ حبابی و اتاق‌های پژواک[7] با ایجاد حباب‌های نامرئی، کاربران را از یکدیگر جدا می‌سازد.

اصل موضوع: از نظر مفهومی، فیلترینگ حبابی وجود دارد (ارجاع به اسطوره ۲۱). در سال ۲۰۰۹، شرکت گوگل الگوریتم‌هایی را در ابزارهای جستجوی خود گنجاند که توسط داده‌های کاربر شخصی‌سازی می‌شدند. در سال ۲۰۱۱، الی پاریسر[8] ادعا کرد که این بدان معناست که نتیجه «استاندارد» (معمول) برای جستجوی گوگل وجود ندارد. این همان چیزی است که وی

1. Cloud
2. Walled Garden
3. Filter Bubbles (شخصی‌سازی نتایج جست‌وجو را فیلتر حبابی می‌نامد)
4. **Source:** Mario Haim, Andreas Graefe, Hans-Bernd Brosius, Burst of the filter bubble? Effects of personalization on the diversity of Google News, Digital Journalism(2018) 6 (3), 330-343; Martin Feuz, Matthew Fuller and Felix Stalder, Personal Web Searching in the Age of Semantic Capitalism: Diagnosing the Mechanisms of Personalisation, First Monday(2011) 16 (2), doi:10.5210/fm.v16i2.3344.
5. Sebastian Randerath
6. Micro Targeting
7. Echo Chambers
8. Eli Pariser

«فیلترینگ حبابی» می‌نامد -فضایی در داخل الگوریتم‌های جستجو و بسترهای رسانه‌های اجتماعی که از داده‌ها برای شخصی‌سازی یک «حباب» به‌خصوص برای هر کاربر استفاده می‌کند. امروزه، باتوجه‌به ظهور پلتفرم‌های بزرگی مانند فیس‌بوک، گوگل، علی‌بابا و بایدو[1]، الگوهای جمع‌آوری داده‌ها و هدف‌گیری خُرد بخشی از یک سرمایه‌داری مبتنی‌بر داده جدید است (سرنیچک[2] ۲۰۱۶). از فیلترینگ حبابی پاریسر[3] برای توضیح پدیده‌های مختلف اجتماعی، اقتصادی و دیجیتالی مانند رشد پوپولیسم، نفرت‌پراکنی، اخبار جعلی، رشد سرمایه‌داری و حتی افسردگی استفاده می‌شود. غالباً مفهوم اتاق‌های پژواک که مدت‌ها قبل از فیلترینگ حبابی وجود داشته و پیش‌تر توسط مارشال مک لوهان[4] برای توصیف فرهنگ‌های قبیله‌ای به‌کار رفته بود (مک لوهان/ نوردن ۱۹۶۹: ۷۲) برای گسترش مفهوم جداسازی (آگاهانه یا ناآگاهانه) از نظرهای جهانی مخالف در پلتفرم‌های رسانه‌های اجتماعی مورد سوءاستفاده قرار گرفته است. فیلترینگ حبابی و اتاق‌های پژواک جهت ساده‌سازی پدیده‌های پیچیده‌ای همچون تصمیم‌سازی‌ها و شکل دادن به افکار عمومی، به مفاهیم مبهمی تبدیل شده‌اند. براساس نتایج مطالعات بی‌شماری که در زمینه شکل‌گیری افکار عمومی صورت گرفته است، آثار شبکه‌ای (ارجاع به اسطوره ۴۱) و سایر ساختارهای ارتباطی که به واسطه روابط صورت گرفته در رسانه‌های اجتماعی ایجاد می‌شوند، در مقایسه با فیلترینگ‌های الگوریتمی، تأثیر عمیق‌تری در شکل‌گیری افکار عمومی در این پلتفرم‌ها دارند (هایم و همکاران ، ۲۰۱۸). به‌لحاظ‌تجربی، هیچ تحقیق یا مدرکی مبنی‌بر تأثیر فیلترینگ شخصی بر شبکه‌ها و شکل‌گیری افکار عمومی وجود ندارد (کرافت و همکاران۲۰۱۸[5]) و حتی آثار مستقیم الگوریتم‌ها بر خود «شخصی‌سازی» نیز بسیار جزئی و ناچیز است (فیوز/ بولر/استالدر[6] ۲۰۱۱). تقسیم‌بندی‌های سیاسی در مباحث و گفتمان‌های پوپولیستی رسانه‌های اجتماعی عمدتاً ناشی از پویایی خود پوپولیسم، تأثیرات شبکه‌ای یا سوشیال بات[7] است و نه به خاطر الگوریتم‌های فیلترینگ (دریر/شولز، ۲۰۱۹؛ لیسترت[8] ۲۰۱۷). فیلترینگ حبابی در الگوریتم‌های جستجو دلیل اصلی آثار شبکه‌ای، نفرت‌پراکنی، پوپولیسم یا اخبار جعلی نیست- بلکه تنها تبدیل به استعاره‌ای برای ساده‌سازی این فرایندهای پیچیده شده است.

1. Facebook, Google, Alibaba and Baidu
2. Srnicek
3. Pariser
4. Marshall McLuhan
5. Haim et al.
6. Feuz/Fuller/Stalder
7. Social Bots
8. Dreyer/Schulz, 2019; Leistert 2017

حقیقت: فیلترینگ حبابی زندگی ما را اداره نمی‌کند. فیلترینگ شخصی‌سازی شده توسط الگوریتم‌ها دلیل ایجاد افکار عمومی نیست و صرفاً آثار ناچیزی در نتایج جستجو با موتورهای جستجوگر بزرگ دارد. این مفهوم عمدتاً به‌عنوان استعاره‌ای برای کاهش پیچیدگی پویایی‌های اجتماعی، اقتصادی و فناورانه در پلتفرم‌ها و مباحث عمومی استفاده می‌شود، اما به غیر از آن از ارزش خاصی برخوردار نیست.

اسطوره بیست‌وسوم: مردم اخبار را تنها از طریق رسانه‌های اجتماعی پیگیری می‌کنند[1]

ساشا هولیگ[2]

باور عمومی: مردم و به‌ویژه کاربران جوان اینترنت، اخبار را تنها از طریق رسانه‌های اجتماعی دریافت می‌کنند. آنها رسانه‌های خبری سنتی را نادیده می‌گیرند. ما در فیلترینگ حبابی زندگی می‌کنیم، توسط اخبار دروغین فریب می‌خوریم و تصمیم‌گیری‌هایمان تحت تأثیر محتوای رسانه‌های اجتماعی دستکاری می‌شود.

اصل موضوع: این‌که بسیاری از افراد از رسانه‌های اجتماعی استفاده می‌کنند حقیقت دارد. به‌عنوان‌مثال، ۷۴ درصد از کاربران بالغ اینترنت در ایالات متحده در طول هفته وارد فیس‌بوک، توییتر یا اینستاگرام می‌شوند؛ در آلمان این رقم ۵۸ درصد است (مطالعات خبرهای دیجیتال انستیتوی رویترز ۲۰۱۹). همچنین صحت دارد که برخی افراد، به‌طوراتفاقی یا عمدی، در معرض محتوای خبری رسانه‌های اجتماعی قرار می‌گیرند. خواه به‌دلیل مشاهده مقالات ارسالی یا اطلاع از مباحث و گفتگوهای مربوط به موضوعات رایج، یا دریافت تبلیغات رسانه‌های خبری یا به‌علت دنبال کردن رسانه‌های خبری، روزنامه‌نگاران یا سیاست‌مداران.

1. **Source:** Uwe Hasebrink and Sascha Hölig, Deconstructing Audiences in Converging Media Environments, in Sergio Sparviero, Corinna Peil, Gabriele Balbi (eds.), Media Convergence and Deconvergence (Basingstoke: Palgrave Macmillan, 2017), 113-133. doi: 10.1007/978-3-319-51289-1_6; Nic Newman, Richard Fletcher, Antoins Kalogeropoulos, Rasmus Kleis Nielsen, Reuters Institute Digital News Report 2019 (University of Oxford: Reuters Institute for the Study of Journalism, 2018), www. digitalnewsreport.org.
2. Sascha Hölig

با این‌حال، به‌طورکلی، مردم عمدتاً از طریق وب‌سایت‌های مربوطه یا اپلیکیشن‌های موجود در اینترنت، (ایالات متحده: ۴۳٪ ؛ آلمان: ۴۷٪) یا از طریق تلویزیون، رادیو، روزنامه‌ها و مجلات (ایالات متحده: ۶۹٪ ؛ آلمان: ۸۳٪) که همچنان نقش مهمی را ایفا می‌کنند، رسانه‌های خبری سنتی را به‌عنوان منبع اطلاعاتی خود انتخاب می‌کنند. ما انسان‌ها، در دریافت و مصرف اخبار نیز، همانند هرچیز دیگر، موجودات پیچیده‌ای هستیم. افراد اطلاعات خود را از طریق ترکیبی جداگانه از رسانه‌های مختلف یا همان به اصطلاح «فهرست رسانه‌های» منتخب دریافت می‌کنند، که اغلب مبتنی‌بر استفاده از چند رسانه متفاوت و مختلف می‌باشد.

برای برخی از افراد، رسانه‌های اجتماعی قطعاً بخشی از فهرست خبری آنها هستند (ایالات متحده: ۴۶٪؛ آلمان: ۳۴٪)، حال آنکه برای عده معدودی از کاربران رسانه‌های اجتماعی مهم‌ترین منبع خبری هستند (ایالات متحده: ۱۸٪؛ آلمان: ۱۰٪) و تنها برای اقلیت کوچکی از مردم که هیچ‌گونه علاقه‌ای به اطلاع از اخبار مهم روز ندارند، تنها منبع خبری مورد استفاده است (ایالات متحده: ۵/۶ ٪ ؛ آلمان: ۲/۷ ٪). در این الگو، اختلاف چندانی بین گروه‌های سنی پیر و جوان وجود ندارد. اگرچه کاربران مسن‌تر درمقایسه‌با افراد جوان علاقه بیشتری به اخبار جهان دارند، کاربران جوان به هر حال خود را از طریق منابع خبری مختلف در معرض اخبار قرار می‌دهند و عمدتاً علایق مختص به سن خود را در رسانه‌های اجتماعی دنبال می‌کنند.

مطالعات مختلف نشان داده‌اند که رسانه‌های اجتماعی عمدتاً به‌منظور کسب و تبادل اطلاعات در مورد آخرین اخبار مربوط به یک چرخه محدود از دوستان و آشنایان استفاده می‌شوند، نه برای اطلاع از اخبار عمومی و نه برای جستجوی ویژه این اخبار. عموماً رسانه‌های اجتماعی مکانی مناسب برای دستیابی به اخبار نیستند و منتشرکنندگان متعدد اخبار در این فضاها نیز مورد اعتماد محسوب نمی‌شوند. بنابراین، برای اکثر رده‌های سنی مختلف، اخبار منتشر شده در رسانه‌های اجتماعی صرفاً امری ناخواسته و اجتناب‌ناپذیر است.

کاربرانی که به‌طورفعال تصمیم می‌گیرند محتوای اخبار را در رسانه‌های اجتماعی دنبال کنند، در مقایسه با تعداد کل کاربران در اقلیت هستند. کسانی که سایت‌های خبری، روزنامه‌نگاران و سیاست‌مداران را دنبال می‌کنند، معمولاً افرادی هستند که کاملاً به موضوعات خبری روز علاقه‌مند

می‌باشند و همچنین در خارج از دنیای رسانه‌های اجتماعی، از فهرست خبری گسترده و متنوع‌تر سایر رسانه‌های خبری نیز استفاده می‌کنند.

بنابراین، درست است که برخی افراد در رسانه‌های اجتماعی در معرض اخبار قرار می‌گیرند، اما معمولاً این رسانه‌ها منبع خبری دلخواه و همچنین تنها منبع خبری آنها نیستند. این فرض که حتی جوانان نیز تنها از طریق رسانه‌های اجتماعی در جریان اخبار قرار می‌گیرند یک باور نادرست است.

حقیقت: رسانه‌های اجتماعی نقش مهمی در زندگی بسیاری از افراد بازی می‌کنند اما معمولاً از رسانه‌های اجتماعی برای دستیابی به اطلاعات خبری استفاده نمی‌شود. به‌نوعی اخبار برای کاربران رسانه‌های اجتماعی امری اجتناب‌ناپذیر است. اکثریت قریب به اتفاق کاربران اینترنت در تمام گروه‌های سنی از رسانه‌های خبری سنتی به‌صورت برخط و غیربرخط استفاده می‌کنند و تنها تعداد محدودی از کاربران رسانه‌های اجتماعی منابع خبری خود را به پلتفرم‌های رسانه‌های اجتماعی محدود می‌کنند.

اسطوره بیست‌وچهارم: لایک و به‌اشتراک‌گذاری نشان از محبوبیت دارند[1]

یولریک کلینگر[2]

باور عمومی: لایک کردن، به اشتراک‌گذاری، بازدیدها، تعداد دنبال‌کننده‌ها و سایر مقیاس‌های کمی در رسانه‌های اجتماعی نشان‌دهنده میزان محبوبیت، شهرت یا موفقیت یک شخص است. افزایش تعداد لایک‌ها یا دنبال‌کنندگان همیشه به منزله بازخوردی مثبت است و می‌توانیم به آنها به‌عنوان شاخص‌های ترند[3] موجود اعتماد کنیم.

---

1. **Source:** Lauren Scissors, Moira Burke, Stephen Wengrovitz, What's in a Like?: Attitudes and behaviors around receiving Likes on Facebook. CSCW ,16 Proceedings of the 19th ACM Conference on ComputerSupported Cooperative Work & Social Computing (2016), https://dl.acm.org/citation.cfm?id=2820066; Pablo Porten-Cheé, Jörg Haßler, Pablo Jost, Christiane Eilders, Marcus Maurer, Popularity cues in online media: Theoretical and methodological perspectives. Studies in Communication and Media 7 (2018) 2, 208–230.

2. Ulrike Klinger 3. Trend Indicators 4. Trolls

اصل موضوع: این برداشت که میزان لایک‌ها، به اشتراک‌گذاری‌ها، یا تعداد دنبال‌کنندگان و دوستان یک شخص در رسانه‌های اجتماعی نشان‌دهنده محبوبیت اوست، بسیار شایع است. بازاریابی نشان می‌دهد که این عوامل میانبری برای سنجش نحوه عملکرد یک نام تجاری یا یک شخص هستند. والدین و معلمان نگران حساسیت بیش از اندازه نوجوانان به تعداد لایک‌های دریافتی در اینستاگرام هستند. در مبارزات انتخاباتی، روزنامه‌نگاران با مقایسهٔ دنبال کنندگان و واکنش‌ها، درباره احزاب سیاسی و موفقیت نامزدها در سازماندهی امور بحث می‌کنند. این تفکر که چنین شاخص‌های سنجش اجتماعی روشی آسان برای ارزیابی میزان محبوبیت است، غیرقابل اجتناب می‌باشد. متأسفانه، این نیز به دو دلیل یک سوءبرداشت است، چراکه: الف) دستکاری در آنها بسیار آسان و امکان‌پذیر است و ب) بسته به بافت و نوع پلتفرم، آنها معانی مختلفی دارند.

این باور که تعداد زیاد لایک‌ها، به اشتراک‌گذاری‌ها و دنبال‌کنندگان شاخص محبوبیت محسوب می‌شوند، مردم و سازمان‌ها را به بالا بردن اعداد و ارقام این شاخص‌های سنجش اجتماعی به‌صورت جعلی ترغیب کرده است. به کمک حساب‌های کاربری خودکار («سوشیال بات»)، ترول‌ها[۴]، فعالان و حساب‌های کاربری جعلی، جعل معیارهای محبوبیت و «محبوب» نشان دادن یک چیز یا یک شخص بسیار آسان می‌باشد (ارجاع به اسطوره ۳۰). در حقیقت، به گزارش پلتفرم‌های رسانه‌های اجتماعی، سالانه میلیاردها حساب کاربری جعلی یا خرابکار از جانب آنها حذف می‌شوند. هر کس به‌راحتی و با هزینه بسیار کمی می‌تواند تعداد لایک‌ها، به اشتراک‌گذاری‌ها یا دنبال‌کننده‌های خود را بالا برده و آنها را خریداری نماید؛ این یک روش معمول است و این معیارهای محبوبیت را به نشانه‌هایی پوشالی تبدیل می‌کند. در کمپین‌های سیاسی، این پدیده با عنوان «آستروتورفینگ یا ایجاد کمپین ساختگی[۱]» شناخته می‌شود –به نمایش گذاشتن دروغین حمایت عمومی و بسیج مردمی با فعالیت‌های ساختگی و حساب‌های کابری جعلی. لایک‌ها و به اشتراک‌گذاری‌ها در رسانه‌های اجتماعی همه‌گیر هستند.

همه ما روزانه چندین‌بار مطلبی را لایک می‌کنیم یا به اشتراک می‌گذاریم و امیدواریم که

1. Astroturfing

محتوای ارسالی ما نیز از جانب مخاطبان فرضی لایک شده و به اشتراک‌گذاشته شوند. پر واضح است که مردم بیشتر به شخصی که مطالبشان را لایک و به اشتراک‌گذاری می‌کند اهمیت می‌دهند تا تعداد دفعات آن که مهم‌ترین آنها دوستان صمیمی، همسران و افراد خانواده هستند. لایک به نشانهٔ تصدیق است، اما نه لزوماً توافق یا پذیرش. درمورد احزاب سیاسی، کاربران رسانه‌های اجتماعی تمایل دارند چند حزب را به‌طور هم‌زمان دنبال کنند، و ارسال مطلب در بیش از یک گروه سیاسی[1] امری عادی است. مردم اغلب اوقات محتوایی را که به اشتراک می‌گذارند مطالعه و بررسی نکرده‌اند (طعمه کلیک)[2] و مطالبی که عمیقاً با آن مخالف هستند را به اشتراک می‌گذارند و درباره آنها نظر می‌دهند. در حقیقت، مطالب بحث برانگیز غالباً باعث ارتقای سطح تعامل و بازدید از صفحات می‌شوند –اما تعداد زیاد لایک‌ها، به اشتراک‌گذاری‌ها و نظرهای ارسالی-لزوماً به‌معنای تأیید محبوبیت یا اعلام موافقت نیستند.

حقیقت: تعداد لایک‌ها، به اشتراک‌گذاری‌ها و دنبال‌کننده‌ها سطح پایینی از بازخورد را ارائه می‌دهند و معمولاً نشان‌دهنده دریافت، دسترسی، برقراری تعامل یا مشارکت در آن موضوع می‌باشند. این بازخورد، لزوماً و همیشه مثبت نیست. بازخورد نوعاً می‌تواند به‌معنای محبوبیت باشد، اما درعین‌حال ممکن است بیانگر این باشد که آن چیز یا شخص از محبوبیت بالایی برخوردار نیست یا بسیار بحث‌برانگیز است. دستکاری این اعداد امری بسیار آسان است و نباید بیش از حد روی آنها حساب کرد.

1. Cross-Posting
2. Clickbait!

اسطوره بیست‌وپنجم: مشکل اصلی، اخبار جعلی است[1]

توماسو ونتورینی [2]

باور عمومی: در چند سال گذشته، رسانه‌های دیجیتال به فضایی برای گردش انواع اخبار و اطلاعات نادرست تبدیل شده‌اند. عوامل اجتماعی و سیاسی خرابکار به‌طور راهبردی از کمپین‌های دروغین و شایعه‌ساز به‌عنوان اخبار موثق استفاده کرده‌اند تا با گمراه ساختن مباحث عمومی به واسطه شواهد ساختگی، نظرها و عقاید غیرواقعی یا نادرست را رواج دهند.

اصل موضوع: باتوجه‌به این‌که رسانه‌های دیجیتالی و فضاهای برخط به عرصه‌های مهمی برای گفتگوهای عمومی تبدیل شده‌اند، اطلاعات غلط قابل دسترس در دنیای مجازی به‌عنوان یک نگرانی اجتماعی جدی مطرح شده است. با این‌حال، هنوز مفهوم «اخبار جعلی» برچسب بسیار نادرستی برای این پدیده است و به جای هدایت پاسخ‌های اجتماعی، آنها را به گمراهی می‌کشد. در حال حاضر هر چیزی را می‌توان «اخبار جعلی» نامید و این اصطلاح به‌طور معمول توسط سیاست‌مداران در مورد گزارش‌هایی که مورد قبول آنها نیست، به‌کار می‌رود. بنابراین باید در مورد به‌کارگیری این مفهوم محتاط باشیم: اخبار جعلی اصطلاحی کاملاً مبهم است که برای رجوع به پدیده‌های متنوعی از جمله اخبار واقعی، طنز انتقادی، تقلید، جعل، دستکاری، طعمه کلیک، نظریه‌های توطئه و محتوایی که به‌صورت مخفیانه حمایت می‌شود مورد استفاده قرار می‌گیرد. در غیاب یک تعریف دقیق، این مفهوم توسط عوامل سیاسی و اجتماعی به‌عنوان یک سلاح کلامی برای بی‌اعتبار کردن منابع اطلاعاتی مخالف استفاده می‌شود. همچنین، درحالی‌که تصور می‌شود با ظهور رسانه‌های دیجیتال، اخبار جعلی مشکل جدی امروز به‌حساب می‌آید، مفهوم ضمنی و مبهم «اطلاعات مغرضانه تأثیرگذار بر مباحث عمومی» آن را از تبلیغات سنتی غیر قابل تشخیص می‌کند.

---

1. **Source:** Henry Jenkins, Sam Ford, and Joshua Benjamin Green, Spreadable Media (New York: New York University Press, 2013); Tommaso Venturini, From Fake to Junk News, the Data Politics of Online Virality, in Didier Bigo, Engin Isin, and Evelyn Ruppert (eds.), Data Politics: Worlds, Subjects, Rights (London: Routledge, 2019).
2. Tommaso Venturini

این مفهوم که نویدبخش «دوران پس از حقیقت[1]» می‌باشد، در بردارنده یک تمایز ساده بین حق و باطل است؛ یعنی انکار جوهره روزنامه‌نگاری که ارزش آن نه‌تنها با وقایع گزارش شده، بلکه با قابل درک ساختن موضوعات پیچیده برای افکار عمومی نامنسجم تعیین می‌شود. در آخر و از همه مهم‌تر، این برچسب حاکی از این است که «اخبار جعلی» شباهت زیادی به اخبار سنتی دارد و هدف اصلی آن القای زودباوری است. در برخی مواقع حقیقت امر این است که اطلاعات غلط زیادی در صفحات طنز انتقادی منتشر می‌شود که خودشان عدم صحت مطالبشان را پنهان نمی‌کنند یا توسط رسانه‌های خبری که تعصبات عقیدتی خود را صریحاً به نمایش می‌گذارند و غالباً چیزی غیر از یک عنوان جالب توجه برای فریب و ترغیب خوانندگان به کلیک کردن روی آگهی‌ها یا باز کردن صفحات نیستند.

درحالی‌که منظور و هدف از انتشار برخی اطلاعات نادرست دنیای مجازی فریب خوانندگان برای باور آنها (مانند کمپین‌های اطلاعات جعلی راهبردی) می‌باشد، به‌ندرت اتفاق می‌افتد که تنها هدف یا هدف اصلی آن، همین باشد. فراتر از ماهیت جعلی این اطلاعات، مسئله اصلی سرعت گسترش و تأثیر گمراه کننده آن ویژگی اصلی این نوع اطلاعات محسوب می‌شود که می‌باید «اخبار بی ارزش[2]» خطاب شوند. درست همانند مواد غذایی بی‌ارزش، اطلاعات جعلی دیجیتالی نیز به‌دلیل ماهیت اعتیادآورشان طرفدار دارند و مصرف می‌شوند؛ نه به این دلیل که آموزنده و مفید هستند. مطمئناً معطوف کردن توجه از عدم صحت این اخبار به‌سرعت پخش و گمراه کنندگی آنها، تهدیدات ناشی از این دسته از محتواها را کم‌اهمیت نخواهد کرد. بلکه دقیقاً برعکس، بیانگر این حقیقت است که این محتویات از همه خطرناک‌تر هستند، چراکه نمی‌توان آنها را به سادگی با کم‌ارزش نشان دادن از بین برد.

حقیقت: این مفهوم که «اخبار جعلی» تهدید اصلی برای مباحث و گفتمان عمومی برخط محسوب می‌شود، خود نوعی «اخبار جعلی» است. تهدید اصلی اطلاعات غلط دیجیتال، تخریب نظام‌مند گفتمان‌های عمومی می‌باشد که با سرعت بخشیدن به چرخه‌های توجه و گسترش برنامه‌های

1. Post-Truth Era
2. Junk News!

اطلاعاتی ایجاد می‌شود. اکثر مطالب خبری جعلی درواقع «اخبار بی‌ارزشی» هستند، که این به‌خودی‌خود به‌معنای کم‌خطر بودن آنها نیست، بلکه تنها بی‌اعتبار ساختن آنها دشوارتر می‌شود.

اسطوره بیست‌وششم: ما همگی اکنون خبرنگار و تولیدکننده خبر هستیم[1]

مایکل دابز[2]

باور عمومی: اینترنت به شهروندان آزادی عمل در ایجاد، همکاری در ایجاد و انتشار خبر می‌دهد و درعین‌حال خبرهای تولیدشده را از سازوکارهای نظارت و دروازه‌بانی معمول در رسانه‌های سنتی رها می‌سازد؛ در نهایت این مهم باعث دموکراتیک شدن حرفه و امر خبرنگاری می‌شود.

اصل موضوع: در اواخر دهه ۹۰ میلادی، برخی سایت‌های خبری مبتنی‌بر شهروند-خبرنگار مانند ایندی مدیا[3] ظهور پیدا کردند که به مردم فرصت تبدیل شدن به «رسانه» از طریق تولید و انتشار اخبار در قالب «رونامه نگاری شهروندی» را می‌داد.

در این مسیر وبلاگ نویسی و سایت‌های اجتماعی مانند فیس‌بوک، یوتیوب، توییتر نیز به گسترش این مفهوم کمک شایانی داشتند و در نهایت به ظهور ساختارهایی اختصاصی مانند «من-گزارشگر»[4] خبرگزاری سی.ان.ان[5] منجر شد. بسیاری این پلتفرم‌های جدید را به‌عنوان قدمی در جهت دموکراتیک کردن روزنامه‌نگاری[6] ارج می‌نهادند (ارجاع به اسطوره ۲۸). چنین دیدگاهی، ادعاهای وسیع‌تری را طنین انداز می‌کرد مبنی‌بر این‌که رسانه‌های دیجیتال از «یک نیاز دموکراتیک برای مشارکت تعداد بیشتری از مردم در تولید و به گردش درآوردن رسانه‌ها» حمایت می‌کند (جنکینز[7]، ۲۰۰۶).

با این‌حال باید توجه داشت این ادعا که محتوای تولیدشده توسط عموم مردم فعالیتی

---

1. **Source:** Michael S. Daubs, The Social News Network: The Appropriation of Community Labour in CNN's iReport, The Political Economy of Communication, 3.2 (2015), 55-73; Sara Platon and Mark Deuze, Indymedia Journalism: A Radical Way of Making, Selecting and Sharing News?, Journalism 4.3 (2003), 336–55.
2. Michael S. Daubs
3. Inndymedia
4. IReporter
5. CNN
6. Democratizing Journalism
7. Jenkins

مبتنی‌بر دموکراسی است، درواقع تعامل و روابط پیچیده بین کاربران و نهادهای روزنامه‌نگاری سنتی را نادیده می‌گیرد. تولید و نشر محتوا و اطلاعات ضرورتاً دسترسی به مخاطب را تضمین نمی‌کند. همچنین، برخی از شهروند-خبرنگاران با اصول ابتدایی خبرنگاری و تولید محتوای خبری مانند ویرایش، راستی‌آزمایی خبر، انگیزه‌های خبری و... آشنایی نداشتند.

به‌عنوان‌مثال، تولیدات اطلاعاتی و خبری برخی از شهروند-خبرنگاران بیشتر شبیه به اظهار نظر شخصی و تفسیر فردی بود تا واکاوی اطلاعات و تحلیل داده‌های سیاسی. درحالی‌که شارون داکتر[1](۲۰۱۰) تأکید داشت که نظرهای مخالف علیه دسته بندی وبلاگ‌نویسان به‌عنوان صنف روزنامه‌نگار، به‌ندرت به‌معنای این است که «وبلاگ نویسان در شکل‌گیری حوزه عمومی[2]، آن‌طور که روزنامه‌نگاران ایفاگر نقش هستند، نقش ندارند»؛ این عوامل باعث ایجاد مباحثی در مورد این موضوع شد که آیا شهروند-خبرنگاران نیز باید همانند روزنامه‌نگاران سنتی مورد حمایت‌های قانونی مشابه قرار بگیرند یا خیر؛ قوانینی که طبق آن خبرنگاران و اصحاب رسانه‌های سنتی را از افشا نمودن منابع اطلاعاتی و همچنین گزارش‌های منتشر نشده خود مصون می‌نمود.

به طورخلاصه، دلایل متعددی برای زیر سؤال بردن باور عمومی راجع به نقش مؤثر اینترنت در دموکراتیک ساختن رسانه وجود دارد. علاوه‌براین، جان تی. کالدول (۲۰۰۴) خاطرنشان می‌کند که تلویزیون «در پذیرش بعضی از تغییرات اساسی اقتصادی، فناورانه و فرهنگی» به‌صورت منعطف عمل کرده است. به‌عنوان‌مثال، رسانه‌های خبری سنتی از جمله تلویزیون، به‌جای احساس تهدید توسط محتوای تولیدشده توسط کاربران، آن را به‌طور فزاینده‌ای در گزارش‌های خود گنجانده‌اند. علاوه‌براین، برخی از شهروند-خبرنگاران، که مایل‌اند در آینده روزنامه‌نگاری حرفه‌ای باشند، به امید بهبود مهارت‌های خود و دریافت پروژه‌های احتمالی شغلی آینده، زحمات زیادی را در آماده‌سازی محتوای خبری محتمل می‌شوند. خبرگزاری‌ها و سایر مؤسسات خبری به‌صورت گسترده‌ای از خدمات بدون بار مالی شهروند-خبرنگاران بهره می‌برند، افرادی که بعضاً از آنها به‌عنوان «نیروی کار امید»[3](کیون و کارگن[4]، ۲۰۱۳) یا «نیروی کار آرمانی»[5] (دافی[6]، ۲۰۱۷) یاد می‌شود که به خبرگزاری‌ها سنتی اجازه پس‌انداز نمودن

1. Sharon Docter
2. Public Sphere
3. Hope Labor
4. Kuehn and Corrigan
5. Aspirational labor
6. Duffy

سرمایه را می‌دهند، و درعین‌حال به‌عنوان مرجعی بلامنازع برای محتوای تولیدشده توسط کاربر عمل می‌کنند و در نتیجه «قدرت اجتماعی خود را برای شکل دادن به مسائل» حفظ کنند (آندرهویویچ[1]، ۲۰۰۴).

حقیقت: ازآنجاکه خبرگزاری‌های سنتی همواره اختیار و امتیاز «حق انتخاب» و متناسب‌سازی محتوای تولیدشده توسط کاربران را برای خود محفوظ می‌دارند، محتوای تولیدشده و به اشتراک گذاشته شده در اینترنت در قالب روزنامه‌نگاری شهروندی، اغلب به‌جای دموکراتیک شدن روزنامه‌نگاری، بیشتر به اقتدار، قدرت و محوریت خبرگزاری‌ها و روزنامه‌نگاران آنها منجر شده است.

اسطوره بیست‌وهفتم: نسل هزاره همگی مسلط به اینترنت و با زندگی دیجیتال عجین هستند[2]

کلادیا لمپرت[3]

باور عمومی: کودکان در محیط‌های رسانه-محور رشد می‌کنند، اینترنت را از نزدیک می‌شناسند، رسانه‌های دیجیتالی را به راحتی به‌کار می‌گیرند و بدین ترتیب سواد رسانه‌ای را به‌طور خودکار فرا می‌گیرند. در مقابل آنها، بزرگسالان قرار دارند که غالباً به‌عنوان «مهاجران دیجیتال» شناخته می‌شوند که هیچ فرصتی برای استفاده از اینترنت و رسانه‌های برخط به‌خوبی نسل جوان فعلی یا آینده ندارند.

اصل موضوع: کودکان، به‌طور فزاینده‌ای در معرض رسانه‌های دیجیتال قرار دارند. حتی نوزادان و کودکان نوپا والدین و یا مراقبان خود را می‌بینند که از تلفن‌های هوشمند استفاده

1. Andrejevic
2.**Source:** Eszter Hargittai und Yuli Patrick Hsieh, Digital Inequality, in William H. Dutton (ed.), The Oxford Handbook of Internet Studies (Oxford: OUP, 2013), DOI: 10.1093/ oxfordhb/9780199589074.013.0007; Marc Prensky, Digital Natives, Digital Immigrants, On the Horizon (2001), www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20 Immigrants%20-%20Part1.pdf.
3. Claudia Lampert

می‌کنند یا در حال تعامل با صفحات نمایش الکترونیکی هستند. دستگاه‌های دارای صفحهٔ نمایش لمسی یا آنهایی که از طریق صدا کنترل می‌شوند (مانند دستیاران دیجیتال از جمله Siri یا بلندگوهای هوشمند مانند Alexa) به مهارت نوشتن یا کار با صفحه کلید احتیاج ندارند، به‌طوری‌که حتی کودکان بسیار خردسال نیز به‌راحتی می‌توانند از برنامه‌های دیجیتال استفاده کنند. داده‌های فعلی نشان می‌دهد که گسترش دستگاه‌های تلفن همراه دیجیتال در سال‌های اخیر افزایش یافته است؛ و رده‌های سنی که در آن کودکان اولین تلفن‌های هوشمند خود را دریافت می‌کنند روبه‌کاهش است. در بین اکثر نوجوانان در کشورهای غربی، امروزه داشتن تلفن هوشمند متداول است. بااین‌حال، استفاده از امکانات دنیای دیجیتال اشکال مختلف پیدا کرده است به‌طوری‌که بیشتر معطوف به ارتباط و سرگرمی شده‌اند تا بهره‌گیری از اطلاعات. اما این استفاده طبیعی و (بعضاً شدیداً) فشرده از انواع مختلف ابزار دیجیتالی است که باعث ایجاد این تصور در اذهان عمومی شده که کودکان به فناوری‌های دیجیتال تسلط داشته و با مهارت بیشتری در مقایسه با بزرگسالان امکان استفاده از این ابزار را دارند.

با این‌حال، ما اغلب این مهم را که مدیریت و استفاده رسانه‌ها به‌صورت مستقل و فرد-محور به دانسته‌ها و اطلاعاتی بیش از کاربری فنی نیاز دارد را نادیده می‌گیریم. ازیک‌سو، درک خاصی از رسانه‌ها، ساختارها و کارکردهای مربوط به رسانه‌ها برای ارزیابی و طبقه‌بندی رسانه‌های مختلف مورد نیاز است (به‌عنوان‌مثال چه چیزی برنامه عمومی[1] را از برنامه‌های تجاری متمایز می‌کند؟ الگوریتم‌ها چیستند و آنها چگونه استفاده از اطلاعات و محتوای اینترنتی را تحت تأثیر قرار می‌دهند؟ تبلیغات برخط چگونه کار می‌کند؟ یک تأثیرگذار[2] کیست؟). ازسویی‌دیگر، خودمختاری به‌معنای استفاده از رسانه‌ها برای بیان تأملات و نظرهای شخصی است، بدون نقض حریم و حقوق یا عزت دیگران. و در نهایت این‌که، مسئله مهم از یک سو در نظر گرفتن احتمالات و خطرهای روند دیجیتالی شدن زندگی در دو سطح فردی و اجتماعی و ازسویی‌دیگر توجه به ظرفیت خلاقانه و قدرت مشارکتی رسانه‌های مختلف است.

مطالعات کنونی نشان می‌دهد که نوجوانان -بسته به عوامل متفاوت مانند سن، بافت اجتماعی

1. Public
2. Influencer

و سوابق تحصیلی- از فرصت‌های دیجیتالی به روش‌های بسیار متفاوتی استفاده می‌کنند و بنابراین این مهارت‌ها بسیار متفاوت پرورانده می‌شوند. هنوز به نظر می‌رسد افرادی که دارای موقعیت ممتاز اجتماعی-اقتصادی و دارای تحصیلات عالی هستند از فرصت‌های دیجیتالی در اشکال متنوعی استفاده می‌کنند و بنابراین از آنها بهره بیشتری می‌گیرند. این تفاوت‌ها همچنین به این واقعیت که نابرابری‌های دیجیتال از دسترسی به امکانات دیجیتال («شکاف دیجیتال») به استفاده از آنها («شکاف دیجیتال دوم») منتقل شده، اشاره دارند. برای مؤسسات آموزشی این بدان معناست که نه‌تنها زیرساخت‌های فنی باید مورد توجه و بهینه‌سازی قرار گیرند بلکه به‌ویژه استفاده و تعامل با برنامه‌های برخط دیجیتالی نیز نیازمند بازخوانی جدی هستند.

حقیقت: این واقعیت که کودکان در محیط‌های رسانه-محور در حال رشد هستند به این معنی نیست که همه (به‌طور یکسان) به استفاده از رسانهٔ دیجیتال مسلط می‌باشند. به‌بیان‌دیگر، ازیک‌سو نیازهای فردی دچار تحول و تنوع‌گرایی شده است؛ ازسویی‌دیگر، استفاده خودمختار و مستقل از رسانه و دنیای دیجیتال نیازمند اطلاعات و درکی بیش از مهارت‌های فنی است.

اسطوره بیست‌وهشتم: اینترنت مانند آنچه در بهار عربی اتفاق افتاد، باعث توسعه دموکراسی می‌شود [1]

لئید زقلامی[2]

باور عمومی: رسانه‌های اجتماعی باعث تقویت و توانمند شدن بخش ستمدیده و حاشیه‌نشین جامعه می‌شوند. اینترنت و رسانه‌های اجتماعی به‌عنوان ابزارهای قدرت نرم، با اعمال فشار بر رژیم‌های سیاسی آنها را از اقتدارگرایی به جوامع دموکراتیک و کثرت‌گرا

1. **Source:** Kamal Eldin Osman Salih, The Roots and Causes of the 2011 Arab Uprisings, 35 Arab Studies Quarterly 35 (2013) 2, http://www.pinxit.com/page101/page115/downloads-23/files/Arab_Spring_Causes. pdf; George Lawson, Revolution, Non-Violence, and the Arab Uprisings, Mobilization: An International Quarterly (2015) 4, 453–470, http://eprints.lse.ac.uk/63156/1/Lawson_Revolution%2C%20non-violence.pdf.
2. Laeed Zaghlami

هدایت می‌کنند. جنبش‌های اجتماعی و خیزش‌هایی مانند بهار عربی فقط از طریق اینترنت امکان‌پذیر است؛ و بنابراین در هر جایی که دسترسی به اینترنت به حد خاصی برسد این مهم رخ می‌دهد.

اصل موضوع: بله، اینترنت و رسانه‌های اجتماعی به‌طور خاص در گسترش آگاهی و سازماندهی اعتراضات در همه کشورهایی که به اصطلاح «انقلاب‌های بهار عربی» در آن‌ها رخ داده نقش مهمی داشته است. باوجوداین، باتوجه‌به تعداد زیادی از مطالعات و تحقیقات در این حوزه، واضح است که نه لیبرال‌های جوان و مسلط بر اینترنت عامل محرک این اعتراضات بوده‌اند و نه تغییر رژیم این کشورها منجر به دموکراتیزه شدن آنها شده است. بهار عربی به‌خودی‌خود یک مفهوم نسبتاً بحث‌برانگیز و مبهم به نظر می‌رسد، زیرا اکنون کشورهایی مانند مصر، لیبی، سودان و تونس را پس از پشت سرگذاشتن هیجانات سال‌های اول انقلاب، به سمت باتلاق بی‌نظمی و وحشت هدایت کرده است. علاوه‌براین، این جنبش‌ها از نظر هنجارها، ارزش‌ها و عملکردهای دموکراتیک در همه ملل منطقه به دستاوردهای توجه‌پذیری نائل نشده‌اند.

الجزایر به‌عنوان‌مثال یکی از این کشورهایی بود که می‌توانست با استفاده از فرصت‌های دموکراتیک موجود به سمت عدالت اجتماعی حقیقی و آزادی واقعی مطبوعات حرکت کند. اما شهروندان این کشور هنوز در تلاشند تا آزادانه نظرهای خود را ابراز کنند و آرمان‌های دموکراتیک را به‌کار گیرند. بنابراین هیچ تغییر اساسی در الجزایر رخ نداده است که بتوان از آن به‌عنوان نتیجه مستقیم استفاده از اینترنت و رسانه‌های اجتماعی یاد نمود. این مورد اخیر، یعنی رسانه‌های اجتماعی را می‌توان تنها به‌عنوان ابزار صرف اطلاعات، تعامل و ارتباطات در این کارزار نام برد. ضمن آنکه، دعوت به کثرت‌گرایی سیاسی، عدالت اجتماعی و آزادی مطبوعات عمیقاً ریشه در جامعه دارد؛ به‌بیان‌دیگر، این مباحث پیش‌تر در دهه ۱۹۸۰ میلادی و درواقع سال‌ها پیش از ظهور اینترنت نیز ابراز شده بودند. بنابراین، ابزارهای ارتباطی برخط عوامل تبلیغ و انتشار اخبار و دیدگاه‌ها هستند. الجزایر ارزش‌های فرهنگی و اجتماعی مشترکی با کشورهایی دارد که جنبش‌های قومی بهار عربی را تجربه کرده‌اند، اما در این کشور هیچ‌گونه «انقلاب

اینترنتی» رخ نداده است. مانند سایر کشورها، الجزایر از الگوی سیاسی خاص خود و همچنین یک ذهنیت متفاوت و منحصربه‌فرد بهره می‌برد.

تعمیم دادن[1] تقریباً در همه موارد گمراه کننده است؛ براین‌اساس می‌توان ادعا نمود اینترنت و رسانه‌های اجتماعی در دستیابی به اهداف بهار عربی نقش پایداری نداشته‌اند. در حقیقت، شخصی‌سازی و تمرکز بیش از حد قدرت در دست یک فرد، ضعف مجلس، آسیب‌پذیری احزاب سیاسی و نقش دولت را می‌توان از موانع اصلی موجود در تغییر سیاسی مثبت در الجزایر دانست. علاوه‌براین، مقامات سیاسی حرص و طمع فراوان به قدرت و مواضع قدرت دارند. در این راه، آنها خود از اینترنت و رسانه‌های اجتماعی برای مقابله با انقلاب استفاده می‌کنند؛ «مگس‌های الکترونیکی»[2]، تعریف سخیفی در جهت تحقیر انقلابیون و مبارزان احتمالی است که از سوی این صاحبان قدرت بیان می‌شود. سوءاستفاده‌های مکرر، استفاده ابزاری، اخبار جعلی و تحریف حقیقت اکنون کاربران را درمقایسه‌با کارایی و قابلیت اطمینان اینترنت و رسانه‌های اجتماعی به‌طورکلی دچار تردید ساخته است. به نظر می‌رسد که یک «دست پنهان و نامرئی» همچنان آشفتگی و ابهام می‌پراکند.

حقیقت: جنبش بهار عربی، البته اگر ورای روایت غرب، انقلابی با این نام وجود داشته باشد، نه منجر به دموکرات‌شدن این جوامع یا شکل‌گیری دولت-ملت جدید شد، و نه باید منشأ این تحولات را در اینترنت یا رسانه‌های اجتماعی جُست. دسترسی به اینترنت و رسانه‌های اجتماعی به‌عنوان پلتفرم‌های آگاهی‌ساز و سازمان‌دهنده، از عوامل تقویت‌کننده ناآرامی‌های اجتماعی بودند که اساساً ریشه در تمایلات عمیق و اساسی مردم و جامعه برای تغییر (سیاسی) داشت.

1.Generalization

2. Electronic Flies

اسطوره بیست‌ونهم: اینترنت ماهیت انتخابات را از بین برده است[1]

فرانچسکا اومر و استفانو پدرازی[2]

باور عمومی: اینترنت به یک منبع اطلاعاتی مهم برای رأی‌دهندگان تبدیل شده است تا از طریق آن بتوانند نه‌تنها نظرهای خود را شکل دهند بلکه با احزاب و نامزدها نیز در انتخابات در تعامل باشند. بااین‌حال، ربات‌ها و ترول‌ها[3] یا مزاحمان اینترنتی در مظان اتهام قرار دارند که به‌طوروسیعی فرایندهای ارتباطی مربوط به جریان رأی‌گیری را دستکاری می‌کنند؛ و بنابراین محبوبیت و میزان رأی واقعی برخی از سیاست‌مداران را تغییر می‌دهند. براین‌اساس، می‌توان ادعا نمود که اینترنت «تصمیم گیری آگاهانه» را برای مردم به خطر می‌اندازد. به‌بیان‌دیگر، اینترنت انتخابات دموکراتیک را از بین می‌برد و فرصت برگزاری یک رفراندوم را می‌رباید.

اصل موضوع: از زمان شروع کارزارهای انتخاباتی ایالات متحده و رأی‌گیری خروج بریتانیا از اتحادیه اروپا[4] در سال ۲۰۱۶، گمانه‌زنی‌هایی در مورد تأثیر واقعی ربات‌ها و ترول‌ها در گفتمان برخط شکل گرفته است(ارجاع به اسطوره ۳۰). فرض بر این است که این حساب‌های (نیمه‌خودکار) در لوای هویت انسانی مشغول تولید و توزیع محتوا یا لایک کردن پروفایل‌ها در شبکه‌های اجتماعی هستند، در واقع، هدفی غیر از انحراف افکار عمومی نداشته‌اند؛ اهدافی مانند به پیروزی رسانیدن ترامپ در کارزار رقابت ریاست جمهوری، یا تشویق انگلیس به خروج از اتحادیه اروپا.

این باور عمومی بر این فرض استوار است که اولاً، ربات‌ها و ترول‌ها به‌صورت کمی با گسترش دامنه اخبار دروغین، افزایش محبوبیت و اهمیت برخی از کاندیداهای سیاسی، جهت‌دهی به مضامین و مواضع مورد بحث هنگام انتخابات و اختفای افراد و سازمان‌ها در پس انبوه فعالیت‌های ارتباطی یا به‌دلیل فیلتر الگوریتمی مهندسی شده، گفتمان سیاسی را تعیین می‌کنند. ثانیاً،

1. Source: Emilio Ferrara, Onur Varol, Clayton Davis, Filippo Menczer, Alessandro Flammini, The Rise of Social Bots, 59 Communications of the ACM (2016) 7, 96-104, https://dl.acm.org/citation.cfm?id=2818717; Samuel C. Woolley, Philip N. Howard (eds.), Computational Propaganda (Oxford: OUP, 2018).
2. Franziska Oehmer، Stefano Pedrazzi
3. Trolls
4. Brexit

این‌طور به نظر می‌رسد که شهروندان به‌طورعمده و سهل‌انگارانه (به‌صورت غیرانتقادی) تصمیم‌گیری‌های انتخاباتی خود را تنها به اطلاعات موجود در اینترنت محدود نموده‌اند.

این‌که تا چه حد ربات‌ها و ترول‌ها حقیقتاً گفتمان قبل از انتخابات و میزان آراء را تعیین می‌کنند را نمی‌توان با اطمینان کامل تعیین کرد. بسته به موضوع رأی، انتخابات و محتواهای ملی، تحقیقات اخیر داده‌ها و پاسخ‌های متفاوتی راجع به حضور و فعالیت ربات‌ها و ترول‌ها در گفتمان برخط ارائه کرده‌اند: از گستردگی نسبی قابل تأمل و درعین‌حال غالب تا حضوری ناچیز و کم اهمیت. نوسانات موجود در داده‌های پژوهش‌ها نیز به‌دلیل دشواری شناسایی چنین حساب‌هایی (در حال حاضر) است. باوجود فرضیه حضور قوی‌تر ربات‌ها و ترول‌ها در مباحث سیاسی برخط، قطعیت تحمیل نتیجه توسط آنها در صندوق‌های رأی امری دور از ذهن می‌باشد. فقط درصد کمی از رأی‌دهندگان منحصراً قبل از انتخابات یا رأی دادن، اطلاعات خود را از طریق اینترنت به‌روزرسانی می‌کنند (ارجاع به اسطوره ۲۳). علاوه‌براین، کسب اطلاعات از رسانه‌ها یا فعالان ناشناس در اینترنت به هیچ وجه نقش تعیین کننده در تصمیم‌گیری مردم ندارد. بلکه در عوض، تعاملات نظری شخصی با محیط اجتماعی یا با رهبران فکری شناخته شده در جامعه ما به‌علاوه ترجیحات سیاسی موجود پیشین را می‌توان به‌عنوان عامل تعیین‌کننده رأی ما دانست.

حقیقت: اینترنت انتخابات و آرای دموکراتیک را از بین نمی‌برد. درحال‌حاضر، ربات‌ها و ترول‌های اجتماعی نقش مؤثر و غالب در شکل‌گیری عقاید و تصمیم‌گیری ندارند. ترجیحات حزبی و شخصی مورد نظر و تعاملات فردی با محیط اجتماعی همچنان از اهمیت اساسی برخوردار است. باوجوداین، این مهم را که ممکن است تأثیر ربات‌ها و ترول‌ها در آینده افزایش یابد را نمی‌توان دور از ذهن دانست.

اسطوره سی‌ام: کارزارهای حقوق دیجیتال توسط ربات‌ها اداره و هدایت می‌شوند، نه فعالیت‌های واقعی [1]

الک تارکوفسکی [2]

باور عمومی: مانند بسیاری از کارزارهای حقوق دیجیتال، اعتراضات ۲۰۱۸-۲۰۱۹ علیه دستورالعمل کپی‌رایت در اتحادیه اروپا [3] بیانگر نگرانی گسترده شهروندان از حقوق دیجیتال نبود. کارزار اعتراضی که می‌توان از آن به‌عنوان بزرگترین پویش اعتراضی در سال‌های اخیر یاد نمود، درواقع نمونه‌ای اساسی از فعالیت‌های مخرب در حوزه اطلاعات بود. به‌بیان‌دیگر، این پویش اعتراضی را می‌توان یک «قیام مردمی جعلی» توسط گروه کوچکی از مردم یاد نمود که با استفاده از ربات‌ها، تعداد اندک خود را به خیل عظیمی از مردم تبدیل کرده بودند.

اصل موضوع: این پیشنهاد که ربات‌ها و نه انسان‌ها مسئول بسیاری از کارزارهای مربوط به حقوق دیجیتالی و به‌ویژه اعتراضات گسترده در برابر دستورالعمل کپی‌رایت اتحادیه اروپا هستند، از یک گروه از فعالان حامی حقوق هنرمندان و نیز لابی‌گرهای مرتبط با آن نشئت گرفته است. این اتهامات بدون ارائه هیچ‌گونه مدرکی مبنی‌بر فعالیت واقعی ربات‌ها در مقیاس گسترده صورت گرفته است.

نویسنده در گزارشی در نشریه فرانکفورتر آلگماینه زایتونگ [4] درباره فعالیت در «زمان ربات‌ها» اظهار داشت که شش میلیون تماس و ایمیل ارسال شده به اعضای پارلمان اروپا عمدتاً به‌صورت خودکار و توسط ربات‌ها انجام شده است. این در حالی است که بسیاری از کسانی که معتقدند فعالیت‌های مرتبط با کارزارهای حقوق دیجیتال توسط ربات‌ها هدایت و پایه‌ریزی می‌شوند، مفهوم فعالیت «خودکار» یا همان «اتوماسیون» را اشتباه متوجه شده‌اند. فعالیت«خودکار» یا همان «اتوماسیون» درواقع اعتراضات گسترده برخط را با استفاده از ربات‌ها یا همان حساب‌های کاربری جعلی امکان‌پذیر می‌کند.

---

1. **Source:** Corporate Europe Observatory (2018), "Copyright Directive: how competing big business lobbies drowned out critical voices", https://corporateeurope.org/en/2018/12/copyright-directive-howcompeting-big-business-lobbies-drowned-out-critical-voices; European Digital Rights (2018), Save Your Internet, https://saveyourInternet.eu.
2. Alek Tarkowski
3. EU Copyright Directive
4. Frankfurter Allgemeine Zeitung

این ادعا که سیستم‌های کارزارهای برخط مورد استفاده برای کمپین .SaveYourInternet eu (و سایر کارزارهای انجام شده طی فرایند تدوین دستورالعمل کپی‌رایت در اتحادیه اروپا) از عناصر خودکار (برای تولید و نشر اطلاعات) بهره می‌برند، صحت دارد. به‌عنوان‌مثال، یک کاربر وب‌سایت تبلیغات می‌تواند به‌راحتی از طریق تلفن - به‌صورت رایگان- با دفترهای چندین سیاست‌مدار ارتباط برقرار کند یا با استفاده از پیام‌ها و گرافیک‌های ایجاد شده به‌صورت خودکار، از طریق رسانه‌های اجتماعی، تبلیغات ارسال نماید. چنین ساختاری از اتوماسیون اجازه می‌دهد تا ابعاد و آثار استفاده از شبکه نمایان شود و امکان رشد توجه‌پذیر کارزار انتخاباتی را فراهم می‌نماید. با این‌حال، این ساختار خودکار همچنان به یک کاربر انسانی برای برقراری تماس، ارسال ایمیل یا به‌اشتراک‌گذاری اطلاعات در رسانه‌های اجتماعی نیاز دارد. منتقدان این کارزار هیچ مدرکی دالّ بر وجود حساب‌های جعلی و ربات‌ها در بین میلیون‌ها شهروند حامی این کارزارها ارائه نکرده‌اند.

این اتهامات در میان برخی از سیاست‌مداران بروکسل وجه اشتراکی ایجاد نمود. زیرا اعضای پارلمان از این مسئله که صندوق پستی آنها با پیام‌های تکراری و تهی از مطالب واقعی انباشته شده بود، شکایت داشتند. به‌دلیل فقدان ابزار مرتبط برای تجزیه و تحلیل ارتباطات از اجزای تشکیل‌دهنده آنها و با عنایت به حجم گسترده نامه‌های ارسالی، برخی از آنها ظاهراً به‌عنوان اسپم[1] شناسایی شده بودند. به‌همین‌دلیل روابط عمومی بدکاره گسترش یافت. براین‌اساس، ادراک ایجاد شده میان سیاست‌مداران و حامیان و رأی‌دهندگان آنها در سیستمی که اثری از تعامل وجود ندارد، چیزی جز یأس و انزوا به همراه ندارد. حال آن که سیاست‌مداران مفهومی ساده را نادیده می‌گرفتند: تأثیرات شبکه (ارجاع به اسطوره ۴۱) که توسط ابزارهای ارتباطی دیجیتال امکان‌پذیر می‌شود و امکان بسیج مردم در سطح میلیون‌ها شهروند را با هزینه‌ای نسبتاً کم امکان‌پذیر می‌کند. شهروندان اروپایی به آزادی‌های برخط بسیار اهمیت می‌دهند و در نتیجه به قوانینی که به نظر آنها آزادی را تهدید می‌نماید، به‌راحتی اعتراض و واکنش نشان می‌دهند.

علاوه‌براین، لابی‌گرهای حامی این کارزارها از درک این مهم بازماندند که از همان ابزارهای

1. Spam

تبلیغاتی برای پیشبرد پویش‌های انتخاباتی آنها نیز استفاده شده بود. همان‌طور که مرکز تحقیقات شرکت‌های اروپایی خاطرنشان می‌کند، در این کارزار چالش اصلی درواقع ربوده شدن گوی سبقت در حوزه مباحث عمومی توسط لابی‌های تجاری به نمایندگی از فناوری‌های بزرگ، ناشران و دیگر جوامع بزرگ بوده است.

حقیقت: درحالی‌که ابزارهای تبلیغاتی در جهت بهره‌مندی از گستره تأثیرات شبکه به‌کار گرفته شده‌اند، کمپین‌های مربوط به حقوق دیجیتالی–مانند اعتراضات سال ۲۰۱۸ علیه دستورالعمل کپی‌رایت اتحادیه اروپا–را می‌بایست نماد تحرکات اعتراضی میلیون‌ها انسان و نه ربات‌های دیجیتال در نظر گرفت که برای ابراز نگرانی‌های خود از تهدیدات مرتبط با آزادی‌های برخط تلاش نمودند. این انسان‌ها بودند که تماس‌های تلفنی برقرار کردند، ایمیل فرستادند و اطلاعات خود را در رسانه‌های اجتماعی به اشتراک گذاشتند– و در همان حال در خیابان‌ها اعتراض کردند و در نهایت شعار موفقیت‌آمیز «ما ربات نیستیم» را معرفی نمودند.

اسطوره سی‌ویکم: اینترنتِ بدون سازمان، امکان سازماندهی را فراهم می‌آورد [1]

سباتین برگ[2]

باور عمومی: اینترنت نوعی سازمان اجتماعی و سیاسی را بدون ساختارهای سلسله‌مراتبی و انعطاف‌ناپذیر فراهم می‌کند. کاهش هزینه‌های ارتباطی و دگرگونی ناشی از فناوری‌های دیجیتال، شبکه سازی از پایین به بالا را امکان‌پذیر می‌کند، و این باعث می‌شود اشکال نهادی سیاست منسوخ شود، اعمال قدرت را به حداقل برساند و در نهایت جامعه دموکراتیک رادیکال را به وجود آورد.

اصل موضوع: ایده جامعه مساوات‌گرا و فراگیر یکی از باورهای عمومی پایه اینترنت است؛

1. **Source:** Clay Shirky, Here Comes Everybody. The Power of Organizing without Organization (London: Penguin Books, 2008); Fred Turner, From Counterculture to Cyberculture (Chicago/London: University of Chicago Press, 2006).
2. Sebastian Berg

همان‌طور که جان پری بارلو[1] بیان کرده است: «ما دنیایی را ایجاد می‌کنیم که همه می‌توانند بدون برتری و تعصب نژادی، اقتصادی، نظامی یا جغرافیایی (محل تولد) در آن حضور داشته باشند» (بارلو، ۱۹۹۶) (ارجاع به اسطوره ۲۸). اساساً فرض بر این بود که اینترنت ابزارها یا پلتفرم‌های ارتباطی‌ای را فراهم می‌کند که به‌راحتی قابل استفاده باشند و ارتباطات را تقویت می‌کند، بنابراین به‌طورطبیعی تشکیل گروه‌های جدید، همکاری متقابل و احتمال مشارکت بدون ساختار رسمی را تسهیل می‌کند و ارتقا می‌بخشد (شرکی[2]، ۲۰۰۸).

اگرچه ما در بسیاری از موارد شاهد ناپدید شدن دروازه‌بانی‌ها و مصادیق آنها بوده‌ایم، این امر به‌خودی‌خود در مورد ساختارها و نهادهای (سیاسی) صدق نمی‌کند. همان‌طور که ملوین کرانزبرگ[3] می‌نویسد، «فناوری نه خوب است و نه بد؛ و نه بی‌طرف است». اینترنت دربرابر بازطراحی شدن باز و منعطف است و شرایطی را که تحت آن به اجرا در آمده است را بازتاب می‌دهد. هر زیرساختی می‌بایست به‌صورت عملیاتی آماده، منابع مالی آن تأمین و در نهایت در ساختار اجتماعی تعیین شده برای آن ادغام شود تا «فعالیت‌های جدیدتر رسانه‌ای در حوزه‌های متداخل و پیچیده‌تر رسانه و سیاست ادغام شده و منطق و رویه‌های رسانه‌های قدیمی‌تر را اتخاذ نمایند» (چادویک ۲۰۱۳). در حقیقت، همان‌طور که عبارت «کد همان قانون است» نشان می‌دهد (لسیگ، ۱۹۹۹) (ارجاع به اسطوره ۳)،ابزارهای مبتنی‌بر اینترنت به‌طور کل ساختارهایی هستند که در اطراف آن سازماندهی شکل می‌گیرد. آنها بسته به معماری پلتفرم و برداشت اجتماعی که طبق آن طراحی شده‌اند، تأثیر ساختاری از خود بروز می‌دهند.

این باور عمومی از «ایدئولوژی کالیفرنیایی[4]» سرچشمه گرفته است، ترکیبی از یک ضد فرهنگی آنارشیستی جایگزین و اتوپیای آزادی‌گرای فناورانه که نیاز به ساختارهای رسمی قدرت را به نفع «تعامل بی‌وقفه بین افراد مستقل و نرم‌افزارهای آنها» رد می‌کند (باربروک/ کامرون ۱۹۹۶). در واقع، می‌توان آن را به‌عنوان اسطوره پایه‌گذار اقتصاد دره سیلیکون در نظر گرفت که با موفقیت شرکت‌های بزرگ اینترنتی به مقبولیتی جهانی دست یافته است (ترنر ۲۰۰۶). بااین‌حال، این مقبولیت نباید با وضعیت فعلی اینترنت و ادعای تملک اینترنت

1. John Perry Barlow
2. Shirky
3. Melvin Kranzberg
4. Californian Ideology

توسط جامعه و مباحث مرتبط اجتماعی اشتباه گرفته شود. در مواجهه با نظرهای مشکوک مانند اهمیت «توسعه زیرساخت‌های اجتماعی جهت ایجاد ساختار قدرت برای مردم در راستای ساخت جامعه‌ای جهانی که برای همه انسان‌ها کارآمد باشد» (زاکربرگ ۲۰۱۷)، نباید این واقعیت را فراموش کنیم که اقتصاد مبتنی‌بر اینترنت نه تساوی‌گرا است و نه منحصراً از پایین به بالا و نه دموکراتیک، بلکه با تکیه بر تمرکزگرایی، نهادینه‌سازی و تأسیس ساختارهای نظارتی جدید تعریف می‌شود (ون دایک / پول ۲۰۱۸). ازآنجاکه فناوری همواره بازتاب‌دهنده شرایط اجتماعی‌ای می‌باشد که در آن محقق شده است، ترجیح می‌دهیم به جای گسترش اسطوره‌های بازاریابی، از انتقاد ایدئولوژیک بهره‌مند شویم.

حقیقت: با وجود آنکه ما می‌توانیم شاهد تحول ساختاری در شیوه سازماندهی سیاسی و اشکال پیونددهنده کنش جمعی باشیم، تاکنون نهادهای موجود (سیاسی) مانند دولت، احزاب یا شرکت‌ها در موقعیتی برتر برای انطباق با امکانات فناوری دیجیتال باقی مانده‌اند. ابزارهای دیجیتالی برای جامع ساختن هرچه بیشتر سازمان‌ها و کاهش موانع قدیمی به‌کار گرفته می‌شوند، اما آنها هیچ‌گاه جایگزین سازمان‌ها و سیاست نمی‌شوند.

اسطوره سی‌ودوم: محصولات دیجیتال غیرمادی هستند [1]

فابیان فراری و مارک گراهام[2]

باور عمومی: دولت‌ها، خیرین، شرکت‌ها و سازمان‌های جهانی در سراسر جهان فعالیت‌های دیجیتالی را عامل رشد اقتصادی مناطق روستایی و حاشیه‌ای تلقی می‌کنند. یکی از دلایل اصلی این گفتمان‌های خوش‌بینانه، فرضیهٔ طبیعت غیرمکانمند و غیرمادی محصولات دیجیتالی

1. **Source:** Mark Graham, Isis Hjorth and Vili Lehdonvirta, Digital labour and development: impacts of global digital labour platforms and the gig economy on worker livelihoods. Transfer: European Review of Labour and Research, 23 (2017) 2, 135-162; Mark Graham and Mohammad Amir Anwar, The Global Gig Economy: Towards a Planetary Labour Market? First Monday 24 (2019) 4, doi.org/10.5210/fm.v24i4.9913.
2. Fabian Ferrari and Mark Graham

است. به‌بیان‌دیگر، به‌دلیل غیرمادی بودن اینترنت می‌توان کار را از هرجایی در دنیا پیش برد و هدایت نمود.

اصل موضوع: فعالیت و شبکه‌هایی که ارزش و مفهوم دیجیتالی بودن را دریافته‌اند، به‌طور فزاینده در سیستم‌های جهانی گنجانده و ادغام می‌شوند. ازآنجاکه بیش از گذشته جریان کالاها و تجارت فراتر از بازارهای کار محلی صورت می‌گیرند، زنجیره‌های تأمین دیجیتالی پنهان توجه کمتری به محل انجام کار نشان می‌دهند.

افرادی که در شبکه‌های تولید دیجیتال مشغول به فعالیت هستند خروجی‌های غیرمادی (غیرکالایی) تولید می‌کنند. این خروجی‌ها می‌توانند به‌سرعت به هر جایی از کره زمین منتقل و ارسال شوند. این بدان معناست که در فعالیت‌هایی که به‌جای دانش فنی، به تولید و پردازش دانش رمزگذاری‌شده متکی هستند، نزدیک بودن کارگران و مواد و موضوعات کاری آنها دیگر اهمیتی نخواهد داشت.

برای بسیاری از مفسران، این واقعیت که پیمانکاران آمازون[1] در رومانی به مکالمات الکسا[2] گوش می‌دهند یا این‌که فیس‌بوک[3] به پیمانکاران هندی مأموریت خواندن پیام‌های خصوصی کاربران را داده است، نقض مشهود حقوق حریم خصوصی است (ارجاع به اسطوره ۴۵). باوجوداین، فراتر از نگرانی‌های معمول در زمینه نقض حریم خصوصی، این موارد نمونه‌ای از شبکه‌های جهانی است که همواره بی‌درنگ و در زمان حقیقی فعالیت شناختی[4] را استخراج می‌نماید. به‌عبارت‌دیگر، محصول را می‌توان در مقیاس جهانی غیرمکانمند ساخت (فارغ از مرزهای جغرافیایی در مقیاس جهانی ارائه داد). این بحث را نمی‌بایست دلیلی بر بی‌اهمیت شدن جغرافیا تلقی نمود. کاملاً برعکس! شبکه‌های تولید دقیقاً در مکان‌هایی با سودمندترین اقتصاد سیاسی مستقر می‌شوند.

بنابراین شبکه‌های تولید دیجیتال معاصر تلاش می‌کنند محصولات تولیدشده به‌صورت الگوریتمی یا دستی را در هم ادغام نمایند. در تاریخ سرمایه‌داری قابل مشاهده نبودن شبکه‌های تولید کالا برای مصرف‌کنندگان پدیده جدیدی نیست. اما در مورد کالاهای غیرمادی مانند

1. Amazon
2. Alexa
3. Facebook
4. Cognitive Labour

نرم‌افزارهای تشخیص چهره یا دستیار گفتار[1] دیگر نمی‌توان به زنجیره تولید به همان شیوه سنتی نگریست، یعنی همان‌طور که برای کالاهایی مانند قهوه یا شکلات معمول بوده است، زیرا این سیستم‌ها همیشه در حال شکوفایی هستند و هرگز ماهیت ثابتی ندارند. براین‌اساس، سیستم‌های هوش مصنوعی را تا حدودی می‌توان به توهمات و خیالات فنی تشبیه نمود، زیرا همیشه به جای بودن (ایستایی) در حال تبدیل شدن و شکل گرفتن (تحول) هستند. این در حالی است که نیروی کار زیادی نیز به‌صورت مداوم در حال مرتفع نمودن نواقص آنها هستند. آنچه به‌عنوان نوآوری‌های هوش مصنوعی مورد توجه قرار می‌گیرد، اغلب حاصل تلاش مشترک کار شناختی با کار تعداد توجه‌پذیری از نیروی انسانی کم‌درآمد (با دستمزدی کمتر از میزان متعارف) است (ارجاع به اسطوره ۴۳).

اهمیت دادن به جنبه مادی فعالیت دیجیتالی، ما را قادر می‌سازد تا سؤالات مهمی را در ارتباط با ماهیت تولیدات دیجیتال از جمله مونتاژ یا غیرمونتاژ بودن، مادی یا غیرمادی بودن، مکانمند[2] یا غیرمکانمند[3] بودن آنها مطرح نماییم.

حقیقت: فعالیت دیجیتال هرگز به‌صورت مجزا (ایزوله شده) از زیرساخت‌هایی که نقش واسطه، تقویت‌کننده و معنادهنده به آنها دارند، مفهوم پیدا نمی‌کند. شبکه‌های تولیدی که سیستم‌های خودکار و محصولات انسانی را با یکدیگر درهم می‌آمیزند اشکال مختلفی از ارزش را ایجاد می‌کنند؛ و باوجود ماهیت به‌ظاهر غیرمادی خود، جغرافیای اقتصادی خاص را مورد بهره‌برداری قرار می‌دهند و ایجاد می‌کنند.

1. Speech Assistants
2. Territorialized
3. Deterritorialized

فصل چهارم
زیرساخت و نوآوری

اسطوره‌سی‌وسوم:فضای‌سایبری‌کاملاًازدنیای‌واقعی‌مجزااست(دوفضای‌متفاوت‌هستند)[1]

دانیل لامباچ[2]

باور عمومی: براساس منطق استثناگرای اینترنت، «اینترنت» نمایانگر فضایی است که از «دنیای واقعی» متمایز است. «فضای مجازی» و «فضای فیزیکی»[3] دو دنیای متفاوت هستند و دست‌کم ، باید براساس منطق، قوانین، ساختارها، هنجارها و بازیگران متفاوت اداره شوند.

اصل موضوع: ارائه‌های هنری، فضای مجازی را به‌عنوان یک فضای واحد با توپوگرافی منحصربه‌فرد و مرزهای خاص خود به تصویر می‌کشند، شاید به‌عنوان یک قاره، یک شبکه مترو یا یک ابر شبکه[4] (ارجاع به اسطوره ۳۵ و۳۷). در تمام این تصویرسازی‌ها، این مهم فرض شده است که فضای مجازی - به‌عنوان یک فضای جداگانه- از «دنیای واقعی» متمایز است. با قاطعیت می‌توان ادعا نمود که تمایز فضای مجازی از دنیای واقعی را به‌صورت کاملاً بی‌پرده می‌توان دراعلامیه استقلال «فضای مجازی» جُست که جسورانه اظهار می‌دارد: «دولت‌های جهان صنعت!

---

1. **Source:** John Perry Barlow, A Declaration of the Independence of Cyberspace (1996), https://projects. eff. org/~barlow/Declaration-Final.html; Daniel Lambach, The Territorialization of Cyberspace, International Studies Review (2019), https://doi.org/10.1093/isr/viz022 or https://www.researchgate. net/publication/308720083_ The_Territorialization_of_Cyberspace (ungated preprint).
2. Daniel Lambach
3. Meatspace
4. Network Cloud

ای غول‌های فرسوده گوشتالود و فولادین، من از فضای سایبری می‌آیم، خانه جدید ذهن» (بارلو ۱۹۹۶).

حامیان اتوپیای فناوری مایل بودند از فضای مجازی به‌عنوان «مرز الکترونیکی[1]» یاد کنند، و عامدانه در رؤیاپردازی خود از مرزهای آمریکا به‌عنوان سرزمین فرصت و عاری از دخالت‌های دولتی استفاده می‌کنند. چنین استعاره‌های مکانی هنوز هم بسیار رایج است. تعبیر معروف آنگلا مرکل از اینترنت به‌عنوان «قلمرو نامکشوف»[2] نیز همچنان ماندگار است. باتوجه‌به این‌که شناخت ما بر یک چشم‌انداز سه‌بُعدی[3] استوار است، استعاره‌های مکانی برای ما بیشتر طبیعی جلوه می‌کند. مطمئناً روش‌های مکان-محور برای تصویرسازی فضای سایبری یا ساختار شبکه‌ای اینترنت در تضاد هستند؛ هرچند هیچ‌کدام از آنها از قدرت کمتری در مقایسه با یکدیگر برخوردار نیستند (لمباک[4]، ۲۰۱۹). اما چنین طرز تفکری در فضای مجازی دو نقص مهم دارد.

اولاً، فضای مجازی یک مکان واحد نیست، بلکه یک فضای الکترونیکی مسطح است. در واقع، این فضا را می‌توان به‌عنوان مجموعه پیچیده‌ای از «قلمروهای سایبری» تلقی نمود که توسط کشورها، شرکت‌ها و کاربران ساخته شده است. کشورها «بخش‌های ملی» اینترنت را به‌طورمثال از طریق وضع قوانین داخلی (همچون محلی‌سازی داده‌ها، پرداختن به زیرساخت‌های موازی و تدوین دکترین دفاعی سایبری) ایجاد می‌کنند (ارجاع به اسطوره ۳۸). شرکت‌ها اکوسیستم‌های مشخصی در آن ایجاد می‌کنند که در آن محصول خود را بفروشند یا دست‌کم «کاربران» خود را بر اساس استانداردهای داخلی و سیاست‌های مدیریت محتوا به تبلیغ‌کنندگان بفروشند. کاربران از طریق اجتماعات برخط یا گروه‌های چت، قلمروهای کوچک و قابل انعطافی ایجاد می‌کنند. این قلمروها یا با یکدیگر هم‌پوشانی و تداخل دارند و یا مدام در حال تغییر هستند. درگیری‌ها و تداخلات معمول در آن بسیار زیاد است؛ به‌عنوان‌مثال، روش‌های بسیاری برای بررسی الزامات قانونی یک گفتار/سخنرانی برخط میان قلمروهای برخط «دولتی» و «شرکتی» وجود دارد (ارجاع به اسطوره ۶).

دوم، تمایز بین فضای «برخط» و «غیربرخط» در حال از بین رفتن است، البته اگر همچنین تمایزی اصالتاً مصداق داشته باشد. فضای مجازی را می‌توان از طریق تلفن‌های هوشمند،

1. Electronic Frontier
2. Neuland (Uncharted Territory)
3. Three-Dimensional Vision
4. Lambach

نمایشگرهای نوری، اینترنت اشیا[1] و دستگاه‌های متصل به آن و سایر دستگاه‌های فراگیر به «دنیای واقعی» وارد کرد. ارتباطات اجتماعی به‌خاطر تعاملات رودررو و نیز مداخلات فناوری (ارتباطات با واسطه فناوری) بیش از همیشه پیچیده شده است. «دنیای واقعی» از طریق فناوری‌های جغرافیایی که اساساً ماهیت اینترنت را تغییر می‌دهند وارد فضای سایبری می‌شوند. این روندها با ادغام موقعیت فیزیکی (مکانی) و فضاهای برخط، در حال ایجاد یک کلیت ترکیبی (هیبریدی) هستند، و بدین‌ترتیب بیش از گذشته فرضیه استثناگرائی اینترنت را نقض می‌نمایند.

حقیقت: فضای سایبری یک فضای واحد نیست بلکه مجموعه‌ای از «قلمروهای سایبری» است که دارای هم‌پوشانی و تداخل بوده و بعضاً دچار تغییر می‌شوند. علاوه‌براین، تقسیم‌بندی فضای سایبری و دنیای «واقعی» با فراگیر شدن علوم محاسباتی کمتر و کمتر قابلیت دفاع می‌یابد. به هرحال، دیگر نمی‌توان اینترنت را به مثابه یک فضای استثنایی تلقی نمود.

اسطوره سی‌وچهارم: هیچ نقطه نامعلومی در اینترنت وجود ندارد؛ همه به‌هم متصل‌اند[2]

مارتین دیتوس، سانا اوجانپرا، مارک گراهام[3]

باور عمومی: اینترنت یک «دهکده جهانی» است که جهان را به یک بازار جهانی و سپهر اجتماعی[4] تقلیل داده است؛ جایی که همه با هم ملاقات می‌کنند و همه به یک نوع از سطح خدمات دسترسی دارند. این «دنیای مجازی»، یا فضای سایبری، یک مکان مشترک و منفک از همه مکان‌های دنیای واقعی است.

---

1. IoT devices
2. **Source:** Mark Graham, Geography/internet: ethereal alternate dimensions of cyberspace or grounded augmented realities?, The Geographical Journal, 182–177 ,(2013) (2)179, https://papers.ssrn.com/ sol3/papers.cfm?abstract_id=2166874; Sanna Ojanperä, Mark Graham, Ralph Straumann, Stefano De Sabbata, Matt Zook, The Geography of Engagement in the Knowledge Economy: Regional Patterns of Content Creation, Information Technologies in International Development 51–33 ,(2017) 13; https://lra.le.ac.uk/handle/40079/2381
3. Martin Dittus, Sanna Ojanperä and Mark Graham
4. Social Sphere

اصل موضوع: امروز، دیگر نمی‌توانیم بگوییم که «مجازی» به وضوح از «واقعی»، و یا «غیر برخط» از « برخط» قابل تشخیص است (ارجاع به اسطوره ۳۳). اکنون که بیش از نیمی از جمعیت جهان به اینترنت متصل شده‌اند، زندگی ما آمیخته با اطلاعات دیجیتالی است که تجربه روزانه ما را افزایش می‌دهد و در پس آن درک ما از جهان و اقدامات ما در جهان را شکل می‌دهد، فارغ از این مهم که در کجای دنیا قرار گرفته‌ایم. تا حدودی این گسترش اتصال جهانی را می‌توان نتیجه فرایندهای مکانی دانست: از طریق ساخت کابل‌های جدید زیر آب اقیانوس‌ها و دریاها، قاره‌ها به یکدیگر متصل می‌شوند و شبکه‌های جدید منطقه‌ای که پهنای باند را به خانه‌ها و محل‌های کار می‌رسانند.

درعین‌حال، بسیاری از مناطق جهان همچنان از یکدیگر جدا هستند، به ویژه مناطق روستایی و دورافتاده. علاوه‌براین، نابرابری جدی در هزینه اتصال به اینترنت همچنان وجود دارد (ارجاع به اسطوره ۳۶): در بسیاری از کشورها، هزینه استفاده از پهنای باند هنوز بیش از حقوق متوسط ماهانه است. در نتیجهٔ این موانع، شاهد عدم توازن جهانی در مشارکت بالقوه دیجیتال هستیم، که عدم تعادل در ظرفیت حضور و شکل دادن به زندگی برخط است. این گره‌های بی‌پایان نابرابری‌هایی را در پوشش ایجاد می‌کند: برای بسیاری از مناطق جهان، اطلاعات دیجیتالی راجع به پلتفرم‌های علمی برخط هنوز به زبان محلی وجود ندارد و به‌عنوان‌مثال، با وجود تلاش‌های ویکی پدیا و ارائه اطلاعات به ۳۰۰ زبان محلی، همچنان عمومی‌ترین اطلاعات آن در مورد کشورهای جنوب (کشورهای موسوم به جنوب) غالباً به زبانی غیرمحلی، به خصوص به زبان انگلیسی نوشته شده است، و ازسویی‌دیگر محتوای ارائه شده راجع به دنیای جنوبی زمین اغلب توسط ویراستاران دنیای شمال (آمریکای شمالی یا اروپا) تولید و پایش می‌شود (ارجاع به اسطوره ۱۸). تا حدودی این شکاف‌های دیجیتال را می‌توان آیینه تمام قد وجود شکاف یا فاصله اقتصادی موجود دانست (ارجاع به اسطوره ۳۹). به‌طورهم زمان، درست همانند زمانی که اینترنت اولیه حضور مقتدرانه‌ای در آمریکا داشت، ما شاهد ظهور فرهنگ‌های موازی دیجیتال گوناگون هستیم. در بسیاری از مناطق جهان سکوها و پلتفرم‌هایی پدید آمده‌اند که جزئی از ساختار اصلی که در ابتدا توسط غرب ارائه شده بود، نیستند. این ساختار شامل WeChat و

Alibaba در چین، Grab و Shopee در جنوب شرقی آسیا، Flipkart و Reliance Jio در هند، MercadoLibre و Universo Online در آمریکای لاتین و موارد دیگر می‌شود. در آینده نزدیک، با آسیا به‌عنوان پیشران اصلی و آفریقا که ظرفیت توجه‌پذیری از خود برای رشد نشان داده، می‌توان رشد بیشتری را در مشارکت دیجیتالی غیرغربی‌ها پیش‌بینی کرد. در مقابل، پلتفرم‌های جهانی شامل غول‌های دیجیتال همچون گوگل، اپل، فیسبوک، آمازون، نتفلیکس و سایر بازیگران این عرصه ممکن است به سختی بتوانند خودشان را در این بازارهای نوظهور تطبیق بدهند.

حقیقت: اینترنت یک دهکده جهانی نیست، بلکه شبکه‌ای گسترده است که زندگی را در بسیاری از مناطق بسط و گسترش می‌دهد. به‌منظور درک بهتر این‌که «اینترنت» چیست؟، حداقل می‌بایست بر ده‌ها فرهنگ جهانی مسلط باشیم. محققان اینترنتی تنها در قلمروهای دیجیتالی خاصی به تحقیق و تفحص پرداخته‌اند. «فاصله» همچنان اهمیت دارد و به همین شکل خواهد ماند.

اسطوره سی‌وپنجم: اینترنت یک نظام شبکه‌ای است[1]

سباستین گابمن[2]

باور عمومی: اینترنت «شبکه‌ای از شبکه‌ها» است. اینترنت عناصر ناهمگن را نه‌تنها از لحاظ فنی، بلکه از نظر اجتماعی و اقتصادی به هم متصل می‌کند. این ساختار شبکه‌ای، اتصال جهانی و قابلیت تعامل و همکاری را تضمین می‌کند و دلالت‌هایی برای رویکردهای شبکه‌ای نظیربه‌نظیر[3] و ایده‌آل‌هایی برای تحقق ارزش‌های دموکراتیک در شبکه‌ای برابر دارد.

---

1. **Source:** John Day, How in the Heck Do You Lose a Layer!?, Future Network Architectures Workshop University of Kaiserslautern, 2012, https://www.researchgate.net/publication/261458332_How_in_the_Heck_ do_you_lose_a_ layer and John Day, Surviving Networking's Dark Ages or How in the Hell Do You Lose a Layer!? (IRATI RINA Workshop, Barcelona, 2013), http://irati.eu/wp-content/uploads/2013/01/1LostLayer130123.pdf; Tarleton Gillespie, Engineering a Principle: "End-to-End" in the Design of the Internet, Social Studies of Science 36 (3) (2006), 427–457.

2. Sebastian Gießman

3. Peer-To-Peer

اصل موضوع: اینترنتی که در اختیار ماست یک شبکه به‌هم پیوسته از شبکه‌های ناهمگن، آن‌طور که ممکن است متناقض به نظر برسد، نیست. پروتکل‌های شبکه زیرساخت‌ها را شکل می‌دهند، و زیرساخت‌ها خسته‌کننده و بوروکراتیک هستند و معمولاً بدون چالش، پذیرفته می‌شوند.

با این‌حال، توسعه‌دهندگان و مدیران پروتکل‌های شبکه در مورد ماهیت و تعاملات اجتماعی زیرساخت‌های دیجیتال و آنچه در طراحی پروتکل‌های شبکه از نظر سیاسی می‌بایست مورد توجه قرار گیرد، آگاه هستند (ارجاع به اسطوره ۴). در مصاحبه‌ای در سال ۲۰۰۶، دیوید رید[1]، محقق علوم رایانه، با ارائه توضیحاتی باعث شفاف‌سازی انتخاب‌های سیاسی توسعه‌دهندگان پروتکل دهه ۸۰ شد: «در حقیقت، ایده دنبال کردن چیزی به نام «اینترنت» (شبکه‌ای از مجموعه شبکه‌ها) یک بازی سیاسی بود که قابلیت همکاری جهانی را امری دست‌یافتنی و مطلوب جلوه می‌داد. این تعریف درواقع هم‌سو با تعریف «یک اروپای واحد» و یا «دولت جهانی» است، البته با درنظر گرفتن تفاوت‌هایی. مهندسان دست اندرکار این پروژه از پیامدهای احتمالی آن در سطوح سیاسی مربوطه مطلع بودند» (رید در ژیلسپی ۲۰۰۶، ۴۵۲). استدلال رید تا حدودی نمونه‌ای از تأثیرگذاری ارزش‌ها در طراحی پروتکل‌های اینترنتی و معماری نقطه‌به‌نقطه آن در دهه مذکور است. دیدگاهی که به یک نکته مهم تاریخی نیز بی‌اعتنایی می‌نماید.

«قابلیت همکاری جهانی» به استانداردسازی بستگی دارد، و پروتکل‌های شبکه درواقع استانداردهای واسطه‌ای دیجیتال را تشکیل می‌دهند. در ۱ ژانویه ۱۹۸۳، برنامه کنترل انتقال[2] و پروتکل اینترنتی[3] توسط وزارت دفاع ایالات متحده به‌عنوان استاندارد وضع شدند. دانشگاه‌های آمریکا از این دستورالعمل پیروی کردند و به استقبال آنها رفتند. ماحصل آن انتقال در آرپانت چه بود؟ به نظر جان دی[4]، دانشمند رایانه، آن تغییر زیرساختی درواقع باعث از بین رفتن لایه شبکه‌بندی[5] شد. سعی کنید استدلال اصلی جان دی را با مطرح کردن پرسش «چگونه یک لایه را از دست می‌دهید؟»، فارغ از همه ظرافت‌هایش و تنها از لحاظ پیامدهای آن در نظر بگیرید؛

1.David Reed
2. Transmission Control Program (TCP)
3. Internet Protocol (IP)
4. John Day
5. Internetworking layer

وی در پاسخ تأکید می‌کند که شکاف میان برنامه کنترل انتقال و پروتکل اینترنتی «تنها اسماً اینترنت تلقی می‌شود» (دی ۲۰۱۳، ۲۲).

اتصال سیستم‌های باز[1] و سایر رویکردهای میان شبکه‌ای بر این مهم تکیه داشتند که شبکه‌های به‌هم پیوسته می‌توانند براساس فناوری‌های کاملاً متفاوت و طرح‌های آدرس دهی بنا شوند (ارجاع به اسطوره ۱۵). اما پروتکل اینترنت فقط یک فضای آدرس برای تمام شبکه‌های متصل ایجاد کرده و نظام نام‌گذاری دامنه‌ها نیز در امتداد آن وابستگی ایجاد شده است (ارجاع به اسطوره ۳۸). مادامی که از سیستم آدرس‌دهی پروتکل اینترنتی صحیح استفاده کنید، می‌توانید هر شبکه دیگری را با پروتکل‌های مبهم به اینترنت متصل نمایید. بنابراین شعار دهه ۱۹۹۰ میلادی مبنی‌بر «پروتکل اینترنتی در همه چیز[2]» منتج به شکل‌گیری ترکیبی از شبکه‌ها نشد. بلکه از بین رفتن لایه میان‌شبکه‌ای یک معماری شبکه‌ای که به لحاظ علمی سالم و از دیدگاه فنی تعامل پذیر است را تقویت نمود. در حال حاضر، می‌بایست به چنین نقصی عادت کنیم. اینترنت، آن‌طور که هنوز بسیاری از مردم فکر می‌کنند، فضایی برای شبکه ناهمگن ناهمگونی‌ها نیست: «سیستم‌های باز یک معماری اینترنتی داشتند و اینترنت یک معماری شبکه‌ای دارد» (دی ۲۰۱۲، ۱۵).

حقیقت: از زمان از بین رفتن لایه شبکه‌بندی در سال ۱۹۸۳، معماری اینترنت بر اساس یک سیستم همگن از نام‌گذاری و آدرس‌دهی بنا شد. سیستم نام‌گذاری دامنه[3] دقیقاً همین کار را می‌کند: یعنی ایجاد یک فضای یکپارچه برای آدرس‌های پروتکل اینترنتی که باید به‌صورت مرکزی اداره شود، حتی اگر مراحل ثبت دامنه غیرمتمرکز باشد. اینترنت فعلی شبکه‌های کاملاً ناهمگن را به هم متصل نمی‌کند، بلکه فقط در قامت یک شبکه واحد در سطح نام‌گذاری و آدرس‌دهی باقی می‌ماند. بنابراین پرسش اصلی چنین خواهد بود: چه زمان شبکه‌بندی واقعی خواهیم داشت؟

1. Open Systems Interconnection (OSI)
2. IP on Everything
3. DNS

اسطوره سی‌وششم: ما برای اینترنتی که توسط دیگران ارائه شده است، هزینه می‌پردازیم[1]

باب فرانکنستون[2]

باور عمومی: ما اینترنت را به‌عنوان سرویسی که توسط یک «ارائه‌دهنده» عرضه می‌شود یا به‌عنوان مکانی که به آن دسترسی پیدا می‌کنیم، در نظر می‌گیریم. مشترک اینترنت می‌شویم، هزینه دسترسی به اینترنت را می‌پردازیم و درنهایت نگران اتمام بسته‌های اینترنتی خریداری شده هستیم.

اصل موضوع: در بهار سال ۱۹۷۳، در یک کلاس ثبت نام کردم که در آن درباره ALOHAnet در هاوایی اطلاعات کسب کردم، برنامه‌ای متشکل از رایانه‌ها و رادیوها. در آن کلاس، چنانچه بسته‌ای از داده‌ها گم می‌شد، برنامه رایانه‌ای مجدداً آن بسته را ارسال می کرد. یکی از هم‌کلاسی‌های من به نام باب متکالف[3]، از این ایده برای پایه‌گذاری فناوری شبکه‌ای معروفش به نام اترنت[4] استفاده کرد. در سال ۱۹۶۰ رایانه‌ها به اندازه کافی سریع شده بودند، بنابراین نیازی به تکیه بر خدمات و سرویس‌های یک شرکت واسطه یا حامل وجود نداشت و در صورت گم شدن بسته‌ها در بستر شبکه، می‌توانستیم به‌سرعت آنها را مجدداً ارسال کنیم. حتی می‌توانستیم به‌صورت بلادرنگ داده ارسال نماییم[5] و بسته‌های گمشده را نادیده بگیریم.

دهه ۱۹۹۰ هنگامی که مشغول کار روی بستر شبکه‌های خانگی در شرکت مایکروسافت بودم، در واقع به اهمیت این‌که این شبکه‌ها، به معنا و مفهوم سنتی آن فقط یک سرویس معمولی مثل ریل راه‌آهن نیستند که به شما اطمینان می‌دهد بسته‌هایتان بالاخره به مقصد خواهند رسید، پی بردم. خوشبختانه دوستان و همکارانم وظیفه کار با شبکه‌های مختلف میان شبکه‌ای را برعهده داشتند و در نهایت به قدرت این فناوری پی بردند. این فناوری نام «اینترنت» را یدک می‌کشید، اما دیگر محدود به یک شبکه نبود بلکه تبدیل به راهی شده بود برای استفاده از تمامی امکانات و تجهیزات موجود بدون نیاز به داشتن واسطه یا حامل. این امر به شبکه‌های مختلف اجازه می‌دهد از تمام

1. **Source:** Jerry H. Saltzer, David P. Reed and David D. Clark, End-to-end Arguments in System Design, ACM Transactions on Computer Systems (TOCS) 2 (1984) 4, 277-288, http://web.mit.edu/Saltzer/ www/publications/ endtoend/endtoend.pdf; Calvin Hennick, How ALOHAnet Helped Hawaii Make Waves in Networking and IT Innovation, StateTech, 30 June 2016, https://statetechmagazine.com/ article/2016/06/how-alohanet-helped-hawaii-make-waves-networking-and-it-innovation.

2. Bob Frankston 3. Bob Metcalfe 4. Ethernet 5. Stream

زیرساخت‌های موجود از جمله امکانات ارتباطی و مخابراتی استفاده نموده و آنها را به یک شبکه متصل[1]مشترک تبدیل کنند. براین‌اساس، اینترنت دیگر تنها تعریفی از یک مکان نیست، بلکه روشی است که ما طی آن از تمامی امکانات و تجهیزات (در قالب شبکه‌ای از شبکه‌های به هم متصل) موجود استفاده می‌کنیم (ارجاع به اسطوره ۳۵).

چنانچه داده‌ها را به‌مثابه «بار» یا یک «محمولهٔ فیزیکی» در حال ارسال در نظر بگیریم، این قیاس نادرست است: زیرا برخلاف یک شبکه سنتی، در اینترنت لزوماً داده‌ای («محتوا») ارسال نمی‌شود، بلکه یک کُد یا رفرنس در شکل URL به یک صفحه وب ارسال می‌شود. هنگام ثبت سفارش از آمازون نیز اتفاق مشابهی می‌افتد و ساختار شبکه این شرکت به‌جای درخواست حمل و نقل کالا از ساختمان مرکزی مستقر در سیاتل، با ارسال شماره مرجع کالا به نزدیک‌ترین انبار عملیات ارسال را شروع می‌کند.

به لطف استفاده از پروتکل‌های متداول، تلاش‌های فردی یا متفرقه (شبکه‌های متفرقه) در یک «کل» ادغام می‌شود که ما از آن به‌عنوان «اینترنت» یاد می‌کنیم. این ساختار یا کلیت توسط یک مرجع مستقل ارائه نمی‌شود، بلکه از تلاش مشترک شبکه‌های متفاوت ظهور می‌یابد. این ساختار همچنین محدود به میزان اطلاعاتی که ما در آن قرار می‌دهیم نیست؛ بلکه به کمک ایده‌های جدید و ایجاد امکانات جدیدتر مدام رشد می‌نماید.

حقیقت: اینترنت آن خدماتی نیست که ما از ارائه‌دهندگان خریداری می‌کنیم، بلکه روش استفاده ما از پیام‌ها و امواج است. هنگامی که یک اتصال پهنای باند[2] خریداری می‌کنیم، درواقع هزینه عبور از یک دروازه را می‌پردازیم. به‌بیان‌دیگر، هزینه پرداخت شده برای خود اینترنت نیست، بلکه جهت عبور از مانعی به نام ساختار خدمات آبونمان-محور[3] است. بنابراین برای بهبود شرایط، ایجاد زیرساخت اینترنت بومی[4] امری ضروری است.

1.Inter-Network
2. Broadband Connection
3. Paywall
4. Internet-Native Infrastructure

اسطوره سی‌وهفتم: اینترنت هم‌اکنون درابرها است[1]

دانیل ولسن[2]

باور عمومی: اینترنت ما را از محدودیت فضای فیزیکی رهایی می‌بخشد. داده‌های ما هم‌اکنون به شکل «ابر»[3] در آمده است، و ما می‌توانیم از هر کجا و در هر زمان و اغلب با استفاده از دستگاه‌های تلفن همراه بی‌سیم به آن دسترسی پیدا کنیم. بنابراین ارتباطات ما از آن نظم قدیمی وستفالی[4] که به تعریف و تعیین قلمرو دولت‌ها می‌پرداخت، فراتر رفته است.

اصل موضوع: اینترنت به زیرساخت‌های عظیم فیزیکی وابسته است: بیش از ۹۰٪ از کل ترافیک جهانی اینترنت امروزه از طریق کابل‌های زیردریایی انجام می‌شود. بسیاری از سرویس‌های برخط که هر روز از آنها استفاده می‌کنیم، از جمله سرویس‌های مختلف «ابری»، به مراکز داده عظیم نیاز دارند. همچنین تلفن‌های هوشمند ما بدون تکیه بر شبکه‌ای متراکم از زیرساخت‌های شبکه تلفن همراه که آنها را به اینترنت جهانی متصل می‌کند کاملاً بی‌فایده خواهند بود.

در بیشتر موارد، این زیرساخت‌ها متعلق به شرکت‌های خصوصی است. ازاین‌رو، جای تعجب نیست که توسعه آنها با ملاحظات کاملاً اقتصادی طراحی شده و شکل گرفته باشند. بنابراین، شرکت‌های خصوصی در مناطقی که نوید بازده مالی بیشتری را می‌دهند، سرمایه‌گذاری گسترده‌تری خواهند داشت: بنابراین در بسیاری از کشورها مناطق شهری بهتر از مناطق روستایی به اینترنت متصل می‌شوند و ایالت‌های با رونق اقتصادی بالا در مقایسه با ایالت‌های در حال توسعه پیوندهای بیشتر و قوی‌تری با شبکه جهانی دارند (ارجاع به اسطوره ۳۹).

علاوه‌براین، در یک معنای کلی، زیرساخت‌های فیزیکی اینترنت، آن را دقیقاً به پیمان جهانی وستفالی پیوند می‌دهد که براساس آن، قلمرو دولت‌ها و کشورها تعیین می‌شد. کلیه اتصالات کابلی، روترهای ایستگاه‌های بی‌سیم، نقاط تبادل اینترنت (IXP)، مراکز داده و سرورها موقعیت

1. **Source:** Tara M. Davenport, Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis, Catholic University Journal of Law and Technology 24 (2015), https://scholarship.law.edu/jlt/vol24/ iss1/4; Laura DeNardis, Hidden Levers of Internet Control. An Infrastructure-Based Theory of Internet Governance, Information, Communication & Society 15 (2012) 5, 720-738, https://www.tandfonline. com/doi/full/10.1080/1369118X.2012.659199.

2. Daniel Voelsen 3. Clouds 4.Westphalian Order

فیزیکی دارند و بنابراین می‌بایست تابع قوانین کشورهایی باشند که در آن قرار دارند. تنها موارد استثنا در این زمینه، بخش‌هایی از کابل‌های زیردریایی که در اقیانوس‌های آزاد قرار دارد و همچنین ماهواره‌هایی در حال حرکت در فضا می‌باشند. فراتر از گذشته، تعداد بیشتری از کشورها تلاش می‌کنند تا کنترل زیرساخت‌های فیزیکی اینترنت را به‌عنوان ابزاری برای اداره مؤثرتر آنچه که از آن به‌عنوان «سهم آن کشور» از اینترنت تلقی می‌شود، به دست بگیرند. یکی از بی‌رحمانه‌ترین رویکردها، مجبور کردن شرکت‌های مخابراتی برای محدود سازی یا قطع کامل دسترسی اینترنت به‌منظور سرکوب تبادل اطلاعات بین شهروندان خودشان است. تعدادی از کشورها با شیوه‌ای پیچیده‌تر سعی در کنترل و اعمال نظارت دقیق بر اطلاعاتی دارند که به محدوده آنها وارد یا از آنجا خارج می‌شود.

به‌عنوان‌مثال، آنها این کار را با محدود کردن نودهایی[1] که کاربران اینترنت داخلی را به وب جهانی وصل می‌کند اعمال می‌نمایند؛ سپس با استفاده از سازوکارهای مختلف فیلترهای خاص برای مسدود کردن اطلاعات ناخواسته تعریف می‌کنند. نوع دیگر از نظارت، اعمال قوانین «محلی‌سازی داده‌ها» است که توسط آن کشورها سعی می‌کنند کنترل زیرساخت‌های فیزیکی را تحکیم بخشند. موضوع اصلی در پَس «محلی‌سازی داده‌ها» این است که کشور مورد نظر تنها راه دسترسی به بازار آن کشور را منوط به ذخیره‌سازی داده‌های کاربران در پایگاه‌های دادهٔ واقع در همان کشور معرفی می‌کند.

حقیقت: اینترنت به زیرساخت‌های پیچیده جهانی بستگی دارد. این زیرساخت علاوه‌بر لایه منطقی استانداردهای نرم‌افزاری و پروتکل‌ها، شامل اجزا و ابعاد فیزیکی مانند کابل‌های زیردریایی و مراکز داده ها نیز می‌شود. این لایه فیزیکی ناگزیر اینترنت را به دنیای قلمرو دولت‌ها و حکومت‌ها پیوند می‌دهد و بنابراین توجه بیشتری را طلب می‌نماید.

1. Node

اسطوره سی‌وهشتم: نظام نام‌گذاری دامنه متضمن جهانی‌بودن اینترنت است[1]

رابین تیم ویس[2]

باور عمومی: اینترنت با ساختار و ماهیتی جهانی طراحی شده است. نظام نام‌گذاری دامنه[3] به‌عنوان دفترچه تلفن اینترنت به همراه چندین سرویس‌دهنده اصلی داخلی از این‌که هرکس هر زمان که دوست داشته باشد به هر سایتی که می‌خواهد برسد اطمینان حاصل می‌کند. این انعطاف‌پذیری غیرمتمرکز پایه‌ای برای همیشه دوام خواهد داشت.

اصل موضوع: زیرساخت‌های TCP / IP نتیجه یک رؤیاپردازی قدیمی است، زیرا کشورها به‌سرعت در حال ارائه و پیشبرد برنامه‌ها و راه‌های جدیدی برای دور زدن DNS هستند. در واقع، اینترنت به‌طور تمام‌وکمال کپی‌برداری و در سیلوهای محتوای ملی درج شده است. جدیدترین روش در جهت تخریب و دور زدن DNS در روسیه در حال انجام است. دولت روسیه در تلاش‌های اخیر خود، به‌طور فعال به‌دنبال بازنویسی و بازطراحی ساختار DNS فعلی است؛ این مهم با ایجاد «سیستم سرورهای پشتیبان نام دامنه ریشه که خارج از کنترل ICANN[4]، IANA[5] و VeriSign» است و در مصوبه اخیر «حکمرانی اینترنت» تصویب و توضیح داده شده است، فراهم خواهد شد. عربستان سعودی نیز تلاش‌هایی «حاکمیتی» را اخیراً به‌کار گرفته و تقلید کرده است که طی آن دولت اقدام به محدود کردن DNS کرده است؛ به‌بیان‌دیگر، ترافیک درخواست DNS در این کشور از طریق خدمات پراکسی تحت کنترل ملی عربستان پایش و هدایت می‌شود. فعالیت‌هایی ازجنس ملی‌سازی اینترنت بر خلاف تلاش‌های اولیه بین‌المللی توسط سازمان‌هایی مانند CSNET[6] یا صفحهٔ معماری اینترنت[7] که در سال ۱۹۸۳ برای هدایت تکامل مجموعه

1. **Source:** William Lehr et al., "Whither the Public Internet?," Journal of Information Policy 9 (2019): 1–42, https://doi.org/10.5325/jinfopoli.9.2019.0001; Charlotte Jee, "Russia Wants to Cut Itself off from the Global Internet. Here's What That Really Means.," MIT Technology Review, 21 March 2019, https://www. technologyreview. com/s/613138/russia-wants-to-cut-itself-off-from-the-global-internet-heres-whatthat-really-means.
2. Robin Tim Weis
3. Domain Name System (DNS)
4. The Internet Corporation for Assigned Names and Numbers
5. The Internet Assigned Numbers Authority
6. The Computer Science Network (CSNET)
7. IAB

پروتکل TCP/IP و ارائه مشاوره‌های تحقیقاتی ایجاد شده بود، در جوامع دیجیتال در حال رشد است.

باتوجه‌به اخلاق بنیادین اینترنت، پروتکل‌های آن به‌صورت آشکار در دسترس بوده‌اند و ازآنجاکه این شبکه از ساختاری میان شبکه‌ای تشکیل یافته است، بنابراین بازطراحی و بازسازی مجدد شبکه‌ای متفاوت مشتمل‌بر شبکه‌های بهم پیوسته کاملاً ممکن است.

به نظر می‌رسد دولت‌های اقتدارگرا مشتاق زدودن خود از آنچه بعدها از آن به‌عنوان DNS «غربی» یاد می‌کنند، هستند؛ و بنابراین در تلاشند تا واقعیت کاملاً متفاوتی برای اکثر کاربران اینترنت خود رقم بزنند. اگر برخی از دولت‌ها تصمیم بگیرند برخی دامنه‌های ملی را از سرورها حذف نمایند، کاربران در آینده‌ای نزدیک شاهد حذف شدن تدریجی کشورها از اینترنت جهانی خواهند بود. این مهم را می‌توان به‌عنوان درآمدی بر شکل‌گیری و تولد اینترنت چند پاره[1] فرض نمود.

حقیقت: باوجود این‌که زیرساخت‌های اینترنت جهانی تصور شده‌اند، به آرامی وارد دوره اینترنت‌های متعدد ملی، منقطع و داخلی می‌شویم. دولت‌ها در سراسر جهان مشتاق‌اند تا با «اینترنت چندپاره» داخلی به زندگی دیجیتال خود ادامه دهند. کاربران دیگر نباید انتظار داشته باشند که بتوانند به همه وب‌سایت‌ها دسترسی پیدا کنند. ماهیت باز DNS در حال تجزیه (نابود) شدن است.

اسطوره سی‌ونهم: «بی‌طرفی شبکه» در کل اینترنت تأمین شده است[2]

برنادت کالیفانو و ماریانو زاکرفلد[3]

باور عمومی: قوانین بی‌طرف، فعالیت‌های تبعیض‌آمیز را در اینترنت منع می‌کنند و بنابراین رفتار یکسان را برای تمام بسته‌های اطلاعاتی مستقل از ماهیت کاربر، محتوا، پلتفرم، مکان

1. Splinternet
2. **Source:** Mariano Zukerfeld and Bernadette Califano, Discutiendo la neutralidad de la red. De los discursos dominantes a las prácticas en contextos periféricos, 8 Commons (2019) 1, 5-43; Martin Cave and Pietro Crocioni, Does Europe Need Network Neutrality Rules?, 1 International Journal of Communication679-669,(2007)
3. Bernadette Califano and Mariano Zukerfeld

یا برنامه تضمین می‌کنند. با ترویج آزادی بیان، رقابت و تبادل اطلاعات در اینترنت، قوانین بی‌طرفانه شبکه جلوی رفتار ناعادلانه کاربران اینترنت را می‌گیرد.

اصل موضوع: تعامل بی‌طرفانه با بسته‌های اطلاعاتی بدون توجه به کاربر، محتوا، پلتفرم و غیره به‌ندرت در کشورها دیده می‌شود؛ این امر حتی در کشورهایی که قوانین مستقیم راجع به تعامل بی‌طرفانه دارند، نیز مصداق می‌یابد؛ به‌طورخاص در کشورهای حوزه جنوب. پنج مطالعه تجربی در گذشته این‌طور نشان می‌دهند که اقدامات مدیریت ترافیک که توسط ISP انجام می‌شود، اولویت‌بندی برخی بسته‌های داده را درمقایسه‌با دیگران نشان می‌دهد. عدم شفافیت در ارتباط با این دسته از اقدامات نشان‌دهنده وجود اهداف و محرک‌های اقتصادی است تا دلایل فنی سفت و سخت.

برخی از ارائه‌دهندگان قدرتمند خدمات یا محتوا، با هدف تقویت و بهبود تبادل داده‌ها از شبکه‌های توزیع محتوا (CDN) بهره می‌برند، یا بخشی از یک توافق همکاری مشترک با سایر ارائه‌دهندگان خدمات می‌شوند. بنابراین، بازیگرانی که می‌توانند هزینه این دسته از خدمات اضافه را بپردازند، از بهبود کیفیت تبادل اطلاعات توجه‌پذیری بهره خواهند برد به شکلی که سرعت توزیع مطالب آنها در برابر سایر ارائه‌دهندگان محتوا و خدمات افزایش ملموسی خواهد داشت. بی‌طرفی شبکه به‌عنوان یک اصل برای تبادل سیگنال به معنی ممانعت از وقوع تبعیض در لایه‌های بالاتر مدل OSI [1] نیست؛ نمونه بارز آن را می‌توان در رتبه‌بندی موتورهای جستجو مشاهده نمود. در نتیجه، برخی از بسته‌های اطلاعاتی–و در پی آن کاربرانی که آنها را ارسال و دریافت می‌کنند– از ساختار اولویت‌بندی حذف می‌شوند. عدم شفافیت الگوریتم‌ها و نبود ساختار «بی‌طرفی در جستجوها» درواقع اصل برخورد یکسان با کاربران اینترنت مخصوصاً در دسترسی/عدم دسترسی آنها به محتوا و رده‌بندی پلتفرم‌ها را نقض می‌نماید.

اختلاف موجود در پهنای باند بین کشورها باعث ایجاد تبعیض درمورد بسته‌هایی می‌شود که از کشورهای حاشیه‌ای با پهنای باند کمتر مخابره می‌گردند. میانگین سرعت بارگیری (دانلود) جهانی در سال ۲۰۱۸ برابر با ۴۵ مگابیت بر ثانیه بود. حال آنکه این میانگین سرعت در سوئد ۹۴

1. The Open Systems Interconnection model

مگابیت در ثانیه، در ایالات متحده ۹۲ مگابیت در ثانیه بود؛ درحالی‌که همان زمان در آمریکای لاتین میانگین سرعت ۱۹ مگابیت در ثانیه و در آفریقا ۱۴ مگابیت بر ثانیه رصد شده بود. تفاوت بین سرعت بارگذاری و بارگیری به‌معنای اولویت‌بندی ترافیک برخی بسته‌های داده درمقایسه‌با دیگر بسته‌ها است. به‌طور کلی، در اکثر نقاط دنیا سرعت بارگذاری بسیار کندتر از سرعت بارگیری (به ترتیب ۴۵ و ۲۲ مگابیت بر ثانیه) است. بنابراین این اصل که تقریباً در همه جا تولیدکننده بودن دشوارتر از مصرف‌کننده بودن است را تأیید می‌نماید. مطمئناً، درصورت در نظر گرفتن وجود تفاوت در مورد پهنای باند و کشورهای حاشیه‌ای، این وضعیت بدتر می‌شود: به‌عبارت‌دیگر بسته‌های دادهٔ تولیدکنندگان مستقر در کشورهای حاشیه‌ای با پهنای باند کمتر مورد تبعیض واقع شده و به حاشیه رانده می‌شوند، هرچند قوانین بی‌طرفی شبکه در حال اعمال باشد.

بنابراین با وجود دلایل کلان اقتصادی حتی اگر قوانین بی‌طرفی شبکه به‌شکل‌رسمی وجود داشته باشد، به‌دلیل قدرت خرید پایین، با کاربران ساکن در کشورهای حاشیه‌ای همچنان ناعادلانه رفتار خواهد شد. این مهم به‌ندرت توسط حامیان رویکرد بی‌طرفی شبکه مورد توجه قرار گرفته است.

حقیقت: قوانین بی‌طرفی شبکه درواقع می‌تواند از اعمال تبعیض مربوط به تبادلات داده جلوگیری نماید، اما این مهم بیشتر به نفع تولیدکنندگان و ارائه‌دهندگان خدمات است تا یکسان‌سازی شرایط برای کاربران و تولیدکنندگان محتوای ساکن در کشورهای «حاشیه‌ای»، زیرا در نهایت بسته‌های اطلاعاتی این کاربران است که طی اشکال مختلف از اولویت‌بندی ارائه خدمات حذف می‌شود. بنابراین، رویکردهای بی‌طرفی شبکه به‌تنهایی متضمن رفتار برابر با کاربران و محتوای تولیدشده در کشورهای دارای سطح دسترسی پایین‌تر به اینترنت نیست.

اسطوره چهلم: اینترنت باعث دموکرات‌شدن نوآوری می‌شود[1]

آلینا ورنیک[2]

باور عمومی: هر فرد و در هر کجا می‌تواند مبتکر نوآوری باشد زیرا اینترنت دانش و ابزار بی‌سابقه‌ای را برای خلق نوآوری در اختیار ما قرار داده است. هسته نوآوری از شرکت‌ها به سمت مردم تغییر خواهد کرد. به لطف اینترنت دسترسی به دانش مرتبط با نوآوری‌ها و ساختار شکل دادن آنها در جهان به‌طور برابر در حال گسترش است.

اصل موضوع: دانش، اطلاعات و داده‌های مربوط به ایجاد فعالیت‌های نوآورانه به‌دلیل عدم ایجاد انگیزه برای به‌اشتراک‌گذاری آنها، وجود محدودیت‌های قانونی یا ترکیبی از هر دو مورد، همیشه در دسترس نیستند. این منابع ممکن است پشت یک ساختار آبونمان (اشتراک با بار مالی) به‌عنوان داده‌های شخصی یا داده‌ای با حقوق مالکیت معنوی پنهان شده باشد. همه مبتکران تمایلی به اشتراک گذاشتن نوآوری‌های خود به‌صورت برخط ندارند، زیرا این روش می‌تواند مدل تجاری آنها را تضعیف کند. نوآوری‌هایی که ریسک‌پذیر هستند و به سرمایه‌گذاری زیادی در تحقیقات و توسعه نیاز دارند، معمولاً جهت اجرا شدن نیاز به محیط شرکت‌های تجاری دارند تا فضای برخط. هرچند حقوق مرتبط با IP مانند حق ثبت اختراع با محافظت از مبتکران در برابر استفاده سودجویانه رایگان، این‌گونه فعالیت‌های نوآورانه را مورد حمایت قرار می‌دهد. بااین‌حال، آنها استفاده و بهره‌مندی مجدد از چنین نوآوری‌هایی را به‌صورت برخط محدود می‌کنند.

باوجوداین، افراد و اجتماعی از مبتکران وجود دارند که به‌طور فعال به‌صورت برخط نوآوری ایجاد می‌کنند و آن را با دیگران به اشتراک می‌گذارند. یک مثال قابل تأمل توسعه «نرم‌افزار منبع باز»[3] است، که در آن از حقوق IP استفاده می‌شود تا بتواند توسعه نرم‌افزار مشترک را ممکن نماید

1. **Source:** Carliss Baldwin and Eric Von Hippel, Modeling a paradigm shift: From producer innovation to user and open collaborative innovation, Organization Science 22 (2011), 1399-1417; Fabian Stephany, Fabian Braesemann and Mark Graham, Coding Together - Coding Alone: The Role of Trust in Collaborative Programming, SocArxiv (2019) https://osf.io/preprints/socarxiv/8rf2h/download .
2. Alina Wernick
3.Open Source Software

(ارجاع به اسطوره ۹). در واقع، اینترنت امکان دسترسی دموکراتیک و ایجاد نوآوری را در قالب برخی ماژول‌ها فراهم می‌کند؛ به‌خصوص هنگامی که همکاری بین نوآوران در کالبدی غیر از رقابت مهیا می‌شود، توسعه مشارکتی کیفیت نوآوری را ارتقا می‌بخشد، و آنجا است که خود نوآوری نیز می‌تواند به‌صورت دیجیتال اجرا و ارائه شود (بالدوین و فون هیپل، ۲۰۱۱)[1]. بااین‌حال، در دسترس بودن اتصال به اینترنت برای تقویت فعالیت نوآوری برخط کافی نیست. سطح اعتماد موجود در جامعه بر شدت تعامل در توسعه نرم‌افزار منبع باز تأثیر می‌گذارد و تفاوت‌های موجود در همکاری‌های سازنده برخط را بین شهرها با شرایط فناورانه و سطح رفاه مشابه به وضوح توضیح می‌دهد (استفانی و همکاران ۲۰۱۹)[2].

در نهایت، اینترنت نیز تنها یک رسانهٔ محدود برای انتشار نوآوری‌ها است که می‌تواند شکل ملموس به خود بگیرد. بنابراین ممکن است بتوان طراحی یک شیء نوآورانه را در اینترنت به اشتراک گذاشت، اما خود آن شیء بالاخره باید به‌صورت فیزیکی تولید شود. در نتیجه، در بسیاری از مواقع این تولید انبوه است که معیارهای اقتصادی را تحت کنترل می‌گیرد و مؤثرترین وسیله برای دموکراتیک کردن دسترسی به محصولات نوآورانه محسوب می‌شود (بالدوین و فون هیپل، ۲۰۱۱). باوجود این‌که فناوری چاپ سه‌بعدی، امکان تولید-تقاضا-محور[3] طرح‌های آپلود شده در اینترنت را میسر می‌کند، تنوع طرح‌های موجود و پیچیدگی محصولاتی که می‌توانند بر اساس این طرح‌ها به‌صورت سه‌بعدی چاپ و تولید شوند، بسیار محدود است.

حقیقت: اینترنت بروز نوآوری‌های قابل اجرا و پیاده‌سازی دیجیتالی طرح‌های متنوع، مانند نرم‌افزار منبع باز، را تسهیل می‌کند. باوجوداین، ساختارهای تشویقی و همچنین عوامل حقوقی و اجتماعی، مشارکت «همه» را در جوامع نوآورانه و در پس آن به‌اشتراک‌گذاری نوآوری به‌صورت برخط را به‌شدت محدود می‌کنند. بنابراین، اکثر نوآوری‌های ملموس، با ریسک‌پذیری بالا، یا با بار مالی سنگین همچنان نیازمند ساختارهای مشخص حمایت مالی و حقوقی است که در نتیجه تنها از طریق مجاری موجود شرکت‌ها/کمپانی‌ها، و نه اینترنت، به ثمر خواهند نشست.

1. Baldwin and von Hippel , 2011
2. Stephany et at 2019
3. On-Demand Manufacturing

اسطوره چهل‌ویکم: بر تأثیرات شبکه نمی‌توان چیره شد[1]

پل بلفلیم[2]

باور عمومی: آثار مثبت شبکه هنگامی تجلی و بروز می‌یابد که ارزش یک راهکار[3] (محصول، خدمات، پلتفرم) با افزایش تعداد کاربرانی که آن را به‌کار می‌بندند ارتقا پیدا می‌کند. همان‌طور که اقتباس زودهنگام راهکار، مسیر اقتباس‌های بعدی را هم تسهیل می‌کند، راهکاری که بتواند از گزینه‌های جایگزین خود پیشی بگیرد، در نهایت، و به‌صورت برگشت‌ناپذیری، غالب خواهد شد.

اصل موضوع: آثار شبکه هنگامی بروز می‌نماید که کاربران در لحظه اتخاذ تصمیم؛ به تصمیمات، حضور و مشارکت سایر کاربران نیز اهمیت دهند. اگر کاربران به یک گروه منحصربه‌فرد[4] تعلق داشته باشند، تأثیرات شبکه «مستقیم» خواهد بود، زیرا استفاده بیشتر از گروه مستقیماً روی هر یک از اعضای گروه تأثیر می‌گذارد (به‌عنوان‌مثال می‌توان به دستگاه‌های ارتباطی اشاره نمود). تأثیرات شبکه همچنین می‌تواند در بین کاربران گروه‌های خاص[5] نیز ایجاد شود، همان‌طور که این مهم راجع به بسیاری از پلتفرم‌های دیجیتالی نیز صادق است(Airbnb با داشتن میزبان‌های بیشتر امکانات جذاب‌تری به کاربران ارائه می‌دهد). در اینجا، تأثیرات شبکه غیرمستقیم است: یک کاربر اضافی نه به‌طورمستقیم بلکه با افزایش مشارکت در گروه دیگر، سایر کاربران گروه خود را تحت تأثیر قرار می‌دهد.

در صورت وجود تأثیرات مثبت شبکه (مستقیم یا غیرمستقیم)، استفاده بیشتر باعث افزایش ارزش آن شبکه می‌شود که به‌خودی‌خود باعث ترغیب سایر کاربران به استفاده هرچه بیشتر از آن می‌شود. این فرایند خود-تقویتی[6]، منجر به این می‌شود که شبکه بَرنده تمامی موقعیت‌ها و فرصت‌ها را از آن خود کند (یک راهکار-در اینجا شبکه- بی‌نظیر در نهایت بیشترین تعداد کاربر- اگرچه نه همه کاربران- را به خود جذب می‌کند)؛ و به‌دنبال آن نوعی از «قفل شدگی»[7] برای کاربر

1. **Source:** Paul Belleflamme and Martin Peitz, Platform and Network Effects, in Luis C. Corchon and Marco A. Marini (eds), Handbook of Game Theory and Industrial Organization (Cheltenham: Edward Elgar, 2018), https://ssrn.com/abstract=2894906; Andrei Hagiu and Simon Rothman, Network Effects Aren't Enough, Harvard Business Review (April 2016), https://hbr.org/2016/04/network-effects-arent-enough.

2. Paul Belleflamme
3. Value of Solution
4. Unique Group
5. Distinct Groups
6. Self-Reinforcing Process
7. Lock-in

تداعی می‌شود (کاربران حاضر نیستند آن راهکار را ترک کنند و به سوی راهکار دیگری-راهکار جایگزین- تغییر مسیر دهند، مگر این‌که در یک شرایط خاص همه کاربران با یکدیگر به سوی راهکار جایگزین شیفت کنند). باوجوداین، ممکن است تعدادی از نیروهای رقیب باعث تضعیف قدرت فزاینده آثار مثبت شبکه شوند. اول، تأثیرات شبکه به‌ندرت در همه موارد مثبت است: این تأثیرات ممکن است برای گروه‌های کوچکی از کاربران (مانند دوستانی که از پیش در رسانه‌ای اجتماعی حاضر بوده‌اند) محدود شده باشد؛ یا درحالت دیگر، این تأثیرات برای برخی از گروه‌ها منفی باشند (مانند فروشندگان رقیب در یک پلتفرم تجاری) یا در زمانی خاص تبدیل به اثری منفی شود (آن هم به‌دلیل تراکم شدید زیرساخت شبکه). دوم، برخی مواقع تمایز می‌تواند نقشی شدیداً منفی علیه آثار شبکه داشته باشد: ممکن است چندین راهکار به‌طور هم‌زمان وجود داشته باشند چراکه هر یک از آنها پاسخگوی یک نیاز خاص و متفاوت کاربران هستند (مانند کنسول‌های بازی رقیب موجود). همچنین، یک راهکار جدید و بهبودیافته ممکن است باعث سرنگونی و حذف یک راهکار غالب شود، زیرا در جهت غلبه بر حس قفل‌شدگی که پیش‌تر به آن پرداخته شد، راهکار جدید ویژگی‌های ارزشمند بسیار زیادی در اختیار کاربران قرار دهد (برای‌مثال حذف مای اسپیس[1] توسط فیس‌بوک را تصور نمایید).

بنابراین، حتی اگر ایده «برنده تمام عیار» تحقق یافته باشد (به‌عنوان‌مثال سهم ۹۵ درصدی موتور جستجوی گوگل در بازار اروپا)، نمی‌توان آن را صرفاً به خاطر تأثیرات مثبت شبکه دانست: ساختارهای اقتصادی (همچون ضوابط مربوط به عرضه) نیز به ظهور و موفقیت آنها کمک می‌کند، ضمن آنکه رفتارهای ضدرقابتی نیز ممکن است در تداوم و پایداری آنها نقش داشته باشند.

حقیقت: تأثیرات مثبت شبکه، فرایندهای خود-تقویتی را ایجاد می‌کند که ممکن است منجر به این شود که یک شبکه بتواند بَرنده تمام موقعیت‌ها و فرصت‌ها شود. باوجوداین، جریان‌های متضاد و رقابتی نیز وجود دارند که باعث می‌شود راهکارهای متنوع به‌طورهم‌زمان حضور و فعالیت داشته باشند و گاهی راه‌حل‌های بهبودیافته جایگزین راه‌حل‌های غالب شوند.

1. MySpace

فصل پنجم
داده و آشفتگی در آن

اسطوره چهل‌ودوم: الگوریتم‌ها همواره بی‌طرف هستند[1]

ماتیاس اسپیلکامپ[2]

باور عمومی: از آنجاکه یک الگوریتم چیزی جز مجموعه دستورالعمل هایی که بر «داده‌ها» اعمال می‌شود نیست- که معمولاً به‌صورت اعداد ظاهر می‌شوند- بنابراین نمی‌تواند جهت‌دار یا دارای سوگیری باشد به‌نحوی که نتیجه یا خروجی فرایند استفاده از این الگوریتم‌ها را تحت تأثیر قرار بدهد.

اصل موضوع: الگوریتم‌ها به مثابه سازوکارهای تصمیم گیری الگوریتمی، ساخته دست انسان هستند؛ از مدیریت شبکه گرفته که اشکال به‌خصوصی از محتوا را در مقایسه با دیگر محتواها ترجیح و در اولویت قرار می‌دهد (نقض بی‌طرفی شبکه)، تا «هوش مصنوعی» که قرار است به شکل خودکار نفرت‌پراکنی، اطلاعات نادرست یا تبلیغات تروریستی را از روزنامه‌نگاری، پارودی[3] و سایر اشکال محتوای مجاز تشخیص دهد (ارجاع به اسطوره ۱۸ و ۴۳). همه این سیستم‌ها از قضاوت‌های ارزشی برای رسیدن به نتایج خوداستفاده می‌کنند: یک الگوریتم برای انجام وظیفه

1. **Source:** Aylin Caliskan Islam, Joanna J. Bryson, Arvind Narayanan: Semantics derived automatically from language corpora necessarily contain human biases, Computing Research Repository (2017), https:// arxiv.org/abs/1608.07187; Alex Salkever, Vivek Wadhwa: A.I. Bias Isn't the Problem. Our Society Is (2019), https://fortune.com/2019/04/14/ai-artificial-intelligence-bias.

2. Matthias Spielkamp

3. Parody

خود، می‌بایست «بداند» با چه بسته داده‌ای در مقایسه با دیگر داده‌ها متفاوت عمل کند و این‌که براساس چه معیار یا تعریفی اقدام به اولویت‌بندی بنماید. فارغ از این پرسش که آیا الگوریتم‌ها در نهایت قادر به ارزیابی صحیح محتوا خواهند بود یا خیر (که پاسخ آن منفی است)، بدیهی است که چنین معیار/تعاریفی همیشه توسط انسان‌ها با اهداف و نیات خاصی تدوین می‌شوند.

ما این معیارها/تعاریف را به‌عنوان تعاریف بی‌طرف تلقی نمی‌کنیم، همچنین الگوریتمی که براساس آنها عمل کند نیز بی‌طرف طبقه‌بندی نخواهد شد.

یک خوانش خوش‌بینانه از این باور عمومی این است که الگوریتم‌ها به‌طور یکسان یک نوع از مجموعه دستورالعمل‌ها را بر همه داده‌هااعمال می‌نمایند؛ و بنابراین کارکرد آنها اساساً بی‌طرفانه هستند، و هیچ هدف و یا انگاشتهٔ خاصی از جانب خود ندارند. این نکته صحیح است، اما بدیهی است نکته اصلی نیست.

باتوجه‌به آنچه «تکنیک‌های یادگیری ماشینی»[1] نامیده می‌شود، یک بُعد دیگر قضیه برجسته می‌شود. وقتی الگوریتم‌ها با انبوهی از «مجموعه داده‌ها»[2] برای شناسایی الگوها یا اولویت‌بندی‌ها تغذیه و آموزش داده می‌شوند (به اصطلاح «داده‌های آموزشی»)، باید پذیرفت که این «مجموعه داده‌ها» معمولاً حاوی سوگیری‌ها و جهت‌گیری‌های ذاتی جامعه بشری هستند. اگر یک «سیستم یادگیری خودکار»[3] بر اساس داده‌های جهت‌دار نتیجه‌گیری کند، این نتیجه‌گیری‌ها نیز به‌طورکلی جهت‌دار خواهند بود، و بنابراین نمی‌توانند بی‌طرف باشند.

حقیقت: الگوریتم‌ها یا به‌طورمستقیم توسط انسان طراحی شده‌اند یا در صورت خودکار بودن، منطق خود را بر اساس فرایندهای کنترل شده و طراحی شده توسط انسان توسعه می‌دهند. آنها نه «عینی» هستند و نه «خنثی»؛ بلکه محصول مباحثات انسانی و جنگ قدرت می‌باشند.

1. Machine-Learning Techniques
2. Data Sets
3. Self-Learning System

اسطوره چهل‌وسوم: هوش مصنوعی چاره مشکل است[1]

کریستین کتزنباخ[2]

باور عمومی: «هوش مصنوعی[3]» را می‌توان به‌عنوان یکی از دستاوردهای اساسی فناورانه زمان ما دانست. هوش مصنوعی نه‌تنها نحوه زندگی، برقراری ارتباط، کار و سفر در آینده‌ای نزدیک را تغییر خواهد داد، بلکه راه‌حل‌های مبتنی‌بر هوش مصنوعی مشکلات اساسی جوامع ما از تشخیص بیماری‌ها و اطلاعات نادرست گرفته تا نفرت‌پراکنی کلامی و پویایی شهری را مرتفع خواهد کرد.

اصل موضوع: غوغای اخیر درباره هوش مصنوعی با این افسانه ارتباط دارد که هوش مصنوعی به‌خودی‌خود مشکلات اصلی جوامع ما را برطرف خواهد کرد. در جلسات استماع کنگره ایالات متحده آمریکا در سال ۲۰۱۸، مارک زاکربرگ، مدیر عامل فیس‌بوک، از عباراتی مانند «هوش مصنوعی چاره مشکل است» و «در آینده ما فناوری‌ای خواهیم داشت که به این موضوعات رسیدگی کند» بیش از ده‌ها بار در پاسخ به اتهامات سوءاستفاده از اطلاعات، عدم نظارت بر نفرت‌پراکنی کلامی و نقض حریم خصوصی استفاده نمود. در بخش‌های دیگر، مشاغل و فناوری‌ها بر این باورند که فناوری‌ها و محصولات مبتنی‌بر هوش مصنوعی می‌توانند سرطان را در مراحل اولیه تشخیص دهند، الگوهای کلاهبرداری مالیاتی را ردیابی کنند، وسایل نقلیه را به‌طور مؤثر در مناطق شهری راهنمایی کنند و همچنین رفتارهای ضداجتماعی و جنایتکارانه را در فضاهای عمومی شناسایی نمایند.

این روایت که فناوری مشکلات اجتماعی را برطرف خواهد کرد درواقع موضوعی تکراری در تاریخ ظهور و رشد فناوری و جامعه است. «تدبیر فناورانه» (رادی وُلتی)[4] به‌دنبال ایجاد و ارائه راه‌حل‌های کاربردی برای مشکلات اجتماعی و سیاسی است: وسایل نقلیه خودران ممکن است با امنیت بیشتری در سطح شهر (طبق برخی معیارها) تردد کنند، اما پویایی شهری را برای

1. **Source:** Evgeny Morozov, To save everything, click here: The folly of technological solutionism (New York: PublicAffairs, 2013); Julia Powles and Helen Nissenbaum, The Seductive Diversion of 'Solving' Bias in Artificial Intelligence, Medium, 8 December 2018, https://medium.com/s/story/the-seductive-diversionof-solving-bias-in-artificial-intelligence-890df5e5ef53.
2. Christian Katzenbach 3. AI 4. Rudi Volti

بخش‌های وسیعی از جمعیت فراهم نمی‌کند. نرم‌افزارهای فیلترینگ ممکن است با شناسایی اطلاعات غلط و نفرت‌پراکنی کلامی بهبود یابند، اما این بهبود باعث ریشه‌کن کردن موارد فوق نمی‌شود و بنابراین قادر به ایجاد تعادل کامل (و به‌طور گسترده پذیرفته شده) میان آزادی بیان و نظارت بر گفتار مضر نخواهد بود. این مشکلات، اساساً ساختاری اجتماعی دارند، و بنابراین تنها یک جواب درست و صحیح که بتواند از لحاظ فناوری عملی باشد وجود ندارد.

این روایت که «هوش مصنوعی چاره مشکلات» است نیز به‌خودی‌خود گمراه کننده است چراکه باعث منحرف نمودن توجه از عامل انسانی و روابط اجتماعی به‌عنوان زیربنای اصلی هوش مصنوعی می‌شود. محصولات مبتنی‌بر هوش مصنوعی به‌خودی‌خود به وجود نمی‌آیند، بلکه محصولاتی ساخته دست بشر هستند (ارجاع به اسطوره ۱۸ و ۴۲). دستگاه‌ها و خدمات معمول مبتنی‌بر هوش مصنوعی مانند وسایل نقلیه خودران و ابزارهای تشخیص تصویر را می‌بایست محصولات شرکت‌هایی با علایق تجاری و مفروضات هنجاری دانست؛ بنابراین مشاهده این‌گونه علایق تجاری در محصولات موجود در بازار به آسانی قابل تشخیص است. علاوه‌براین، محصولات هوش مصنوعی ماحصل میزان توجه‌پذیری از کار انسانی است، از مدل‌های پیچیده ریاضی گرفته تا فعالیت‌های روزمره مانند روش‌های آموزش هوش مصنوعی به تشخیص تصویر در تصویر.

در نتیجه، حتی اگر خدمات و دستگاه‌های دارای هوش مصنوعی در آینده عملکرد کاملاً قابل قبول و مطابق با معیارهای از پیش تعیین شده داشته باشند، جمله «هوش مصنوعی چاره مشکلات است» همچنان به‌عنوان ساختاری کاملاً گمراه کننده باقی خواهد ماند. بسیاری از این مشکلات اساساً اجتماعی هستند و راه‌حل عملی فناورانه برای آنها وجود ندارد. فناوری هوش مصنوعی یک عامل خودمختار نیست بلکه ماحصل تعامل انسان و جامعه است.

حقیقت: درحالی‌که هوش مصنوعی نمی‌تواند همه چیز را اصلاح کند، ممکن است انسان‌هایی که از هوش مصنوعی استفاده می‌کنند، بعضی از مشکلات را مرتفع نمایند. تحولات سریع در حوزه فناوری‌های هوش مصنوعی فرصتی را برای بسیاری از ذی‌نفعان فراهم می‌کند تا دربرابر چالش‌های اجتماعی پاسخگو باشند. این فناوری‌ها به نوآوری در بسیاری از بخش‌های

اجتماعی کمک می‌کنند و درنتیجه شیوهٔ زندگی، برقراری ارتباط، کار و مسافرت را تغییر می‌دهند- البته نه به‌طورخودکار در جهت منافع عمومی.

اسطوره چهل‌وچهارم: آینده هوش مصنوعی در دست شرکت‌ها قرار دارد[1]

فیلیپه لورنز و کیت ساسلو[2]

باور عمومی: دولت‌ها به‌خودی‌خود قادر به تقویت پایه نوآوری هوش مصنوعی نیستند. شرکت‌های خصوصی منابع ملی هوش مصنوعی را خریداری می‌کنند. دولت‌ها قادر به تدوین برنامه‌های میان‌مدت و بلندمدت در مورد رویکردهای قوی ملی به هوش مصنوعی نیستند، زیرا سیاست‌گذاران از درک کامل هوش مصنوعی و کاربرد آن ناتوان هستند.

اصل موضوع: فناوری هوش مصنوعی با فناوری‌های نوظهور قبلی متفاوت است زیرا امروزه شرکت‌های بخش خصوصی مبتکر فناوری‌های هوش مصنوعی هستند. با این‌حال دولت‌ها هنوز هم می‌توانند در ایجاد اکوسیستم‌های هوش مصنوعی که در آن شرکت‌های نوآورانه رشد می‌کنند تأثیرگذار باشند. این امر مستلزم تأمین منابع لازم برای شرکت‌ها و دانشگاه‌ها برای تولید فناوری‌های پیشرفتهٔ هوش مصنوعی است. بازیگران بخش خصوصی و بازیگران دولتی صرفاً نقش‌های مختلفی را دنبال می‌کنند.

هوش مصنوعی جادویی نیست: ورودی‌های لازم صنعتی برای تولید فناوری یادگیری ماشین[3] عبارت‌اند از داده، نرم‌افزار، سخت‌افزار و استعداد (ارجاع به اسطوره ۴۳). درک یادگیری ماشینی به‌عنوان ترکیبی از این ورودی‌ها به سیاست‌گذاران این امکان را می‌دهد تا اهمیت اقتصادی آن را درک کنند و اهمیت بازیگرانی را که این فناوری را تولید می‌نمایند، بشناسند. اما گفتمان پیرامون

1. Source: Philippe Lorenz and Kate Saslow, Demystifying AI & AI Companies. What foreign policy makers need to know about the global AI industry (July 2019), Stiftung Neue Verantwortung, https://www.stiftung-nv. de/sites/default/files/demystifying_ai_and_ai_companies.pdf.
2. Philippe Lorenz and Kate Saslow
3. ML (Machine Learning)

هوش مصنوعی در سیاست امروز همچنان متناقض و مبهم است. بنابراین درک عمیق‌تر راجع به هوش مصنوعی امری ضروری است. این امر باعث بهبود مباحث در سیاست خارجی نیز می‌شود و بنابراین زمینه را برای نظارت بهتر بر روندهای جهانی فراهم می‌کند؛ و به‌طور هم‌زمان بر سیاست‌گذاری داخلی نیز اثر می‌گذارد. در حوزه هوش مصنوعی، شرکت‌ها/کمپانی‌ها دارای اهمیت هستند، زیرا نوآوری در مورد یادگیری ماشینی به‌طور قابل ملاحظه‌ای توسط نهادهای بخش خصوصی تأمین می‌شود. شرکت‌ها تلاش‌های تحقیق و توسعه خود را متمرکز بر ایجاد محصولات خاص یادگیری ماشینی نموده، و جریان درآمد خود را بر اساس توسعه برنامه‌های کاربردی با محوریت یادگیری ماشینی بنا کرده‌اند. از این‌گونه شرکت‌ها می‌توان به‌عنوان «شرکت‌های هوش مصنوعی» واقعی یاد نمود که پیشرفت فناوری‌های هوش مصنوعی و استفاده بهینه از آن را اصل اساسی خود قرار داده‌اند. اما این بدان معنا نیست که دولت‌ها نقشی در این زمینه ندارند: به‌طورمثال کارشناسان سیاست خارجی(دیپلمات‌ها) کانال‌هایی برای جمع‌آوری اطلاعات مربوط به هوش مصنوعی و تجزیه و تحلیل ابعاد سیاسی و اقتصادی آنها متناسب با تخصص‌های منطقه‌ای هستند و می‌توانند نتایج این تحلیل‌ها و اطلاعات را به دولت متبوع خود ارسال نمایند. فناوری توسعه و استقرار هوش مصنوعی با سرعت زیادی در حال انجام بوده و از اهمیت اقتصادی توجه‌پذیری نیز برخوردار است. اما منابع برای نظارت فعالانه بر پیشرفت‌های جهانی آن در حال حاضر محدود هستند. بااین حال، سیاست‌گذاران در سراسر جهان متوجه اهمیت زیاد هوش مصنوعی شده و بنابراین شاهد حضور فزاینده دولت‌ها در این گفتمان هستیم. این اشتیاق برای حضور در قالب اجتماعات و ابتکارات بی‌شمار بین‌المللی با محوریت حاکمیت هوش مصنوعی قابل مشاهده است.

اما این تحرکات و ابتکارات همچنان کارایی و اثر ندارند؛ و ازسویی‌دیگر، دولت‌ها نیز همچنان فاقد یک سیاست منسجم و مشترک برای تحلیل و نظارت بر تحولات جهانی در رابطه با هوش مصنوعی هستند. استفاده از شبکه بین‌المللی سفارتخانه‌ها و قدرت خدمات خارجی-اطلاعات و تحلیل‌های جمع‌آوری شده- آنها می‌تواند کمک مؤثری به دولت‌ها در شکل دادن به سیاست خارجی و داخلی آنها در زمینه هوش مصنوعی بنماید. همچنین می‌تواند در راستای افزایش

آگاهی و ظرفیت‌سازی برای سیاست‌گذاری جامع‌تر و مؤثرتر برای «حکمرانی هوش مصنوعی»[1] مفید واقع شود. بنابراین کشورها با فراهم کردن اکوسیستم مساعد برای نوآوری هوش مصنوعی و ردیابی تحولات راهبردی در نوآوری هوش مصنوعی در سطح جهان، نقش مهمی ایفا می‌کنند.

حقیقت: دولت‌ها همچنان نقش اساسی در حکمرانی هوش مصنوعی دارند. اما آنها برای مدیریت بهتر هوش مصنوعی باید خیلی فعالانه‌تر عمل کنند. سیاست‌گذاران امروزه باید بدانند که دولت‌ها چگونه می‌توانند بر داده‌های ورودی «فناوری‌های یادگیری ماشینی»[2] (داده‌ها، نرم‌افزارها، سخت‌افزارها و استعدادها) اثر بگذارند و به دولت‌های متبوع خود چشم‌انداز روشنی در زمینه دفاع و تقویت توسعه راهبردی اکوسیستم‌های هوش مصنوعی ارائه دهند.

اسطوره چهل‌وپنجم: حریم خصوصی به‌کلی از بین رفته است[3]

پائولا هلم و توبیاس داینلین، یوهانس آیزنهاوفر و کاترینا برونلیچ[4]

باور عمومی: حریم خصوصی به‌کلی از بین رفته است. حریم خصوصی قربانی پدیده‌های اجتماعی-فنی جدید از جمله نظارت جمعی بی‌هدف، فروپاشی بافت‌ها و ساختارها، تلفن‌های هوشمند، فناوری‌های پوشیدنی[5]، رسانه‌های اجتماعی و اینترنت اشیا شده است. حال آنکه مردم اهمیتی به این موضوع نمی‌دهند: آنها از خدماتی استفاده می‌کنند که برای جمع‌آوری داده‌ها برنامه‌ریزی شده‌اند، حجم زیادی از اطلاعات را بدون تأمل به اشتراک می‌گذارند، و از فاش شدن کامل این اطلاعات ابایی ندارند.

---

1. AI Governance
2. Machine Learning Technologies
3. **Source:** Paula Helm, Johannes Eichenhofer, Reflektionen zu einem social turn in den privacy studies. In Martin Hennig et al.: Digitalität und Privatheit (Bielefeld: Transcript, 2019), 139-165; Tobias Dienlin, Miriam Metzger, An extended privacy calculus model for SNSs—Analyzing self-disclosure and self-withdrawal in a representative U.S. sample, Journal of Computer-Mediated Communication, 21 (2016), 368–383, https://doi.org/10.1111/jcc4.12163.
4. Paula Helm with Tobias Dienlin, Johannes Eichenhofer and Katharina Bräunlich
5. Wearables (دستگاه‌های کوچکی که می‌توانید بپوشید یا روی بدن خود قرار دهید)

اصل موضوع: فقدان کامل حریم خصوصی نه‌تنها یک بار، بلکه بارهاوبارها اعلام شده است. در سال ۱۸۷۴، روزنامه تایمز مطلبی با عنوان «لغو حریم خصوصی» چاپ کرد. در سال ۱۹۰۹، واشنگتن پست نوشت: «تنها یک مکان مخفی در جهان باقی مانده است که آن هم قطب جنوب است [...].» در سال ۱۹۹۹، اسکات مک نیلی[1] اظهار داشت «همین حالا هم حریم خصوصی ندارید- فراموشش کنید». در این مقالات -و بسیاری دیگر- به‌دنبال برخی تحولات گستردهٔ اجتماعی و فناورانه از قبیل اختراع دوربین عکاسی یا اینترنت، به نقض کامل حریم خصوصی اشاره شده است. باتوجه‌به این روند رو به افول و آخرین تحولات فناوری، آیا حریم خصوصی به‌کلی از بین رفته است؟

قطعاً این‌گونه نیست. موارد ذکر شده در درجه اول بیانگر یک چیز هستند: حریم خصوصی جاودانه است. در واقع، حریم خصوصی که به واسطه اینترنت، فناوری‌های کلان داده[2] و رواج تلفن‌های هوشمند و اینترنت اشیا مطرح شده است، در حال حاضر یک کالا محسوب می‌شود، به فروش می‌رسد، معامله می‌شود، بهره‌برداری می‌شود، مورد بی‌توجهی قرار گرفته و رها شده است. هرچند، مثل همیشه شدت و ضعف دارد. نقض حریم خصوصی هرگز به‌صورت‌کامل صورت نگرفته است. مردم همواره به‌دنبال روش‌هایی برای جداسازی خود از دیگران، نهادهای سیاسی و شرکت‌های بزرگ بوده‌اند چراکه آنها حفظ حریم شخصی را پیش شرط استقلال فردی، یکپارچگی روانی و توانایی در ایجاد روابط شخصی می‌دانند.

گفته می‌شود امروزه مردم داوطلبانه حریم شخصی خود را به خطر می‌اندازند-اما این حقیقت ندارد. بسیاری از مطالعات تجربی نشان داده‌اند که افراد در حقیقت در جهت حفظ حریم شخصی عمل می‌کنند–این امر در مورد رسانه‌های اجتماعی نیز صدق می‌کند. هرچه بیشتر نگران این موضوع باشند، اطلاعات کمتری به اشتراک می‌گذارند. باوجوداین، همواره بر سر دوراهی انتخاب بین ضرورت اشتراک‌گذاری وبرقراری ارتباط از یک‌طرف والزامات حفظ حریم خصوصی از طرف دیگر قرار می‌گیرند.

از دیدگاه اجتماعی، امروزه حریم خصوصی -احتمالاً بیش از هر زمان دیگری- به‌عنوان یک نیروی دموکراتیک نیز عمل می‌کند. در حقیقت هنگامی که حریم خصوصی از جانب جامعه و فعالان

1.Scott McNealy (of Sun Microsystems)

2. Big Data

سیاسی که برای دستیابی به استقلال ارتباطی تلاش می‌کنند، مطالبه می‌شود، به‌عنوان یک عمل مدنی به حساب می‌آید (ارجاع به اسطوره ۱۴). این عمل برای محافظت از یک فرهنگ دموکراتیک پویا که ممکن است شامل عقاید مختلفی باشد که در آن مورد بحث قرار می‌گیرند بسیار مهم است. در راستای حفظ چنین فرهنگی، پشتیبانی گسترده‌تری از جانب فناوری‌های تقویت‌کننده حریم خصوصی مورد نیاز است -برای‌مثال، مرورگرهای وب ناشناس مانند TOR- که در حال حاضر وجود دارند اما باید بهبود یافته و به‌عنوان نرم‌افزار پیش‌فرض تعیین شوند (ارجاع به اسطوره ۱۷).

حقیقت: در برخی مناطق و خصوصاً برای افراد محروم، حریم خصوصی امری بسیار ضروری و نگران‌کننده می‌باشد. حریم خصوصی نباید به موضوعی تجملی تبدیل شود. به‌دنبال واکنش‌های صورت گرفته به این موضوع، در حال حاضر حریم خصوصی توجه زیادی را به خود جلب کرده است. در زندگی روزمره و در جامعه دانشگاهی، حریم خصوصی در حقیقت به‌عنوان یک عمل اجتماعی و ارزش سیاسی حیاتی دوباره یافته است.

اسطوره چهل‌وششم: اینترنت هرگز فراموش نمی‌کند[1]

استفان دریِر[2]

باور عمومی: هر آنچه در فضای برخط نوشته شده، بارگذاری شده یا به اشتراک گذاشته می‌شود، برای همیشه آنجا خواهد ماند. تصاویر خاطره‌انگیز مهمانی‌های دوستانه ممکن است شانس شما را برای به‌دست آوردن یک شغل مناسب به خطر بیندازد. اینترنت بایگانی غول‌پیکری است که حقایق و دروغ‌ها را برای همیشه حفظ می‌کند و عواقب آن در سراسر زندگی دامن گیرمان خواهد شد.

1. **Source:** Andrew Neville, Is it a Human Right to be Forgotten? Conceptualizing the World View, Santa Clara J. Int'l L. 15 (2017) 157, https://digitalcommons.law.scu.edu/scujil/vol15/iss2/2; Shawn Walker and Sheetal Agarwal, The missing link: a preliminary typology for understanding link decay in social media, IConference Proceedings 2016, http://hdl.handle.net/2142/89413.
2. Stephan Dreyer

اصل موضوع: به‌دلیل ساختار کم‌وبیش غیرمتمرکز اینترنت، هزینه‌های جانبی نسخه‌برداری دیجیتال و به کمک میلیون‌ها میلیون کاربر و دستگاه‌های ذخیره‌سازی محلی، بسیاری از محتواها مدت طولانی‌تری در اینترنت و در نتیجه در خاطره ما باقی می‌مانند. موتورهای جستجوی عمومی و تخصصی به ما این امکان را می‌دهند تا به اطلاعات زیادی از زمان‌های دور دست پیدا کنیم. تمام حوزه‌های تجاری متحول شده به‌طوری‌که حتی خدماتی همچون «مدیریت شهرت برخط[1]» نیز ارائه می‌شوند.

آنچه به اصطلاح اثر «استرایسند»[2] نامیده می‌شود، احتمالاً مشهورترین معضل در این زمینه است: با تلاش فعالانه برای از بین بردن یک متن، تصویر یا ویدئوی به‌خصوص از اینترنت، توجه عمومی بیشتری به حذف محتوای مورد نظر جلب می‌شود و بنابراین، درواقع آن اطلاعات پررنگ‌تر نیز می‌شوند. به‌همین‌خاطر، حذف هرگونه اطلاعات اینترنتی که در مقطعی از زمان به‌طور گسترده‌ای مخاطب را به خود جلب کرده باشد، همیشه دشوار خواهد بود. اما این موارد بسیار خاص و -در مقایسه با میزان اطلاعات موجود در اینترنت- بسیار نادر هستند.

فرض غالب برای بخش اعظمی از محتوای برخط این است که دیر یا زود از بین خواهد رفت: تمام مطالعاتی که به بررسی قابلیت در دسترس بودن منابع برخط پرداخته‌اند، وجود تعداد زیادی «لینک/آدرس مرده[3]» را گزارش می‌دهند. از میان دیگر موارد، دلایل کمرنگ شدن یا تغییر یک منبع برخط عبارت‌اند از: از کار افتادن سرویس یا سرور، حذف دامنه سطح دوم[4] (اخیراً حتی حذف دامنه سطح بالا)، حذف یا به تعلیق درآمدن حساب کاربری، حذف یا جابه‌جایی محتوا، تغییر محتوا، خرابی کوتاه‌کننده پیوند یکتا، خرابی پیوندهای تغییر مسیر داده شده یا محتوای درون‌گذاری شده.

علاوه‌براین، رویکرد کاربران به خود افشایی[5] و به‌طورکلی حریم خصوصی در ۱۰ سال گذشته کاملاً دستخوش تحول شده است. این باور عمومی پیشاپیش سبب ایجاد پروفایل‌ها و حساب‌های کاربری محدودتر شده است، به‌عنوان‌مثال در شبکه‌های اجتماعی، مسدود ساختن

1. Online Reputation Management
2. Streisand Effect (تلاش برای متوقف کردن اطلاعات حتی می‌تواند توجه ناخواستهٔ بیشتری را جلب کند)
3. "URL rot" or "link rot"
4. Second Level Domain
5. Self-Disclosure

دسترسی عمومی به تصاویر مهمانی‌های دوستانه بسیار رایج است.

همچنین قوانین و مقرراتی وجود دارد که به همه افراد «حق فراموش‌شدگی» را می‌دهد که به واسطه آن قادر خواهند بود آن دسته از نتایج موتورهای جستجو که باعث نقض حقوق شخصی آنها می‌شوند را حذف کنند (ارجاع به اسطوره ۴۵). حق فراموش‌شدگی از طریق «قوانین عمومی حفاظت از اطلاعات[1]» با فراهم ساختن امکان درخواست حذف اطلاعات شخصی تحت کنترل دیگران، این رویکرد را حمایت و تأیید می‌کند.

هم از بین رفتن منابع و هم ابزارهای قانونی برای حذف یک محتوای به‌خصوص از اینترنت نشان می‌دهد که اینترنت خلاف تصور بسیاری از افراد بایگانی دائمی اطلاعات جهانی نمی‌باشد. در حقیقت، محتوای معمولی به هیچ وجه شرایط ایده‌آلی برای محافظت دیجیتال را ندارد-به نوعی ضرورتی برای حفاظت دیجیتال دائمی از آنها وجود ندارد.

حقیقت: بسیاری از فایل‌های اینترنتی عمر کوتاهی دارند و تخریب شدن سرویس‌ها و پیوندهای مرده به‌طور توجه‌پذیری به چشم می‌خورد. مقررات مربوط به حذف اطلاعات یا حذف نتایج به‌خصوص از موتورهای جستجو، چنین پدیده‌هایی (یعنی حذف اطلاعات و داده‌ها) را تقویت می‌کند. محتوای برخط معمولی و پیش‌پاافتاده ارزش بایگانی کردن طولانی‌مدت -و به خاطر سپردن- را ندارند.

اسطوره چهل‌وهفتم: قوانین «حافظت از اطلاعات» مرتبط با کنترل اطلاعات است[2]

مکسی میلیان وون گرافنشتاین[3]

باور عمومی: قوانین حفاظت از اطلاعات حول محور کنترل داده‌های شخصی عمل می‌کنند. عنوان این قانون «محافظت از اطلاعات» و همچنین جمله معروف هر فرد از «حق افشا

1. General Data Protection Regulation (GDPR)
2. **Source:** Maximilian von Grafenstein, The Principle of Purpose Limitation in Data Protection Laws: The RiskBased Approach, Principles, and Private Standards as Elements for Regulating Innovation (BadenBaden: Nomos, 2018).
3. Maximilian von Grafenstein

و به‌کارگیری اطلاعات (شخصی) خود برخوردار است» به‌خوبی بیانگر این مطلب هستند. این دیدگاه که پردازش هر نوع اطلاعات شخصی تنها با اعلام رضایت از جانب مالک آنها امکان‌پذیر است، نمونه بارز این قانون است.

اصل موضوع: این باور عمومی که افراد از حق کنترل اطلاعات شخصی «خود» (در مقابل ریسک ناشی از «پردازش اطلاعات»[1]) برخوردارند، برگرفته از یک درک کاملاً شهودی است: چنانچه من قادر به کنترل اطلاعات شخصی خود باشم، می‌توانم ریسک سوءاستفاده از آن اطلاعات را نیز کنترل نمایم. باوجوداین، هم در زندگی روزمره و هم آن‌طور که در نظریه‌ها انعکاس یافته، تمرکز روی داده‌ها به‌خودی‌خود به وضعیتی منجر می‌شود که مشکل واقعی، یعنی ریسک سوءاستفاده از آن، تحت نظارت و پایش قرار می‌گیرد. این امر به محافظت بیش از اندازه و ناکارآمد منجر می‌شود که در نوع خود غم‌انگیز است. دو نمونه زیر بیانگر این نکته است:

در قانون حفاظت از اطلاعات، رضایت شخصی اغلب به‌عنوان معیار هنجاری اصلی برای «خودمختاری فرد»[2] در دنیای دیجیتالی در نظر گرفته می‌شود. بااین‌حال، اکثر مردم نیز با این امر موافق هستند که رضایت، به شکل فعلی آن، در راستای این هدف قرار ندارد. در عمده موارد، به‌جای توانمندسازی افراد برای تصمیم گیری و این‌که خودمختار عمل کنند، عموماً تلاش می‌شود به طرق مختلف با کلیک کردن روی کلمه «موافقم» (بدون خواندن متن رضایت‌نامه) رضایت شخصی آنها دریافت شود. دلایل زیادی برای این به اصطلاح «رضایت دادن» از روی بی‌اعتنایی وجود دارد. هرچند، یکی از دلایل مهم آن عبارت‌است از آنکه افراد رضایت خود را دربرابر هرآنچه دیده می‌شود و نمی‌شود اعلام می‌کنند: همواره اعلام رضایت در همه جا لازم و ضروری است درحالی‌که پیامدهای رضایت دادن (یعنی خطرهای واقعی آن) کاملاً نامشخص و پوشیده باقی می‌ماند. حجم زیاد اطلاعاتی هم که براساس الزامات شفافیت در چارچوب‌های محافظت از اطلاعات در اختیار افراد قرار داده می‌شود، ارتباط تنگاتنگی با این پدیده دارد. غالباً، چنین اطلاعاتی روی داده‌های جمع‌آوری شده از افراد متمرکز است، درحالی‌که پیامدهای پردازش آنها مبهم باقی

1. Data Processing
2. Individual Self-Determination

می‌ماند. علاوه‌براین، حجم اطلاعات جمع‌آوری شده از افراد آن‌قدر زیاد است که شخص از موضوع اصلی غافل می‌شود و شانس این را پیدا نمی‌کند که از خودش این سؤال را بپرسد: چه نوع اطلاعاتی به من مرتبط است؟ بنابراین، تمرکز روی اطلاعات به‌جای ریسک ناشی از پردازش آن، کاربران عادی را منحرف و مفهوم‌پردازی در زمینه «محافظت» را از اصل آن دور می‌کند.

در مباحث اخیر، ممکن است این دیدگاه بر رویکردهای مترقی جدید با هدف حل ساختارمند این مشکل نیز اعمال شود. به نمونه‌هایی ازاین رویکردها دقت کنید: مراکز اطلاعات[1] می‌توانند حقوق حفاظت از اطلاعات را از جانب اشخاص اعمال کنند؛ حتی این‌که افراد باید به‌منظور بهره‌مندی بیشتر از داده‌ها (به‌عنوان‌مثال از طریق فروش آنها)، از حق مالکیت «اطلاعات شخصی» برخوردار باشند، تأثیرات بسیار گسترده‌تری دارد. تا زمانی که مشکل اصلی، یعنی، ریسک سوءاستفاده از داده‌ها رفع نشود، این رویکردهای جدید همچنان با شکست مواجه خواهند شد.

حقیقت: قانون حفاظت از اطلاعات ریسک ناشی از پردازش داده‌ها (نه داده‌های خام) را کنترل می‌کند. این تفاوت ممکن است ظریف به نظر برسد، اما تأثیرات گسترده‌ای در میزان دسترسی و محدودیت‌های محافظت از آن دارد. برای اجرای مؤثر قوانین محافظت از اطلاعات، مانند رضایت فردی و اقدامات شفافیت‌ساز، باید بر پیامدهای پردازش داده‌ها تمرکز کرد.

اسطوره چهل‌وهشتم: اطلاعات میل به رایگان بودن و آزادی دارد[2]

مارک پِری[3]

باور عمومی: ماهیت ذاتی اطلاعات، گرایش به انتشارآن است. این فرایند باید بدون هزینه

1. Data Fiduciaries
2. **Source:** Graham Greenleaf, An Endnote on Regulating Cyberspace: Architecture vs Law? 52 (1998) 21 (2) UNSW Law Journal, 593, http://www.austlii.edu.au/cgi-bin/viewdoc/au/journals/UNSWLawJl/1998/52. html?context=1;query=%22information%20wants%20to%20be%20free%22; Steven Levy, "Hackers" and "Information wants to be Free", Medium (2014), https://medium.com/backchannel/the-definitivestory-of-information-wants-to-be-free-a8d95427641c.
3. Mark Perry

و قابل دسترس باشد. دانشمندان معتبر به‌دنبال «دسترسی باز»[1] هستند و آن دسته از افرادی که مالکیت معنوی را مورد انتقاد قرار می‌دهند و از اطلاعات آزاد پشتیبانی می‌کنند، این فرضیه را بهانه‌ای برای عملیات هک کردن تلقی می‌کنند.

اصل موضوع: مطمئناً، خود اطلاعات میل به انجام کاری ندارند، تمام اینها به خواست و اراده مردم صورت می‌گیرد. از زمانی که افراد از در اختیار داشتن اطلاعات آگاهی پیدا کرده‌اند، از کاربرد آن مطلع بوده و گاهی آن را به‌عنوان یک دارایی با ارزش به دیگران داده‌اند (ارجاع به اسطوره ۹). اگرچه ساختارهای حقوقی به‌دلیل اعمال محدودیت در زندگی روزمره، از دارایی محسوب نمودن داده‌های خام امتناع می‌کنند، طی قرن‌های گذشته با روی کار آمدن مفاهیم حریم خصوصی، محافظت از پایگاه اطلاعاتی (اروپا)، حفاظت از اطلاعات و سازوکارهای مختلف دیگر، از قبیل قوانین اطلاعات محرمانه که به‌اشتراک‌گذاری آن را محدود می‌کنند، مفهوم باز بودن و آزادی مطرح شده در راستای به‌اشتراک‌گذاری اطلاعات، به تدریج از بین رفته است. به‌عنوان‌نمونه، آن دسته از اطلاعاتی که به‌منظور بررسی و نظارت بر یک محصول جدید توسط شرکت‌های دارویی ارائه می‌شود نیز تحت محافظت قرار می‌گیرد (ارجاع به اسطوره ۴۰). درطرف‌دیگر، و احتمالاً به‌عنوان یکی از ریشه‌های کلیشه «اطلاعات میل به رایگان بودن و آزادی دارد»، کاهش هزینه به‌اشتراک‌گذاری اطلاعات و فراهم آوردن امکان دسترسی گسترده از طریق اینترنت نیز مطرح بوده است. آنچه انتشار آن به سال‌ها زمان و هزینه زیادی نیاز داشت اکنون می‌تواند تنها با فشار دادن یک دکمه رایانه در دسترس نیمی از جهان قرار گیرد.

این تفکر که به اشتراک گذاشتن اطلاعات آسیبی برای فرد به همراه ندارد در تعدادی از پرونده‌های قضایی جرایم رایانه‌ای مطرح شده است، به‌گونه‌ای‌که در اکثر آن پرونده‌ها امکان پیگرد قانونی «سرقت» اطلاعات یا نقض قانون کپی‌رایت و جمع‌آوری داده وجود ندارد. این موارد به تغییراتی در قانون منجر شده است؛ از حمایت از پایگاه داده در اتحادیه اروپا گرفته تا تصویب گسترده قوانین ضدهک. در مورد دوم، یعنی قوانین ضدهک، ورود به سیستم‌ها به‌منظور

1. Open Access

دستیابی به اطلاعات، تغییر یا حذف آنها به‌صورت غیرقانونی جرم محسوب می‌شود. تا قبل از این، روند کار به این صورت بوده است که افرادی که امکان دسترسی به هر نوعی از اطلاعات برای آنها مسیر بوده، اجازه جمع‌آوری و سپس فروش آن اطلاعات را داشته‌اند. در این مواقع، اغلب برای جلوگیری از «فروش» داده‌ها، از طریق انعقاد قراردادهایی، محدودیت‌های به‌خصوصی برای «به اشتراک‌گذاری» اطلاعات اعمال می‌شده است، با این‌حال خود «داده‌ها» تحت پوشش قانون مالکیت معنوی قرار ندارند.

حقیقت: داده‌های مفید به‌ندرت آزاد هستند، چه به لحاظ هزینه و چه به لحاظ قابلیت دسترسی قانونی. اطلاعات با سرعت بی‌سابقه‌ای جمع‌آوری، تلفیق و تجزیه و تحلیل می‌شوند. بخش اعظمی از این عملیات توسط دولت‌ها و شرکت‌های صورت می‌گیرد که به کسب شهرت یا تأثیرگذاری بر رفتار اشخاصی مایل هستند که اطلاعات مربوط به آنها جمع‌آوری شده است. بنابراین، همان‌طور که کوری دکترو[1] بیان می‌کند، احتمالاً این افراد هستندکه می‌خواهند آزاد و قابل دسترس باشند.

اسطوره چهل‌ونهم: فناوری «نظیربه‌نظیر» یعنی اشتراک‌گذاری غیرقانونی اطلاعات [2]

فرانچسکو موسیانی[3]

باور عمومی: فناوری شبکه «نظیربه‌نظیر»[4] یک فناوری جذاب است که با ظهور اپلیکیشن‌های به‌اشتراک‌گذاری فایل مانند نپستر[5] یا وینمکس[6] به‌طور گسترده‌ای توسعه پیدا کرده است. این برنامه‌ها درواقع بیشتر برای به اشتراک گذاشتن موسیقی یا فایل‌های دارای حق

1. Cory Doctorow (فعال حامی حذف حق نسخه برداری)
2. **Source:** Malcolm Campbell-Verduyn (Ed.), Bitcoin and beyond: Cryptocurrencies, blockchains, and global governance. Routledge (2017), https://www.taylorfrancis.com/books/e/9781315211909; Francesca Musiani, "Giants, Dwarfs and Decentralized Alternatives to Internet-based Services: An Issue of Internet Governance", Westminster Papers in Communication and Culture, 10(1) (2015), 81–94, http://doi.org/10.16997/wpcc.214.
3. Francesca Musiani
4. Peer-to-Peer (P2P) 5. Napster 6. WinMX

چاپ استفاده می‌شوند. بنابراین فناوری نظیربه‌نظیر از ساختار و تفکر «دزدان دریایی» دیجیتالی و به‌اشتراک‌گذاری غیرقانونی فایل حمایت می‌کند.

اصل موضوع: اصطلاح «نظیربه‌نظیر» به شبکه‌ای از افراد برابر یا کاربران -افراد و ماشین‌ها- اطلاق می‌شود که با کمک سیستم‌های ارتباطی و تبادلات مناسب قادر به همکاری مستقل و بدون نیاز به هماهنگی مرکزی با یکدیگر هستند. باتوجه‌به موفقیت گستردهٔ اپلیکیشن‌های به‌اشتراک‌گذاری فایل نظیربه‌نظیر در اوایل دهه ۲۰۰۰، اعتقاد بر این است که این ساختار تبادل اطلاعات یک فناوری صمیمانه از جنس «سرقت» است که به‌طور انحصاری برای به‌اشتراک‌گذاری فایل‌های محافظت شده توسط قانون کپی‌رایت استفاده می‌شود. بااین‌حال، این فناوری شبکه فقط برای به‌اشتراک‌گذاری فایل استفاده نمی‌شود: مطمئناً فقط در مراحل اولیه، استفاده از ساختار مذکور محدود به این کاربرد شده بود که ساده‌ترین گزینه فنی است و برای اجرای آن به حداقل منابع انسانی و فنی نیاز دارد.

علاوه‌براین، ارتباط نظیربه‌نظیر همچنین برای برنامه‌های جایگزین و حقوقی که می‌تواند نیازهای بسیاری از کاربران/ مصرف‌کنندگان/ شهروندان در اینترنت امروز را تأمین کند نیز اعمال می‌شود. خدمات نظیربه‌نظیر خود را به‌عنوان گزینه‌های غیر متمرکز برای خدمات اساسی و ابزارهای اساسی زندگی روزمره شبکه امروز ما معرفی می‌کنند: از جمله موتورهای جستجو، شبکه‌های اجتماعی،سرویس‌های ذخیره برخط فایل، پخش ویدئو، محاسبات شبکه، پیام فوری و همکاری‌های گروهی تحت شبکه.

این ساختار نه‌تنها به‌دلیل تحولات گستردهٔ فناوری (بهبود کیفیت اتصالات اینترنت کاربران، میزان فضای دیسک موجود در هر رایانه) بلکه به‌دلیل افزایش آگاهی (چه توسط محققان و چه توسط عموم مردم) در زمینه ضرورت حفظ کثرت، تنوع و امکان نوآوری در اکوسیستم اینترنت امروزی می‌باشد.

به‌عنوان‌مثال در گوگل، فیس‌بوک یا دراپباکس[1] هر بار که کاربر جستجویی انجام می‌دهد،

1. Dropbox

یا شخصی پیام ارسال می‌کند یا آلبوم عکس را ذخیره می‌کند، داده‌ها قبل از رسیدن به گیرنده مورد نظر، در مجموعه‌ای از سرورها تحت عنوان محتوای «تجمیع» شده، ذخیره می‌شود. از طرف دیگر، با بهره‌گیری از ظرفیت غیرمتمرکز ارتباط نظیربه‌نظیر، سایر برنامه‌ها نیز با هدف برآورده کردن نیازهای مشابه از دید کاربر نهایی (که به ارسال درخواست‌های جستجو، به‌اشتراک‌گذاری پیام و ذخیرهٔ محتوای خود ادامه می‌دهد)، ولی بر اساس تکنیک‌های مختلف معماری و پیکربندی شبکه و نحوه ذخیره و گردش اطلاعات، به این ساختار ارتباطی نزدیک می‌شوند.

حقیقت: ساختار ارتباطی نظیربه‌نظیر با وجود تعریف عمومی از آن، به‌عنوان یک فناوری «سرقت اطلاعات» برای به اشتراک گذاشتن فایل‌های محافظت شده تحت قانون کپی رایت، توسط تعدادی دیگر از اپلیکیشن‌ها نیز استفاده می‌شود، از جمله تلاش برای ارائه گزینه‌های غیرمتمرکز و کاملاً قانونی برای موتورهای جستجوی مشابه گوگل و یا شبکه‌های اجتماعی مشابه فیس‌بوک. همچنین این روش ارتباطی (نظیربه‌نظیر) ساختار اصلی زنجیره بلوکی (بلاکچین) را تشکیل می‌دهد.

اسطوره پنجاهم: بلاکچین همه مشکلات ما را حل خواهد کرد[1]

مارتین فلورین[2]

باور عمومی: «بلاکچین»[3]، فناوری‌ای که از بیت‌کوین[4] و سایر ارزهای رمزنگاری شده پشتیبانی می‌کند، کاربردهای گسترده‌ای در همه زمینه‌های زندگی دارد. به‌دلیل کاربرد موفق بلاکچین در تحقق ارزهای دیجیتال، همچنین از آن می‌توان به‌عنوان عاملی مناسب برای «تمرکززدایی» طیف گسترده‌ای از اپلیکیشن‌ها و خدمات دیگر نیز استفاده کرد و بدین‌ترتیب

1. **Source:** Karl Wüst and Arthur Gervais, Do you need a Blockchain?, 1st Crypto Valley Conference on Blockchain Technology (2018), https://eprint.iacr.org/2017/375.pdf, http://doyouneedablockchain.com; Florian Tschorsch and Björn Scheuermann, Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies, IEEE Communications Surveys & Tutorials 18 (2016) 3, https://eprint.iacr.org/2015/464.pdf.
2. Martin Florian 3. Blockchain 4. Bitcoin

نیاز به واسطه‌ها و نیز صرف زمان برای اعتمادسازی را از بین برد.

اصل موضوع: اگر از «بلاکچین» به‌عنوان مترادف «دیجیتالی شدن» یا «چیزی مترادف با کاربرد رایانه و رمزنگاری» استفاده می‌کنید، ممکن است برای شما حقایقی که در این بخش به آن پرداخته می‌شود جذاب باشد! البته پیش‌بینی استفاده از راهکارهای فناوری برای مشکلات پیچیده بشر نیز قابل ذکر است.

اما «بلاکچین» درواقع به چه معنی است؟ در محدودترین شکل خود، بلاکچین درواقع ساختاری در جهت سازماندهی داده‌ها معنی شده است. به‌بیان‌دیگر، ساختاری مشتمل‌بر فهرستی از «چیزها»[1] است که به‌صورت «بلوک» طبقه‌بندی شده‌اند. هر بلوک جدید در بالای آخرین بلوک قرار دارد و شما مجاز به تغییر یا حذف داده‌های قدیمی نیستید. «قرار گرفتن در بالای» داده‌های پیشین با استفاده از رمزنگاری ایمن‌سازی شده است. هر بلوک به سلف خود «اشاره دارد»، و با اطلاع از « آخرین بلوک صحیح»، می‌توانیم بررسی کنیم که داده‌های همه بلوک‌های قبلی به شکل اصلی خود هستند یا خیر. این مسئله جهت حصول اطمینان از عدم دستکاری شدن وقایع بسیار مفید است. بااین‌حال، یک فرد مهاجم می‌تواند به‌راحتی با ایجاد زنجیره‌ای جعلی از بلوک‌ها، از آنها برای پنهان کردن تغییرات اعمال شده توسط خود استفاده نماید. بنابراین شما چگونه می‌توانید تصمیم بگیرید که به کدام زنجیره اعتماد کنید؟

ظهور بیت‌کوین: بیت‌کوین (و همچنین برخی از پروژه‌هایی که از آن الهام گرفته است) سعی در حل یک مشکل بسیار حساس دارد: چگونه گروهی از کاربران ناشناس با اطمینان در زمینه «صحت» بلوک‌ها توافق می‌نمایند؟ مسئله اعتمادسازی امری بسیار پیچیده و دشوار است. به‌عنوان‌مثال، شما نمی‌توانید با اطمینان رأی دهید، چراکه ارائه آرای جعلی در شرایطی که تمامی کاربران ناشناس هستند کار دشواری نیست. بیت‌کوین سعی می‌کند با استفاده از راهبرد «یک رأی به‌ازای هر واحد انرژی الکتریکی» این مشکل بسیار پیچیده را مرتفع نماید.

احتمالاً شما فقط با کاربران ناشناس و نامطمئن سروکار ندارید. بنابراین می‌توانید صریحاً

1. Things

گروهی از کاربرانی با حق رأی تعریف نمایید و بر اساس ساختار اعتمادسازی آن گروه همچنان به استفاده از ساختار داده‌های بلاکچین ادامه دهید. شما شکلی از بانک اطلاعاتی توزیع شده را دریافت خواهید نمود؛ چیزی که می‌تواند بسیار کارآمد باشد؛ البته اگر کاربران گروه شما بتوانند در مورد یک مدیر گروه به توافق برسند یا این‌که «ساخت و نامیدن یک بلاکچین» را الزامی ندانند.

اما شاید «قراردادهای هوشمند»[1] به ما کمک کند تا همه چیز را غیرمتمرکز کنیم؟ متأسفانه، آنها فقط برای کار با داده‌هایی که در حال حاضر بر روی بلاکچین تعریف شده‌اند مفید هستند. اطمینان از صحت داده‌ها در وهله اول هنوز یک مشکل برجسته و بسیار پیچیده است. به‌علاوه، این بلاکچین فقط یک زنجیره از بلوک‌ها است -یک بلاکچین چگونه می‌تواند از ماهیت اطلاعات مطلع باشند؟

حقیقت: ایده‌های مربوط به بیت‌کوین برای گروه‌هایی از کاربران که می‌خواهند مشترکاً یک رویداد را اجرا و حفظ نمایند، بسیار جذاب است؛ ایده‌ای جذاب که متاسفانه با مسئله عدم اعتماد به اطلاعات بدیهی ذخیره شده در هر واحد زنجیره همراه می‌باشد. خارج از این نگاه محدود، سیستم‌های مبتنی‌بر بلاکچین معمولاً عملکرد بدتری در برابر رویکردهای موجود دارند (از نظر توان، تأخیر، هزینه). در مورد موضوع عدم اعتماد - یک بلاکچین ممکن است به ما کمک کند تا از صحت داده‌های ذخیره شده اطمینان حاصل کنیم که تغییر در زنجیره ایجاد نشده است؛ اما از سنجش صحت اطلاعات اولیه باز می‌ماند.

1. Smart Contracts

نویسندگان این کتاب

توبیاس داینلین؛ پژوهشگر پسادکتری در گروه روان‌شناسی رسانه در دانشگاه هوهنهایم[1] آلمان است.

مارتین دیتوس؛ جغرافی‌دان دیجیتالی در انستیتوی اینترنت آکسفورد بوده و دارای بیش از یک دهه تجربه در محاسبات اجتماعی، پلتفرم‌های مشارکت انبوه، جغرافیای دیجیتال و کلان داده می‌باشد.

استفان دریر؛ پژوهشگر ارشد حقوق رسانه و حکمرانی رسانه و همچنین رئیس برنامه پژوهشی «تحول ارتباطات عمومی» در مؤسسه تحقیقات رسانه‌ای لایب‌نیتس و انستیتو هانس بردو هامبورگ است.

یوهانس آیزنهاوفر؛ پژوهشگر پسادکتری در دانشکده حقوق دانشگاه بیلفلد (آلمان) است.

فابیان فراری؛ دانشجوی دکتری در انستیتوی اینترنت آکسفورد، دانشگاه آکسفورد است.

مارتین فلورین؛ پژوهشگر ارشد مؤسسه جامعه شبکه‌ای ویزنباوم در برلین است. وی ریاست گروه تحقیقاتی میان‌رشته‌ای «اعتماد در محیط‌های توزیع شده»[2] را نیز به عهده دارد.

باب فرانکستون؛ مهندس رایانه و یکی از پیشگامان حوزه فناوری است که شهرت خود را با همکاری در ساخت اولین VisiCalc به دست آورده است

---

1. Universität Hohenheim
2. Trust in Distributed Environments

سباستین گابمن؛ مدرس ارشد مطالعات رسانه‌ای در دانشگاه زیگن[1] آلمان و پژوهشگر اصلی پروژه تحقیقاتی «فناوری‌های شبکه دیجیتال بین تخصص و تعمیم» در مرکز پژوهش‌های مشارکتی دانشگاه زیگن است.

مارک گراهام؛ استاد مؤسسه اینترنت آکسفورد، عضو هیئت علمی مؤسسه آلن تورینگ، پژوهشگر مهمان در مرکز علوم اجتماعی برلین[2] و مؤسسه جامعه شبکه‌ای ویزنباوم در برلین، و همچنین دستیار پژوهش دانشگاه کیپ تاون است.

نیکولاس گوگنبرگر؛ مدیر اجرایی پروژه جامعه اطلاعاتی و مدرس حقوق در دانشگاه ییل[3] در نیوهیون ایالات متحده است.

آملی پیا هلد؛ پژوهشگر حقوقی در مؤسسه تحقیقات رسانه‌ای لایب‌نیتس و انستیتو هانس بردو هامبورگ، کاندیدای دکتری در دانشگاه هامبورگ و فعال در مؤسسه اینترنت و جامعه هامبولد در برلین است.

پائولا هلم؛ پژوهشگر پسادکتری در پروژه تحقیقاتی «تحولات ساختاری حریم خصوصی» در دانشگاه فرانکفورت/ ماین است و در حال حاضر به‌عنوان استاد مهمان در مرکز نظارت‌پژوهی، دانشگاه کوئینز، کینگستون، کانادا مشغول به تدریس است.

اسون هرپیگ؛ مدیر پروژه سیاست امنیت سایبری بین‌المللی در اندیشکده «بنیاد مسئولیت‌های جدید»[4] در آلمان است.

ساشا هولیگ؛ پژوهشگر ارشد مؤسسه تحقیقات رسانه‌ای لایب‌نیتس وانستیتو هانس بردو در هامبورگ است.

کریستین کتزنباخ؛ پژوهشگر ارشد مؤسسه اینترنت و جامعه الکساندر فون هومبولت در برلین بوده و ریاست برنامه پژوهشی « جامعه دیجیتال در حال تحول» را به عهده دارد.

ماتیاس سی. کتمان؛ کارشناس ارشد حقوق (هاروارد)، رئیس برنامه پژوهشی «ساختارهای نظارتی و ظهور قوانین در فضاهای برخط» در مؤسسه تحقیقات رسانه‌ای لایب‌نیتس و انستیتو هانس بردو هامبورگ و همچنین دستیار پژوهش در مؤسسه اینترنت و جامعه الکساندر فون

1.University of Siegen
2. WZB Berlin Social Science Center
3. Yale University
4. Stiftung Neue Verantwortung

هومبولت در برلین است.

یولریک کلینگر؛ استاد ارتباطات دیجیتال در مؤسسه مطالعات رسانه و ارتباطات در دانشگاه فرای برلین[1] و رئیس گروه پژوهشی «اخبار، کمپین‌ها و عقلانیت گفتمان عمومی» در مؤسسه جامعه شبکه‌ای ویزنباوم در برلین است.

ریکا کولو؛ استادیار حقوق و دیجیتال‌سازی در دانشگاه هلسینکی و رئیس آزمایشگاه فناوری حقوقی این دانشگاه است.

امیلی لیدلو؛ استادیار دانشکده حقوق دانشگاه کالگری و عضو مؤسسه امنیت، حریم خصوصی و تضمین اطلاعات است.

دانیل لامباچ؛ پژوهشگر اصلی پروژه هایزنبرگ با عنوان «فضا، ابزار و اقدامات در هیئت فراملی» در مجمع تعالی « شکل‌گیری قواعد هنجاری» در دانشگاه فرانکفورت است.

کلادیا لمپرت؛ پژوهشگر ارشد در مؤسسه تحقیقات رسانه‌ای لایب‌نیتس و انستیتو هانس بردو هامبورگ بوده و حوزه تحقیقاتی وی متمرکز بر معاشرت رسانه‌ای و ارتباطات بهداشتی می‌باشد.

سوزت لیل؛ دانشجوی دکتری در دانشگاه ژوهانسبورگ آفریقای جنوبی است. پژوهش‌های او بر مشارکت برخط در جوامع حاشیه نشین و فقیر تمرکز دارد.

فیلیپه لورنز؛ مدیر پروژه هوش مصنوعی و سیاست خارجی در اندیشکده اس.ان.وی[2] کشور آلمان است.

استرید میجر؛ پژوهشگر ارشد پسادکتری در مؤسسه ارزیابی فناوری، آکادمی علوم اتریش و همچنین مدرس گروه مطالعات علوم و فناوری در دانشگاه وین است.

ژوزف میچال مینتال؛ دانشجوی دکتری در دانشگاه ماتج بل[3] در کشور اسلواکی، پژوهشگر و یکی از بنیان‌گذاران آزمایشگاه داده و جامعه UMB بوده و در مرکز رسانه، داده و جامعه در دانشگاه اروپای مرکزی نیز مشغول به فعالیت‌های پژوهشی است.

کاترینا موسن؛ دانشمند علوم سیاسی (کارشناس ارشد) در مؤسسه تحقیقات رسانه‌ای لایب‌نیتس و انستیتو هانس بردو در هامبورگ و یکی از بنیان‌گذاران انجمن سیاست و خط‌مشی

1.Freie Universität Berlin
2. Stiftung Neue Verantwortung (SNV)
3. Matej Bel

اینترنتی فمینیستی است.

فرانچسکو موسیانی؛ استادیار پژوهشی مرکز ملی تحقیقات علمی فرانسه[1] و معاون مرکز اینترنت و جامعه این دانشگاه در پاریس است.

اندرو اودلیزکو؛ تجربه زیادی در پژوهش و مدیریت پژوهش دارد، از جمله موضوعات امنیتی در آزمایشگاه‌های Bell و آزمایشگاه‌های AT&T و اکنون مدرس دانشکده ریاضیات دانشگاه مینسوتای مینیاپولیس است.

فرانچسکا اومر؛ پژوهشگر ارشد و دستیار آموزش در گروه ارتباطات و تحقیقات رسانهٔ دانشگاه فریبورگ (CH) است. وی دارای دکتری علوم ارتباطات از دانشگاه زوریخ است و دوره کارشناسی خود را در رشته حقوق گذرانده است.

سانا اوجانپرا؛ پژوهشگر و دانشجوی دکتری در مؤسسه اینترنت آکسفورد، دانشگاه آکسفورد و همچنین در مؤسسه آلن تورینگ و نیز محقق آینده‌پژوه در سازمان همکاری و توسعه اقتصادی است.

استفانو پدرازی؛ دستیار پژوهش و تدریس و دانشجوی دکتری در گروه ارتباطات و تحقیقات رسانه‌ای دانشگاه فریبورگ (CH) است. وی دارای مدرک علوم ارتباطات و رسانه، اقتصاد و تاریخ مدرن از دانشگاه زوریخ است.

مارک پری؛ استاد حقوق و رئیس هیئت علمی دانشگاه نیوانگلند، استرالیا و همچنین استاد بازنشسته دانشگاه وسترن آنتاریو کانادا است. وی در آنجا علوم رایانه تدریس می‌کرد.

ایان پیتر؛ یکی از پیشگامان اینترنت و مورخ است. وی به‌عنوان هماهنگ کننده کارگروه حکمرانی اینترنت[2] و نماینده فعال جامعه مدنی در تحولات حکمرانی اینترنت بوده است.

آمادئوس پیترز؛ یک پژوهشگر حقوق جزا و دیجیتالی‌سازی در مؤسسه اینترنت و جامعه الکساندر فون هومبولت (HIIG) در برلین است.

رکسانا رادو؛ پژوهشگر پسادکتری در مرکز مطالعات اجتماعی-حقوقی دانشگاه آکسفورد و همچنین دستیار پژوهشی در مرکز حکمرانی جهانی[3] انستیتوی فارغ التحصیلان مطالعات

1.French National Centre for Scientific Research
2. Internet Governance Caucus
3. Global Governance Centre

بین‌المللی و توسعه ژنو است.

سباستین راندراث؛ در رشته رسانه و مطالعات اقتصادی در دانشگاه سیگن مشغول به تحصیل است، در مرکز تحقیقاتی رسانه‌های مشارکتی به پژوهش می‌پردازد و همچنین در هماهنگ‌سازی مجموعه همایش‌های Pre_Invent درباره فرهنگ‌های دیجیتال، جامعه، فناوری و هنر همکاری دارد.

توماس رینهولد؛ دانشمند رایانه و پژوهشگر انستیتوی تحقیقات صلح و سیاست امنیتی در دانشگاه هامبورگ ست.

کیت ساسلو؛ مدیر پروژه هوش مصنوعی و سیاست خارجی و سیاست امنیت سایبری بین‌المللی در اندیشکده سیاست فناوری آلمان در برلین است.

کورت ام. ساندرز؛ استاد حقوق تجارت در دانشگاه ایالتی کالیفرنیا در نورتریج است.

دیوید شولز؛ دارای مدرک کارشناسی ارشد بوده و دستیار پژوهشی بخش آسیا در مؤسسه آلمانی امور بین‌الملل و امنیتی در برلین است.

ماتیاس شولز؛ دکتر ماتیاس شولز پژوهشگر سیاست امنیت سایبری در بخش امنیتی مؤسسه آلمانی امور بین‌المللی و امنیتی در برلین است.

ایلجا اسپرلینگ؛ مشاور فناوری پروژه رتبه‌بندی حقوق دیجیتال (آمریکای جدید) است.

ماتیاس اسپیلکامپ؛ یکی از بنیان‌گذاران و مدیر اجرایی AlgorithmWatch در برلین، یک سازمان وکالت مبتنی‌بر شواهد با هدف نظارت جدی بر استفاده از نظام‌های تصمیم‌گیری خودکار،است. وی دارای دو مدرک کارشناسی ارشد روزنامه‌نگاری از دانشگاه کلرادو در بولدر و مدرک کارشناسی ارشد فلسفه از دانشگاه آزاد برلین است.

آلک تارکوفسکی؛ یکی از بنیان‌گذاران و رئیس بنیاد دیجیتال[1]، یک اندیشکده دیجیتال لهستانی، است که هدف آن اطمینان از تعلق اینترنت به مردم می‌باشد. وی همچنین عضو مؤسس کمونیا، انجمن اروپایی در حوزه عمومی دیجیتال لهستان است.

تورستن تیل؛ دکتر تورستن تیل نظریه‌پرداز سیاسی و رهبر گروه پژوهشی «دموکراسی و

1.Centrum Cyfrowe

دیجیتال‌سازی» در مؤسسه جامعه شبکه‌ای ویزنباوم در برلین است.

توماسو ونتورینی؛ توماسو ونتورینی پژوهشگر در حوزه اینترنت و جامعه در انستیتو مطالعات سیاسی پاریس[1] است.

دانیل ولسن؛ پژوهشگر حوزه مسائل جهانی انستیتو «مسائل امنیتی و بین‌المللی»[2] کشور آلمان است.

مکسی میلیان وون گرافنشتاین؛ پروفسور مکسی میلیان وون گرافنشتاین، کارشناس ارشد حقوق، مدرس حوزه دیجیتال در دانشگاه هنر برلین، و مدیر برنامه تحقیقاتی «داده‌ها، عوامل، زیرساخت‌ها: حکمرانی نوآوری و امنیت سایبری مبتنی‌بر داده» در مؤسسه اینترنت و جامعه الکساندر فون هامبولت (HIIG) در برلین است.

رابین تیم ویس؛ کارشناس ارشد (هایدلبرگ)، مدیر ارشد پروژه در دفتر علم و فناوری اتریش (OSTA) واقع در سفارت اتریش در واشنگتن دی‌سی است.

آلیا ورنیک؛ پژوهشگر مؤسسه اینترنت و جامعه الکساندر فون هومبولت (HIIG) در برلین و دانشجو دکتری در دانشگاه لودویگ ماکسیمیلیان مونیخ است.

لئید زقلامی؛ دارای مدرک دکتری و مدرس دانشکده اطلاعات و ارتباطات، دانشگاه الجزایر ۳ و داور خارجی دانشگاه موریس است.

ماریانو زاکرفلد؛ دکتر ماریانو زاکرفلد پژوهشگر شورای ملی تحقیقات علمی و فنی (CONICET)، مرکز فناوری علمی و جامعه، دانشگاه میمونیدز و مدرس جامعه‌شناسی انفورماتیک در دانشگاه بوئنوس آیرس است.

1.Paris Institute of Political Studies (Sciences Po Paris or Sciences Po)
2. Institute for International and Security Affairs (Stiftung Wissenschaft Und Politik)

فهرست اختصاری مفاهیم و اصطلاحات

G7	Group of Seven
G20	Group of Twenty
AI	Artificial Intelligence
ASEAN	Association of Southeast Asian Nations
BRICS	Brazil, Russia, India, China and South Africa
CDA	Communications Decency Act
CSNET	Computer Science Network
DNC	Democratic National Committee
DNS	Domain Name System
DoT	DNS over Transport Layer Security
E2EE	End-to-End Encryption
GGE LAWS	Group of Governmental Experts on Autonomous LethalWeapons Systems
HTTPS	Hypertext Transfer Protocol Secure
IAB	Internet Architecture Board
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Name and Numbers
ICTs	Information and Communication Technologies
IETF	Internet Engineering Task Force
ILO	International Labour Organization

IoT	Internet of Things
IP	Intellectual Property
ITU	International Telecommunication Union
ML	Machine Learning
NN	Net Neutrality
OEWG	Open-ended Working Group
OECD	Organization for Economic Co-operation and Development
OPM	United States Office of Personnel Management
OSCE	Organization for Security and Co-operation in Europe
OSI	Open Systems Interconnection
P2P	Peer-to-Peer Networking Technology
SCO	Shanghai Cooperation Organization
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
UGC	User-Generated Content
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNCTAD	United Nations Conference on Trade and Development
UNGGE	United Nations Group of Governmental Expertson Developments in the Field of Information and Telecommunications in the Context of International Security
USG	United States Government
GDPR	General Data Protection Regulation
WHO	World Health Organization
WIPO	World Intellectual Property Organization
WSIS	World Summit on Information Society
WTO	World Trade Organization

مرکز ملی فضای مجازی
انتشارات پژوهشگاه فضای مجازی

BUSTED! THE TRUTH ABOUT THE 50 MOST COMMON INTERNET MYTHS

به موازات توسعه فناوری، ابعاد رفتار کاربران و همچنین پیامدهای استفاده آنها از اینترنت و شبکه‌های وابسته به آن نیز روزبه‌روز پیچیده‌تر و گسترده‌تر می‌شود. اگر تا چندی پیش صرفاً بحث «استفاده» و یا «عدم استفاده» از اینترنت یا «عضویت» یا «عدم عضویت» در شبکه‌های اجتماعی مطرح بود، امروزه جامعه و به طور خاص طیف وسیعی از کاربران در بین حجم انبوهی از موضوعات و مسائل فنی با آثار و پیامدهای فراوان و طولانی‌مدت اجتماعی، فرهنگی، سیاسی و دینی همچون «اثرات استرایسند»، «الگوریتم پروتکل‌های اینترنتی»، «واقعیت رمزگذاری پایان-به-پایان»، «دارک وب»، «فیلترینگ حبابی»، «حقوق دیجیتال»، «حق فراموش‌شدگی»، «آستروتورفینگ و شهرت جعلی»، « فناوری نظیر به نظیر»، «دستکاری یا سرقت اطلاعات» و ده‌ها مقوله فنی، حقوقی و ارتباطی دیگر آشکارا سردرگم و رها شده است.