بسم الله الرحمن الرحیم

عصر فضای مجازی

گزارش شماره ۶۶

خرداد ۱۴۰۰

مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

مواجهه با اطلاعات کاذب:
ارزیابی استدلال به نفع اصلاحیه بخش ۲۳۰ قانون حسن رفتار ارتباطات

محتوای انتشار یافته در این اثر
الزاماً بیانگر دیدگاه مرکز ملی فضای مجازی نیست

تهیه شده در پژوهشگاه فضای مجازی
(گروه مطالات بنیادین)

مترجم: دکتر مهدی خلیلی

ناظر علمي: ناظر علمي: دکتر علیرضا کاظمی-
دکتر حسین مطلبی کربکندی

نشانی: تهران، میدان آرژانتین، خیابان بیهقی، نبش
خیابان ۱۶ غربی، پلاک ۲۰
تلفن: ۰۲۱-۸۶۱۵۱۰۶۱
کد پستی: ۱۵۱۵۶۷۴۳۱۱

فهرست

سخن نخست

سخن نخست

فضای مجازی با شتاب شگرف و رو به تزایدی که در حال بسط و گسترش است تمام ساحات اجتماعی، اقتصادی، سیاسی و فرهنگی زندگی بشر را درنوردیده و هر روز بخش بزرگی از زندگی واقعی را در خود فرو برده و حیات متفاوت و جدیدی به آن می‌دهد. لذا به نظر می‌رسد دو نگاه کلان به فضای مجازی وجود دارد: نگاه اول که بالاخص در ابتدای رشد و تکوین فضای مجازی مسلط شده بود، آن را همچون ابزاری کنار سایر ابزارهای بشری تصویر می‌کرد که تنها طریقیت داشت. اما نگاه دوم، در نتیجه رشد تحولات خیره‌کننده فضای مجازی و سایه گستری آن در حوزه‌ها و شئون بشر در یک دهه اخیر آن را چون سکویی می‌داند که بسیار فراتر از شأن ابزاری حیات انسان‌ها را سامان جدیدی داده و ادعای تمدن نوینی را دارد. رویکردی که از قضا از چشمان بصیر رهبر انقلاب نیز دور نمانده و انتظاری تمدنی از فضای مجازی در ایران را مطالبه داشته‌اند.

در همین راستا گزارش‌های عصرفضای مجازی تلاش می‌کند تا فهم سازمان‌ها و دستگاه‌های مرتبط با حوزه فضای مجازی را ارتقاء بخشیده و آن‌ها را برای مواجهه فعال و خردمندانه با تحولات این عرصه مهیا سازد.

سید ابوالحسن فیروزآبادی
دبیر شورای عالی و رئیس مرکز ملی فضای مجازی

چکیده

چکیده

مقالـه « مواجهـه بـا اطلاعـات کاذب: ارزیابـی اسـتدلال به‌نفـعِ اصلاحیـه بخـش ۲۳۰ قانـون حسـن رفتـار ارتباطـات» نوشـته تیـم هوانـگ پژوهشـگر مرکـز امنیـت و فنـاوری نوظهـور در دانشـگاه جرج‌تـاون اسـت کـه در سـال ۲۰۲۰ در کتـاب «رسـانه‌های اجتماعـی و مردم‌سـالاری» چـاپ انتشـارات دانشـگاه کمبریـج بـه چاپ رسـیده اسـت.

مسـئله میـزان مسـئولیت سـکوها در قبـال محتوایـی کـه از بسـتر آن‌هـا انتشـار می‌یابـد، یکی از مسـائل پیچیده حقوقی اسـت کـه در مجامع مختلفی از جمله در کشـور ما مورد بحث و بررسـی قرار گرفته و محل نزاع واقع شـده اسـت. ایـن مقالـه به بررسـی بخـش ۲۳۰ اقدام حسـن رفتار ارتباطـات ایالات متحده می‌پردازد که قانونی اسـت که مسـئولیت سـکوها را نسـبت به محتوای تولیدشـده توسـط کاربـران در آن‌ها مشـخص می‌کند. این قانون کـه به‌عنوان سـنگ بنای آزادی اینترنت و انتشـار آزاد ایده‌ها مطرح می‌شـود، تا حد زیادی به سـکوها نسـبت به محتوای تولیدشـده توسـط کاربرانشـان مصونیت قضایی اعطا می‌کند. با گسـترش اطلاعـات کاذب در فضای مجازی، بالأخص اطلاعات کاذب سیاسـی کـه نظام‌هـای مردم‌سـالار و انتخابـات را بـا چالش‌هـای جدی مواجـه کـرده اسـت، درخواسـت‌ها برای اصـلاح این قانـون به منظـور افزایش

مسئولیت سکوها گسترده‌تر شده است. در این فصل پیشنهادهای حقوقی متنوع برای اصلاح در این قانون به بحث گذاشته شده است و نویسنده نشان می‌دهد که پیچیدگی‌های زیادی در این پیشنهادها وجود دارد تا جایی که برخی از آن‌ها می‌تواند مشکلات جدیدی را به وجود آورند. برای مثال چنین اصلاحاتی می‌تواند سکوها را بیش از اندازه محتاط کند تا حدی که از ترس مسئولیت قضایی اقدام به تصحیح بیش از اندازه و حذف محتویات بدون مشکل کنند. همچنین نویسنده راهکارهای حقوقی بدیلی را به بحث می‌گذارد که بدون نیاز به اصلاح این قانون، بتوان سکوها را ملزم به همکاری در راه مبارزه با اطلاعات کاذب نمود.

قانون‌گذاری و تنظیم‌گری رفتار سکوها، بالأخص در زمینه‌های سیاسی یکی از مهم‌ترین راهکارهای مطرح شده برای مقابله با انتشار اطلاعات کاذب است. با این حال، پیچیدگی‌های حقوقی بسیاری در این زمینه وجود دارد و قوانین ناکارآمد می‌توانند عواقب ناخواسته زیادی به جای بگذارند و در برآورده کردن هدف اصلی ناموفق باشند. از این رو این مقاله که در آن با بررسی نزدیک به ۱۰۰ منبع به‌روز، مسئله قوانین فعلی ایالات متحده و امکان اصلاح آن‌ها برای افزایش مسئولیت سکوها در برابر اطلاعات کاذب به بحث گذاشته است، از منظر قانون‌گذاری و سیاست‌گذاری دارای نکات ارزشمند فراوانی است.

واژگان کلیدی: اطلاعات کاذب، مسئولیت سکوها، مصونیت سکوها، قانون حسن رفتار ارتباطات

مقدمه

مقدمه

مواجهه با اطلاعات کاذب: ارزیابی استدلال به نفع اصلاحیه بخش ۲۳۰ قانون حسن رفتار ارتباطات [1]

تیم هوانگ [2]

افشاگری‌های پیرامون دخالت روسیه در انتخابات ریاست‌جمهوری ۲۰۱۶ آمریکا و نقشی که ممکن است «اخبار جعلی» در شکل‌گیری ترجیحات رأی دهندگان بازی کرده باشد، باعث ایجاد گفتگویی گسترده در میان پژوهشگران، سیاست‌گذاران، فناوران، و دیگران در مورد چگونگی مبارزه با گسترش و نفوذ اطلاعات کاذب برخط شده است. تعدادی از پیشنهادهای قانونی یا تنظیم‌گرانه که از این گفتگوها برخاسته‌اند احیاناً باعث می‌شوند که اطلاعات کاذب از طریق وب دشوارتر جریان یابد.

با توجه به ماهیت تکه‌تکه‌ی ایجاد اطلاعات در سرتاسر وب، بسیاری از این پیشنهادها به نقش مرکزی که سکوهای برخط مانند گوگل، فیسبوک، و توییتر در شکل دادن به توزیع اطلاعات در سراسر وب ایفا می‌کنند اتکا دارند. با ایجاد مشوق‌ها - یا مجازات‌هایی - که سکوها را به پذیرفتن نقش فعالانه‌تر در از بین بردن یا مبارزه با اطلاعات کاذب تشویق می‌کند، این مداخلات به دنبال استفاده حداکثری از موقعیت منحصر به فرد این شرکت‌ها به‌عنوانِ مؤثرترین و «کم‌هزینه‌ترین جلوگیری کننده‌های»[3] بالقوه در پرداختن به چالش ناشی از اطلاعات کاذب است.

برای این منظور، این مداخلات با حمایت‌های قانونی طولانی‌مدت ارائه شده

1. Dealing with Disinformation: Evaluating the Case for Amendment of Section 230 of the Communications Decency Act
2. Tim Hwang
3. Least cost avoider

در بخش ۲۳۰ قانون حسن برای این منظور، این مداخلات با حمایت‌های قانونی طولانی‌مدت ارائه شده در بخش ۲۳۰ قانون حسن رفتار ارتباطات ۱۹۹۶ (۲۳۰ CDA)،[1] مواجه است؛ ماده قانونی کلیدی که به طور گسترده‌ای از سکوها در برابر مسئولیت[2] قانونی اقدامات کاربران شخص ثالثِ خدمات آنها محافظت می‌کند. طی دو دهه گذشته، این ماده به عنوان پیش‌رانه‌ی اصلی رشد خدمات برخط و سنگ بنای حمایت از آزادی بیان در وب تلقی شده است. همچنین چنین استدلال شده است که CDA ۲۳۰ از پاسخ‌گو بودن سکو به آسیب‌های ناشی از آزار و اذیت، افترا، پورنوگرافی کودکان و بسیاری از دیگر فعالیت‌های برخط جلوگیری می‌کند. بحث‌های کنونی در مورد نحوه مواجهه با «اخبار جعلی» به تلاش‌های پیشین برای اصلاح یا از بین بردن سپر فراهم‌شده توسط CDA ۲۳۰ ملحق می‌شوند.

این فصل بنا دارد با توجه به این پیشینه تاریخی به سه پرسش بپردازد. اول، آیا اصلاحات در CDA ۲۳۰ می‌تواند راه را برای پاسخی مؤثر به چالش‌های ناشی از اطلاعات کاذب برخط هموار کند؟ دوم، اگر می‌تواند، آیا چنین اصلاحاتی باید انجام شود؟ نهایتاً، چگونه باید چنین اصلاحاتی انجام شود؟

«بخش ۱: چالش اطلاعات کاذب» چالشی را چهارچوب بندی می‌کند که بوسیله اطلاعات کاذب برخط، مشخصاً بوسیله تهدید ناشی از تلاقی بازیگران با انگیزه سیاسی، مجاریِ رسانه‌ای با انگیزه مالی، و فرهنگ «ترول»[3] برخط، ایجاد می‌شود. «بخش ۲: چگونه CDA ۲۳۰ تلاش‌ها برای مبارزه با اطلاعات کاذب سیاسی برخط را شکل می‌دهد؟» تاریخ قانون‌گذاری و دادرسی[4] موجود پیرامون CDA ۲۳۰ را بررسی، و تأثیر آن

1. Section 230 of the Communications Decency Act of 1996 (CDA 230)
2. Liability
3. Troll. در فضای اینترنت، ترول شخصی است که با گفتار و رفتارش افراد دیگر را ناراحت می‌کند. م.
4. Case law

را در مبارزه با چالش اطلاعات کاذب برخط ارزیابی می‌کند. «بخش۳: آیا CDA ۲۳۰ باید اصلاح شود تا اطلاعات کاذب سیاسی را برطرف کند؟» این چالش را مطرح می‌کند که آیا CDA ۲۳۰ باید با توجه به این تحلیل اصلاح شود یا خیر، و نتیجه می‌گیرد که اصلاح بخشیِ متمرکز بر تکنیک‌های استفاده‌شده توسط کارزارهای اطلاعات کاذب[1] موجّه است.

1. Disinformation campaigns

بخش اول

بخش اول

چالش اطلاعات کاذب

«اخبار جعلی» برای توصیف شیوع داستان‌های نادرست یا غیردقیقِ برخط، که به عنوان نشانه‌ای از وضعیت ضعیف کیفیت اطلاعات در رسانه‌ها و به‌طورکلی در جامعه تلقی می‌شود، به اصطلاحی رایج تبدیل شده است. این داستان‌ها حین انتخابات ریاست‌جمهوری ۲۰۱۶ ایالات متحده به طور گسترده پخش شدند، به‌طوری‌که یک نظرسنجی حاکی از آن است که نزدیک به یک پنجم بزرگسالان آمریکایی عناوینی (کذب) دیدند که ادعا می‌کرد که پاپ از دونالد ترامپ، نامزد آن زمان ریاست‌جمهوری، حمایت کرده است و به معترضان برای اخلال در تجمعات حمایت از ترامپ ۳۵۰۰# پرداخت شده بود.[1] این داستان‌ها همچنین معتبر در نظر گرفته شدند، به‌طوری‌که ۶۴ درصد و ۷۹ درصد پاسخ‌دهندگان اظهار داشتند که معتقدند این داستان‌ها به ترتیب «بسیار یا تاحدودی دقیق» اند.[2]

با این حال، همان‌طور که دیگران متذکر شده‌اند، استفاده از «اخبار جعلی» به عنوان چهارچوبی مفهومی در تعدادی از سطوح مشکل‌آفرین است.[3] به خودی خود، گسترش اطلاعات نادرست در لباس حقیقت، چه به صورت برخط و چه به‌طورکلی در کانال‌های ارتباطی،

1. Silverman and Singer-Vine 2016
2. Silverman and Singer-Vine 2016
3. Oremus ،2016 Sullivan ،2017 Nielsen and Graves 2017

یک پدیده جدید نیست.[1] علاوه بر این، مشکلات زیادی در تعریف خطوطِ کلی پدیده «اخبار جعلی» وجود دارد. آیا این [تعریف] فقط باید در موردِ تولید کامل و کلی وقایع و ادعاها درباره واقعیت اعمال شود؟ یا شامل ارائه غیرکامل اطلاعات یا توصیف نامنصفانه وقایع نیز می‌شود؟

یک چهارچوب بندی واضح‌تر از ماهیت تهدید ادعا شده برای ارزیابی پرونده‌ی اصلاح یا حذف CDA ۲۳۰ لازم است. این فصل بر سه پیشرفت عمده متمرکز است که محرکِ انگیزه بحث‌های پس از ۲۰۱۶ درباره اطلاعات کاذب برخط و پاسخ تنظیم‌گرانه آن بوده‌اند. این سه مورد بدین قرار است: (۱) انتشار فعالانه‌ی اطلاعات کاذب توسط دولت‌ها و رسانه‌های متعلق به دولت، (۲) بازیگرانی با انگیزه مالی که برای به دست آوردن درآمد تبلیغاتی، اطلاعات کاذب را پیش می‌رانند، و (۳) فعالیت‌های جوامعِ «ترول» برخط به عنوانِ بردار گسترش اطلاعات کاذب. این فصل به ویژه بر کارزارهای اطلاعات کاذب سیاسی، یعنی اطلاعات نادرستی که هدف آنها شکل دادن به ادراک [افراد] درباره‌ی برخی از جنبه‌های گفتمان سیاسی است، تمرکز دارد و نه بر تلاش‌هایی که داستان‌های نادقیق را در موضوعات دیگر مانند کسب سود شرکت‌ها یا مرگ افراد مشهور منتشر می‌کنند.[2]

این فصل برخی از انواع دیگر نادرستی را نیز حذف می‌کند چرا که آن‌ها در بحث‌های تنظیم‌گرانه حول «اخبار جعلی» محل تمرکز اصلی نبوده‌اند؛ این امر شامل گسترش سهوی اطلاعات نادرست یا گمراه‌کننده از طریق وب است که از یک تلاش هماهنگ حاصل نمی‌شود. همچنین، این فصل بر فعالیت‌هایی که اساساً در پی انتشار اطلاعات کاذب‌اند متمرکز است - و آن را از مواردی که یک کارزار صرفاً سعی در تقویت دیدگاه یا گسترش آگاهی از یک واقعیت دارد متمایز می‌کند.

1. Barnoux 1966; Mulford 2008
2. Lee 2017

تردیدی نیست که این دسته‌بندی‌ها اساساً در مصادیق مرزی مبهم‌اند. یک کارزار اطلاعات کاذب ممکن است از یک تصور غلط موجود که به صورت ارگانیک گسترش می‌یابد استفاده حداکثری کند، یا تلاش برای جلب توجهات به سمت یک دیدگاه خاص ممکن است حقیقت را به صورت استراتژیک قالب‌بندی کند یا حتی به تدریج به نادرستی و کذب بینجامد. موضوعات غالباً از مرز مبهم میان گفتمان «سیاسی» و «غیرسیاسی» عبور می‌کنند، به طور مثال: نظریه‌های نادرست پیرامون خطرات واکسن‌ها که توسط فعالان «ضد واکسن»[1] تبلیغ شد. با این حال، این بخش در تلاش است، از طریق این چهارچوب تقریبی، پیش‌زمینه برخی از فعالیت‌هایی را ارائه کند که انگیزه دعوت‌های اخیر برای اقدامات قانونی و تنظیم‌گرانه در مورد اطلاعات کاذب برخط را فراهم کرده‌اند.

اطلاعات کاذب بواسطه‌ی عاملان دولتی

شاید محرک اصلی دعوت‌ها به واکنش تنظیم‌گرانه به چالش‌های ناشی از تهدیدهای اطلاعات کاذب برخط این موضوع باشد که توسط جامعه‌ی اطلاعاتی[2] [ایالات متحده] تأیید شد که عاملان دولتی روسیه در تلاشی فعال برای شکل دادن به گفتمان پیرامون انتخابات ریاست‌جمهوری ۲۰۱۶ ایالات متحده درگیر بودند.[3] کارزار ۲۰۱۶ روسیه تلاشی چند جانبه با قصدِ تضعیف اعتماد به چهره‌های سیاسی مورد هدف بود. این موضوع شامل نظریه‌های توطئه مانند «پیتزاگیت»[4] بود، این تلقی را گسترش می‌داد که نامزد حزب دموکرات، یعنی هیلاری کلینتون، و رئیس ستاد انتخاباتی کلینتون، یعنی جان پودستا، اعضای یک حلقه زیرزمینی قاچاق رابطه جنسی‌اند.[5] فراتر از تلاش برای گسترش اطلاعات کاذب، این تلاش‌ها

1. Antivax
2. Intelligence community
3. NCCIC 2016; National Intelligence Council 2017
4. Pizzagate
5. Robb 2017

شامل کوشش برای تشدید دو قطبی سیاسی بود، که در یک مورد باعث ایجاد بحث و اختلاف نژادی در مورد اجرای قانون بین فعالان گروه‌های «جان سیاهان مهم است»[1] و «جان آبی‌ها مهم است»[2] شد.[3]

این کارزار همچنین از طریق طیف وسیعی از کانال‌های مختلف فعالیت کرد. رسانه‌های معتبر دولتی مانند اسپوتنیک[4] و راشا تودی[5] برای ایجاد و انتشار گسترده اطلاعات کاذب استفاده شدند. این کانال‌ها [که] مشخص‌تر]عمل می‌کردند[در کنار رخنه «شبه-مردمی»[6] ظریف‌تر جوامع برخط و خرید تبلیغات هدفمند از طریق سکوهای مختلف رسانه‌های اجتماعی فعالیت کردند.

فراتر از شیوع دادنِ اطلاعات کاذب، این کارزار همچنین درگیرِ هک کردن‌هایی بود که اطلاعاتِ حساس و رسوایی آورِ خصوصی نگهداری شده توسط احزاب سیاسی و نامزدهای دو طرف رقابت انتخاباتی را هدف قرار می‌داد.

اگرچه کارزار روسیه در سال ۲۰۱۶ نمونه‌ای بسیار بحث شده از اطلاعات کاذب برخط تحریک‌شده توسط یک دولت بوده است، استفاده از این روش‌ها امر جدیدی نیست. محققان در سال‌های اخیر کارزارهای اطلاعات کاذب برخط مشابهی را که روسیه برای تأثیر بر گفتمان سیاسی در اروپای مرکزی و شرقی و همچنین خاورمیانه راه‌اندازی کرده، ردیابی کرده‌اند.[7]

در ضمن این کارزارها مختص روسیه نیستند. محققان دریافته‌اند که در سال‌های اخیر از شبکه‌های اجتماعی برای اهداف مرتبط با اطلاعات کاذب سیاسی در طیف وسیعی از زمینه‌های گوناگون استفاده شده است. این حوادث شامل تلاش‌هایی است که، برای نمونه، در مکزیک، برزیل،

1. Black Lives Matter
2. Blue Lives Matter
3. Alcindor 2017; Seetharaman 2017
4. Sputnik
5. Russia Today
6. “grassroots” infiltration
7. Chen 2015; Lange-Ionatamishvili, Svetoka, and Geers 2015; NPR 2017; Wintour 2017

منظور پلیس‌هاست که یونیفرم آبی به تن دارند. م .

کانـادا، و چیـن مشـاهده شـده اسـت.[1] ایـن کارزارهـا توسـط عامـلان دولتی، همچـون مـورد روسـیه، راه انـدازی شـده‌اند، و عـلاوه بـر ایـن، توسـط طیـف وسـیعی از گروه‌هـای مسـتقل نیـز راه‌انـدازی شـده‌اند.[2]

مشوق‌های مالی برای اطلاعات کاذب

تشـخیص اینکـه عامـلان بـا انگیـزه سیاسـی در تـلاش بـرای تأثیرگذاری در انتخابـات ۲۰۱۶ بوده‌انـد، در کنـار تعـداد فزاینـده‌ای از گزارشـگرانی ظهور کـرده اسـت که مشـوق‌های مالـی ایجاد و انتشـار اطلاعـات کاذب را گوشـزد کرده‌انـد. بـه طـور خـاص، تبلیغـات برخـط بـه عنـوان محرکـی بـرای ایجـاد محتـوای کاذب اما بسـیار اشـتراک‌پذیر شـناخته شـده اسـت کـه بازدیدهای صفحـات درآمـدزا را بـه سـمت محتـوای برخـط سـوق می‌دهد.

در زمینه‌ی انتخابات ریاسـت‌جمهوری ۲۰۱۶ ایالات متحده، هم در داخل و هـم در خـارج کشـور، مشـاغلی در ایجادِ سـایت‌هایی برای انتشـار اطلاعات کاذب از طریـق وب فعالیـت داشـتند. مجـاری رسـانه‌ای شـامل سـایت‌هایی ماننـد «دنـور گاردیـن»[3] طیـف وسـیعی از نظریه‌هـای توطئـه را گسـترش می‌دادنـد، ماننـد داسـتانی کـه کلینتـون را بـه قتـل یـک مأمور افبـی‌آی در تحقیـق دربـاره اسـتفاده وی از یـک سـرور ایمیـل خصوصی مرتبـط می‌کرد، کـه ایـن داسـتان میلیون‌هـا بـار در سراسـر فیسـبوک بـه اشـتراک گذاشـته شـد.[4] در حالـی کـه ایـن سـایت بـا ظاهـر یـک روزنامـه محلـی در کلـرادو[5] طراحـی شـده بـود، در واقـع توسـط یـک کارآفرین مسـتقر در لـس آنجلس[6] اداره می‌شـد کـه همچنیـن مجموعـه‌ای از سـایت‌های دیگر را که از اشـتراک اطلاعـات کاذب سـود می‌بردنـد، اداره می‌کـرد.[7]

در خارج از ایالات متحده، روزنامه‌نگاران گروه‌هایی از کارآفرینان را در مقدونیه

1. Finley ،2015 Robertson et al. ،2016 Woolley and Howard 2017
2. Robertson et al. 2016
3. The Denver Guardian
4. Coler 2016
5. Colorado
6. Los Angeles
7. Coler 2016

و سایر کشورها کشف کرده‌اند که از طریق فروش تبلیغات در کنار تهیه اطلاعات کاذب به خوانندگان راست‌گرای[1] برخط، سود می‌برند.[2] داستان‌ها شامل «اخبار» حمایت پاپ فرانسیس از ترامپ، نامزد وقت، و گزارش‌های جعلی از سیلی‌زدن نامزد [دموکرات] به یک معترض در یک اجتماعِ انتخاباتی بود.[3] این سایت‌ها گاهی اوقات به عنوان تقویت‌کننده و نه مبدع اطلاعات کاذب عمل می‌کردند، یعنی مطالب را از سایت‌های دیگر به صورت برخط کپی می‌کردند و آنها را از طریق انبوه حساب‌های جعلی در سکوهای رسانه‌های اجتماعی مانند توییتر و فیسبوک ترویج می‌دادند.[4]

بحث پیرامون انگیزه‌های مالی برای اطلاعات کاذب به بحث در مورد مجاری تولید و ترویج برخط این محتوا محدود نشده است. از آنجا که بسیاری از برجسته‌ترین سکوهای برخط مانند گوگل و فیسبوک خود به تبلیغات متکی‌اند، منتقدان و محققان همچنین تأکید کرده‌اند که با توجه به اینکه محتوای اطلاعات کاذب اغلب به طور گسترده‌ای به اشتراک گذاشته و مشاهده می‌شود، شرکت‌های میزبان این فعالیت ممکن است انگیزه‌هایی را برای حفظ آن‌ها داشته باشند.[5] به نوبه خود، این سکوها در بیانیه‌های عمومی متعدد این تصور را انکار کرده و اقداماتی را علیه اطلاعات کاذب با محدود کردن پخش شدنِ تبلیغات انجام داده‌اند.[6]

«فرهنگ ترول» به عنوان یک منبع اطلاعاتی نادرست

فراتر از فعالیت عاملان با انگیزه‌های سیاسی و مالی، مشارکت فرهنگ «ترول» برخط شبه - مردمی[7] نیز نیرویی در تسهیل اطلاعات کاذب سیاسی بوده است. فعالیت انبوه مردم - که اغلب به صورت ناشناس انجام می‌شود - برای غافل‌گیری و اذیت شهروندان خصوصی، شخصیت‌های

1. right-wing
2. Tynan ،2016 Subramanian 2017
3. Subramanian 2017
4. Subramanian 2017
5. Allcott and Gentzkow ،2017 Thompson 2017
6. Wingfield، Isaac and Benner ،2016 Ling 2017
7. grassroots

عمومی و نهادها برای اهداف صرفاً سرگرم‌کننده، یکی از ویژگی‌های دیرینه رفتارهای اجتماعی در اینترنت بوده است.[1] این فعالیت‌ها در گذشته طیف وسیعی از تاکتیک‌ها را مورد استفاده قرار داده است، از دست‌کاری در نظرسنجی‌های برخط گرفته تا هدف‌گیری استراتژیک روزنامه‌نگاران و «کوبه زدن»[2]- یعنی گزارش‌های اضطراری جعلی به نهادهای مجری قانون با هدف آوردن کارمندان پلیس به آدرسی هدف گرفته‌شده.[3] در سال‌های اخیر، بسیاری از این جوامع توسط گروه‌های تندرو رادیکالیزه شده‌اند تا «افکار سفیدبرترانگار، اسلام هراسی، و زن‌ستیزی را از طریق کنایه و دانشِ فرهنگ اینترنت گسترش دهد»، همان‌طور که محققان آلیس مارویک[4] و ربکا لوئیس[5] مستند کرده‌اند.[6]

در زمینه انتخابات ریاست‌جمهوری سال ۲۰۱۶ ایالات متحده، بسیاری از این جوامع درگیر کارزارهای هماهنگ‌شده‌ای شدند که درگیرِ گسترش اطلاعات کاذب سیاسی بودند. این موضوع شامل ترویج نظریه‌های توطئه‌ای بود که [طبق آن] جورج سوروس[7] در کارزاری در سطح ملی که بودجه اعتراض‌های علیه ترامپ را تأمین می‌کرد مشارکت داشت، و همچنین ترویج ادعاهایی که [طبق آن‌ها] ست ریچ،[8] کارمند کمیته ملی مردم‌سالارانه[9] (DNC)، به عنوان بخشی از تلاش‌ها برای پنهان کردن نشت ایمیل‌هایی از DNC در ۲۰۱۶، ترور شد.[10] در واقع، این کارزارها از تلاش‌های داوطلبان، ائتلاف غیررسمی و با هماهنگی ضعیف از گروه‌ها «راست‌گرای جایگزین»[11] دارای هم‌پوشانی استفاده می‌کرد. این موضوع طیف گسترده‌ای از عاملان، از جمله جوامع بازیکن‌ها، کاربران بحث برخط محبوب ردیت،[12] اعضای جامعه سفیدبرترانگار استرمفرانت،[13] و مجاری

1. Coleman 2015
2. Swatting
3. North 2017
4. Alice Marwick
5. Rebecca Lewis
6. Marwick and Lewis 2017; Schreckinger 2017
7. George Soros
8. Seth Rich
9. Democratic National Committee
10. Dreyfuss 2017
11. alt-right مخفف راست جایگزین. یک گروه راست‌گرای افراطی در آمریکا که از ملی‌گرایی سفیدپوستانه دفاع می‌کند. م .
12. Reddit
13. Stormfront

خبری «راست‌گرای جایگزین»[1] را، که برخی از پیام‌های راست افراطی را منعکس می‌کنند اما برخی از دیدگاه‌های مناقشه‌برانگیز را حذف می‌کند، دور هم جمع می‌کند.[2] این تکنیک‌ها به طور واضحی برگرفته از تلاش‌های «ترول‌گرانه»[3] بود. همان‌طور که مایک سرنوویچ،[4] یکی از چهره‌های برجسته «راست‌گرای جایگزین» که در هر دو کارزار قبلی علیه فمینیست‌ها در صنعت بازی ویدیویی و همچنین در انتخابات ۲۰۱۶ شرکت داشت، بیان می‌کند «تاکتیک‌های ترول» وسیله‌ای برای «ساختِ برند[ش]» بودند.[5]

مشارکت این جوامع در کارزارهای هدفمند اطلاعات کاذب سیاسی، این نکته مهم را برجسته می‌کند که این سه منبع - دولتی ، مالی ، و ترول مجازی - به طور مستقل عمل نمی‌کنند. بلکه، پیوندهای بی‌شماری این موتورهای اطلاعات کاذب برخط را به یک زیست‌بوم گروه‌های متداخل و گهگاه همکار بدل می‌کنند. به طور قابل توجهی، تلاش‌های دولتی با هماهنگی روسیه، از عواملِ وابسته به پول که به نوبه خود برای نفوذ و بسیج جوامع برخط برای گسترش اطلاعات کاذب سیاسی تلاش می‌کردند استفاده حداکثری کرد.[6] به همین ترتیب، تلاش‌های دولتی همچنین به انواع کانال‌های رسانه‌ای که با انگیزه مالی برای انتشار «اخبار جعلی» و اطلاعات نادرست از طریق وب عمل می‌کنند یارانه می‌دهد و آن‌ها را پشتیبانی می‌کند.[7] [البته] این گروه‌ها به تنهایی نیز فعالیت می‌کنند و به دلایل خاص خود مستقلاً نیز برای توزیع اطلاعات کاذب وارد عمل می‌شوند.

تأثیر (مبهم) اطلاعات کاذب برخط

در حالی که تمام فعالیت‌های بحث شده در این بخش به‌خوبی مستند است،

1. “alt-light»
2. Marwick and Lewis 2017, p. 26
3. Trolling
4. Mike Cernovich
5. Marantz 2016
6. Kosoff 2017
7. Belford, Cvetkovska, Sekulovska, and Dojc ˇinovic´ 2017

توجه به این نکته مهم است که، در زمان نگارش این متن، هنوز شواهد تجربی واضح از تأثیر واقعی آنها بر نتایج سیاسی روشن نیست. در حالی که برخی از محققان به این نتیجه رسیده‌اند که تلاش برای ایجاد اطلاعات کاذب در انتخابات ریاست‌جمهوری ۲۰۱۶ آمریکا تأثیر داشته است، این موضوع همچنان محل بحث علمی است.[1] با توجه به مشاهده‌پذیری محدودِ فعالیت‌های اطلاعات کاذب مختلف و داده‌های مربوط به مشارکت سیاسی کلی در رسانه‌های اجتماعی و سایر سکوها، احتمالاً این مسئله برای مدتی مبهم باقی بماند.

اگر واقعاً مؤثر باشند، خطر بالقوه آن‌ها برای نهادها و فرایندهای مردم‌سالار روشن به نظر می‌رسد. توانایی قدرت‌های خارجی برای دستکاری مؤثر گفتمان سیاسی در داخل یک کشور سؤالات دشواری را در مورد نمایندگی مقامات منتخب و تصمیمات گرفته شده توسط آنها ایجاد می‌کند. تا آنجا که اطلاعات کاذب زیادی که در طول کارزار انتخاباتی ریاست‌جمهوری ۲۰۱۶ ایالات متحده دیده شد بر تشدید درگیری‌های سیاسی و تقویت قطب‌بندی متمرکز بود، این فعالیت‌ها همچنین ممکن است توان مردم‌سالاری‌ها را برای عملکرد مؤثر در جهت سازش بین اقشار جامعه از بین ببرد.[2] با این حال شواهد در این جهت مبهم است. مشخص نیست که اینترنت در حقیقت در حال افزایش قطب‌بندی است یا نه.[3] علاوه بر این، مشخص نیست که آیا رسانه‌های جناح‌گرایانه بیشتر باعث دو قطبی شدن جامعه می‌شوند یا نه.[4]

اما صرف نظر از مؤثر بودن یا نبودن آن‌ها، این فعالیت‌های هدفمند سیاسی - و دانش عموم در مورد آنها - همچنان ممکن است سلامتی فرایندهای مردم‌سالارانه را تهدید کند. کارزارهای اطلاعات کاذب ممکن

1. Howard and Kollanyi 2017; Kollanyi, Bradshaw, and Neudert 2017
2. Epstein and Graham 2007
3. Boxell . Gentzkow and Shapiro 2017
4 Prior 2013

است در اعتماد عمومی به نهادهایی که برای حفظ مردم‌سالاری حیاتی‌اند لطمه وارد کند. اول از همه شک و تردید در مورد صحت اطلاعات برخط به طور کلی ممکن است تأثیر کانال‌های روزنامه نگاری تولید و توزیع اطلاعات دقیق را نیز محدود کند.[1] این ممکن است در توانایی مردم‌سالاری‌ها برای درگیر شدن در تامّل مؤثر و اصیل و رسیدن به تصمیم‌هایی که «مشروع» در نظر گرفته می‌شوند، ایجاد مانع کند.[2]

ثانیاً، صرف نظر از اثربخشی بالفعل، تلقی عمومی گسترده مبنی بر اینکه این کارزارهای اطلاعات کاذب واقعاً مؤثر هستند، خود می‌تواند باعث ایجاد بی‌اعتمادی نسبت به مشروعیت مقامات منتخب، خصوصاً افراد مورد حمایت دولت‌ها و منافع خارجی شود. این موضوع در مورد عواقبِ کارزار سال ۲۰۱۶، با پرس‌وجوهای متعدد کنگره و تحقیقات ویژه‌ی در حال انجام که گواه ادامه نگرانی‌های سیاست‌گذاران و عموم مردم است، صادق بوده است.

اگرچه هنوز ابهام وجود دارد، این خطرات و سایر موارد باعث ایجاد بحث زنده در مورد مجموعه پاسخ‌ها – تنظیم‌گرانه یا سایر موارد – شده است که برای مبارزه با این فعالیت‌ها و محدود کردن تأثیر بالقوه آنها بر رسانه‌ها و زیست‌بوم اطلاعات مورد نیاز است. این پیشنهادها با چهارچوب CDA ۲۳۰ مواجه‌اند.

1. Barthel and Mitchell 2017

۲. برای مرورِ نظریه‌های مردم‌سالاری که مبتنی بر نقش تامل اند، به‌طور کلی نگاه کنید به Dryzek (2002) و همچنین ببینید Arendt (1971).

بخش دوم


۲۳۰ CDA چگونه تلاش‌ها برای مبارزه
با اطلاعات کاذب سیاسی برخط
را شکل می‌دهد؟

بخش دوم

CDA ۲۳۰ چگونه تلاش‌ها برای مبارزه با اطلاعات کاذب سیاسی برخط را شکل می‌دهد؟

به دلیل تهدید بالقوه اطلاعات کاذب سیاسی برای فرایندها و نهادهای مردم‌سالارانه، سیاست‌گذاران و محققان شروع به ارائه طیف وسیعی از پاسخ‌های قانونی و تنظیم‌گرانه نسبت به این سنخ از اطلاعات کاذب برخط کرده‌اند. همان‌طور که در سایر زمینه‌ها نیز این‌گونه است، توجه به سمت نقش اصلی سکوهای برخط در میزبانی و تسهیل فعالیت‌های آزاردهنده معطوف شده است.[۱] یک بررسی اخیر در مورد رسانه‌های برخط و رفتار به اشتراک‌گذاری در فصل انتخابات ۲۰۱۶ به این نتیجه رسیده که «اطلاعات کاذب و پروپاگاندا ریشه در جناح‌گرایی دارد و بیشتر در شبکه‌های اجتماعی دیده می‌شود».[۲] مشخصاً، این مطالعه نشان داد که مجموعه‌ای از وب‌سایت‌ها که به میزان غیرمتناسبی در فیسبوک مورد توجه قرار می‌گیرند همچنین توسط منابع مستقل و گزارش رسانه‌ای به عنوان سازندگان و توزیع کنندگان «گزارش نادقیق اگر نه آشکارا غلط» ذکر شده‌اند.[۳]

در طیف وسیعی از موضوعات، این سکوها به عنوان «جلوگیری کننده‌ها با کمترین هزینه» عمل می‌کنند - یعنی عاملانی‌اند که برای مدیریت ریسک ناشی از فعالیت‌های مشخص در بهترین موقعیت قرار دارند. در زمینه اطلاعات کاذب برخط، سکوها دارای اطلاعات بسیار ریز در

۱. برای بررسی‌ای اولیه درباره نقشی که سکوهای مختلف در توزیع اطلاعات کاذب ایفا کرده اند نگاه کنید به Feingold et al. (2017).

2. Faris et al. 2017

3. Faris et al. 2017, p. 15

مـورد فعالیت در سراسـر خدمات خود هسـتند و توانایی تأثیرگـذاری بر توزیع محتـوا را دارنـد. ایـن ممکن اسـت به صـورت الگوریتمی با اصلاح سـامانه‌های توصیه‌گـر کـه محتـوای خاصـی را نسـبت به سـایرین ترویـج می‌کننـد انجام شـود یـا از طریـق مالـی، یعنـی بـا ممنوعیـت تبلیغاتی کـه از انـواع خاصی از محتـوای برخـط پشـتیبانی می‌کننـد، انجـام گیـرد. در مورد سـکوهای بزرگ ماننـد گـوگل و فیسـبوک، شـرکت‌ها همچنیـن دارای منابـع و صلاحیت فنی بـرای ایجـاد مؤثـر سـامانه‌های مؤثر تشـخیص و کاهش مشـکل‌اند.[1]

بـدون همـکاری این سـکوها، پیشـنهادها بـرای مواجهه بـا اطلاعات کاذب سیاسـی بـا چالشـی کلی‌تر و مکـرر درباره چگونگـی اعمال برخط خط‌مشـی، یعنـی چالـش شناسـایی و پیگیـری عامـلان خاصـی کـه قوانیـن را نقـض می‌کنند، مواجه اسـت.[2] قوانینی که توسـط مرتکبان اطلاعات کاذب سیاسـی برخـط شکسـته می‌شـود، و قوانیـن جدیـدی کـه ممکن اسـت علیـه این نوع فعالیت‌هـا تصویـب شـود، احتمـالاً بـا توجه بـه الزامـات پرهزینه شناسـایی و اجـرای قوانین علیه یک زیسـت‌بومِ متفـرق و در حال رشـدِ مرتکبان اطلاعات کاذب محـدود خواهـد ماند.

تـا آنجـا کـه اقدامـات قانونـی و تنظیم‌گرانـه بـه دنبـال ایجـاد انگیزه‌هایی بـرای سـکوهای برخـط برای مقابله بـا اطلاعات کاذب سیاسـی برخط خواهند بـود، ایـن تلاش‌هـا در سـایه CDA ۲۳۰ انجـام می‌شـود، کـه بـرای سـکوها سـپری محکـم فراهـم می‌کنـد تـا از مسـئولیت در قبـال اقدامات انجام‌شـده توسـط کاربرانشـان محفـوظ باشـند. این مـاده‌ی قانونی تا حدی مانـع از تأثیر اهرم‌هـای قانونـی موجود و جدیدی اسـت کـه اطلاعات کاذب سیاسـی برخط را هـدف قـرار می‌دهد.

دو مسیر باقی می‌ماند که طبق آنها اقدامات قانونی ممکن است با این کارزارها

۱. ایـن تصـور اغلـب توسـط پروژه‌هایـی کـه خـود شـرکت‌ها راه‌انـدازی کرده‌انـد تقویـت می‌شـود کـه شـامل سیسـتم هایـی ماننـد YouTube's Content ID (www.youtube.com/watch?time_continue= 2&v=9g2U12SsRns) اسـت کـه تشـخیص نقـض IP را بـه صـورت خـودکار انجـام می‌دهـد. ایـن موضـوع همچنیـن شـامل فناوری‌هایـی ماننـد Perspective (www.perspectiveapi.com/) اسـت، محصولی که به طور خودکار نظرات آنلاین «سمی» را تشخیص می‌دهد.

2. Lessig 1999

مبـارزه کنـد در حالـی کـه CDA ۲۳۰ را دسـت نخـورده باقـی بگـذارد. یکی، کـه بـر اسـاس سـابقه قانونـی تعیین‌شـده توسـط حـوزه‌ی نهـم در پرونـده Roommates.com[1] اسـت، دادگاه‌هـا را مجـاز می‌دانـد تـا در تعییـن درجـه‌ای کـه سـکوها می‌تواننـد موجـبِ فعالیـت اطلاعـات کاذب غیرقانونـی شـوند، ورود پیـدا کننـد. دوم، قانون‌گـذاری و مقرراتی اسـت که خود سـکوها را هـدف می‌گیـرد و بـر تغییـر محیـط اطلاعاتی کـه پیرامون اطلاعـات کاذب سیاسـی برخط اسـت تمرکـز دارد و نه بر ایجاد مسـئولیت بـرای عملکردهای خـود سـکوها، کـه ایـن مسـیر نیـز از اصـلاح CDA ۲۳۰ پرهیـز می‌کنـد.

تاریخچه مختصر CDA ۲۳۰

CDA ۲۳۰، کـه در سـال ۱۹۹۶ تصویـب شـد، قیـد می‌کنـد کـه «هیـچ ارائه‌دهنـده یـا کاربـر یـک خدمـت رایانـه‌ای تعاملی نبایسـتی به عنوان ناشـر یـا سـخنگوی هرگونه اطلاعات ارائه‌شـده توسـط یـک ارائه‌دهنـده‌ی محتوای اطلاعاتـی دیگـر در نظر گرفته شـود»، مشـروط بـر مجموعه‌ای از اسـتثناهای مربوط به قوانین مجرمانه، مالکیت فکری، دولتی، و حریم خصوصی ارتباطات.[2]

ایـن قانـون در واکنـش بـه تصمیـم اسـتراتون اکمونـت درمقابـل پرادجی سرویسـز[3] تصویـب شـد، تصمیمـی در سـال ۱۹۹۵ کـه پیشـنهاد می‌کـرد ارائه‌دهنـدگان خدمـت برخـط در قبـال محتوای افتراآمیز ارسال‌شـده توسـط کاربـران بـر روی سـکوهای خـود تـا حدی که آنهـا از نظـر ویراسـتاری بر آن محتـوا کنتـرل داشـته باشـند، مسـئول باشـند.[4] ایـن تصمیم عملیاتی شـدن اصـول قانون عرفی[5] تثبیت‌شـده پیرامون مسـئولیت توزیع‌کنندگان و ناشـران را نشـان مـی‌داد. تحـت ایـن چهارچـوب، «توزیع‌کنندگانـی» که بـر محتوای توزیع‌شـده خـود - از جملـه کتاب‌فروشـی‌ها و کتابخانه‌هـا - نظـارت تحریری

1. the Ninth Circuit in the Roommates.com case
2. 47 U.S.C. § 230
3. Stratton Oakmont v. Prodigy Services
۴. نگاه کنید به Stratton Oakmont, Inc. v. Prodigy Services Co., 1995 WL 323710 (N.Y. Sup. Ct. 1995).
۵. Common law. مجموعه‌ای از قوانین نانوشته مبتنی بر اصول حقوقی که توسط دادگاه‌ها تعیین می‌شود. م.

محـدودی اعمـال می‌کردنـد، در صـورت اطـلاع از مطالـب و عـدم حـذف آن، در برابر افترا مسـئولیت داشـتند. در مقابل، «ناشـرانی» که از نظر ویراسـتاری کنتـرل و قضـاوت فعال‌تری داشـتند - مانند روزنامه‌ها و مجلات – مسـتقل از دانسـتن محتوا مسـئول محتوای افتراآمیز محسـوب می‌شـدند، انگار که آن‌ها آن محتـوا را در اصـل منتشـر کرده بودند.[1] اسـتراتون اکمونـت نگرانی‌هایی را مطـرح کـرد که سـکوها اگـر در معرض مسـئولیت اعمـال هر یـک از کاربران باشـند، پایـدار نخواهنـد مانـد و از انجام اقدامات پیشـگیرانه بـرای فیلترکردن محتـوای توهین‌آمیـز بـاز می‌مانند.[2]

بـرای ایـن منظـور، انگیزه اصلـی CDA ۲۳۰، همان‌طور که عنوانش نشـان می‌دهـد، محافظـت از سـکوها در قبـال مسـئولیت اقدامات «سـامری نیکو»[3] بـرای حـذف محتـوای توهین‌آمیـز بـود.[4] بـا ایـن حـال، کنگـره همچنین در تصویـب CDA ۲۳۰ اهـداف دیگـری داشـت، از جمله هدف «ترویجِ پیشـرفت مسـتمر اینترنت و سـایر خدمات رایانه‌ای تعاملی و سـایر رسـانه‌های تعاملی» و «حفـظ بـازار آزاد پـر جنـب و جـوش و رقابتـی کـه در حـال حاضـر بـرای اینترنـت و سـایر خدمـات رایانـه‌ای تعاملـی وجـود دارد، کـه توسـط مقـررات فـدرال یـا ایالت محدود نشـده اسـت.»[5]

طـی دو دهـه بعـد، دادگاه‌هایـی کـه CDA ۲۳۰ را بررسـی می‌کردند، این آمـوزه را بـرای محافظت از سـکوهای برخط در قبال طیف وسـیعی از اقدامات انجـام شـده توسـط کاربـران آنهـا تفسـیر می‌کردنـد.[6] در سـال ۱۹۹۷، حوزه چهـارم در زران درمقابـل امریکـن آنلایـن[7] نتیجه گرفت کـه CDA ۲۳۰ برای محافظت سـکوها در برابر هر دو دسـته سـنتی مسـئولیت ناشـر و توزیع‌کننده

1. Id.
2. Reidenberg et al. 2012, pp. 6–5
3. Good Samaritan Acts.
قانونی که به افرادی که به یک شخص در شرایط اضطراری کمک می‌کنند مصونیت قضایی اعطاء می‌کند. م.
4. Reidenberg et al. 2012, p. 7
5. 47 U.S.C. § 230(a).
6. For a general review of leading cases in this space, see Goldman (2017).
7. Zeran v. American Online

عمل می‌کند، و در نتیجه استدلال شاکیان مبنی بر اینکه این ماده فقط برای جلوگیری از مسئولیت ناشر است را رد کرد.[1] در سال ۲۰۰۳، حوزه نهم در باتزل درمقابل اسمیت[2] به این نتیجه رسید که عبارت «خدمات رایانه‌ای تعاملی» در CDA ۲۳۰ محدود به خدماتی که دسترسی به اینترنت را فراهم می‌کنند، در زران و پرونده‌های قبلی، نیست بلکه «هرگونه خدمت اطلاعاتی یا سایر سامانه‌ها» مانند لیست‌سرو[3] را نیز شامل می‌شود.[4] پرونده‌های بعدی نیز تأیید کردند که کاربرانی که مستقل از یک ارائه‌دهنده خدمات برخط بودند به حمایتِ CDA ۲۳۰ می‌توانستند استناد کنند. در سال ۲۰۰۸، حوزه پنجم در دو درمقابل مای‌اسپیس[5] دریافت که مصونیت CDA ۲۳۰ به طور گسترده‌ای برای دعاوی خطای مدنی،[6] و نه فقط مواردی که همانند تصمیم استراتون اکمونت صرفاً متکی به افترا بودند، اعمال می‌شود. این نگاه گسترده به CDA ۲۳۰ یک سال بعد توسط حوزه نهم در بارنز درمقابل یاهو[7] دنبال شد.[8] در آن پرونده، حوزه نهم روشن کرد که دامنه CDA ۲۳۰ می‌تواند فراتر از علل دعوی[9] که خطای مدنی به نظر می‌رسد باشد و هر علت دعوی را که «اساساً دادگاه را ملزم می‌کند که با متهم به عنوان «ناشر یا سخنگوی» محتوای ارائه شده توسط دیگری برخورد کند»، شامل شود.[10]

در مجموع، این تصمیمات CDA ۲۳۰ را به عنوان سپر گسترده‌ای برای واسطه‌های برخط تثبیت کرده و حیطه گزینه‌های قانونی موجود را در مبارزه با اطلاعات کاذب تحت تأثیر قرار داده است.

1. Zeran v. American Online, Inc., 129 F.3d 4) 32th Cir. 1997).
2. Batzel v. Smith
3. Listserv
روشی برای ارسال گروهی ایمیل. م .
4. Batzel v. Smith, 333 F.3d 9) 1018th Cir. 2003).
5. Doe v. MySpace
6. tort claims
7. Barnes v. Yahoo!
8. Barnes v. Yahoo!, 570 F.3d 9) 1096th Cir. 2009).
9. Causes of action.
مجموعه‌ای از حقایق که پیگرد قانونی توسط یک شخص علیه شخص دیگر را موجه می‌سازد.
10. Id. at 1102.

CDA ۲۳۰ سکوها را از اقدامات اطلاعات کاذب برخط که توسط کاربران انجام شده محافظت می‌کند

CDA ۲۳۰ و تأثیرات آن بحث‌برانگیز بوده است و این ماده قانونی هدف تلاش‌های مکرر برای اصلاح آن به روش‌های مختلف باقی مانده است.[1] در زمینه اطلاعات کاذب سیاسی برخط، CDA ۲۳۰ با تلاش‌ها برای استفاده از علل دعوی فعلی و ایجاد علل دعوی جدید که سکوها را مسئول اقدامات غیرقانونی کاربران خود می‌دانند در تعارض است.

تعدادی از علل دعوی که بالقوه قابل اعمال‌اند وجود دارد. اطلاعات کاذب سیاسی برخط غالباً اطلاعاتی نادرست درباره یک فرد است و به همین منظور ممکن است موجب خطای مدنیِ افترا و وهن شود. این موارد ممکن است شامل فعالیت‌هایی برای گسترش نظریه‌های توطئه مانند شایعه قاچاق رابطه جنسی «پیتزاگیت» شود که در بخش «اطلاعات کاذب توسط عاملان دولتی» بحث شد.[2] سازگار با مواردی که در بخش «تاریخچه مختصر CDA ۲۳۰» بحث شد، CDA ۲۳۰ مانع از آن می‌شود که یک سکوی برخط که چنین محتوای افتراآمیزی که توسط یک کاربر ارسال شده را میزبانی می‌کند، مسئول افترا باشد.[3]

اطلاعات کاذب سیاسی برخط همچنین ممکن است تعدادی دیگر از قوانین را که موارد کمتر الگویی[4] برای CDA ۲۳۰ است نیز نقض کند. به عنوان مثال، طبق قانون فدرال، ملیت‌های خارجی از «هرگونه مشارکت یا کمک مالی یا چیزهای با ارزش دیگر یا هر گونه هزینه‌کرد، هزینه مستقل یا پرداخت در رابطه با هر انتخابات فدرال، ایالتی یا محلی در ایالات متحده» منع شده‌اند.[5] این شامل

1. Reidenberg et al. 2012, pp. 49-46، همچنین نگاه کنید به Allow States and Victims to Fight Online Sex Trafficking Act of 2017, Pub. L. No. 132 ,164-115 Stat. 2018) 1253).
2. Robb 2017
۳. نگاه کنید مثلا به Zeran v. American Online, Inc., 129 F.3d 32 (4th Cir. 1997).
4. less prototypical
5. 52 U.S.C. § 30121. See also, 11 CFR 110.20.

تلاش‌های عاملان خارجی برای دخالت در انتخابات ایالات متحده از طریق خرید تبلیغاتِ غلط‌پراکن در مورد یک نامزد بخصوص است. دادگاه‌هایی که غیرقانونی بودن تبلیغات را در شرایط فراتر از زمینه انتخابات بررسی می‌کنند، به طور کلی از تحمیل مسئولیت به سکوهایی که میزبان این مطالب‌اند، امتناع ورزیده‌اند، فارغ از برخی موارد خاص که به قضاوت[1] در Roommates.com اعمال شد که در بخش «گزینه اول: تنظیم‌گری مبتنی به دادگاه از طریق CDA ۲۳۰» بحث شده‌اند.[2] بر این اساس، اقدامات سازمان‌هایی چون کمیسیون انتخابات فدرال برای اجرای این قوانین علیه سکوها با محدودیت‌های CDA ۲۳۰ روبرو می‌شود.[3]

علل دعوی جدید نیز احتمالاً با موانع مشابهی روبروست. در پی انتخابات ریاست‌جمهوری سال ۲۰۱۶، قانون‌گذاران ایالت کالیفرنیا لایحه‌ای را پیشنهاد کردند که این را غیرقانونی می‌دانست که «یک شخص با آگاهی و تمایل خود در یک وب‌سایت اینترنتی . . . عبارتی غلط یا فریبنده تولید، منتشر یا ترویج کند که آن عبارت طراحی شده است برای تأثیرگذاری در فرایند رأی‌گیری بر . . . (الف) هر موضوعی که در انتخابات به رأی‌دهندگان گفته یا پیشنهاد می‌شود، (ب) هر کاندیدِ انتخاب منصب عمومی.»[4] فراتر از طیفی از چالش‌های ناشی از متمم اول[5] به قوانینی که تلاش برای غیرقانونی کردن ایجاد یا گسترش اطلاعات کاذب سیاسی داشتند، CDA ۲۳۰ همچنان برای جلوگیری از اعمال‌پذیری آن قوانین بر سکوها عمل

1. Holding

۲. نگاه کنید به Jane Doe No. 1 v. Backpage.com, LLC, 817 F.3d 12 (1st Cir. 2016) (ads for prostitution); Chicago Lawyers' Committee for Civil Rights under the Law v. Craigslist, 519 F.3d 666 (housing ads violating the Fair Housing Act)).

3. Federal Election Commission

۴. نگاه کنید به Federal Trade Commission v. Accusearch, Inc., 570 F.3d 1187 (10th Cir. 2009) (suits by an agency to enforce federal law still subject to CDA 230 analysis)).

5. First Amendment

می‌کند.[1]

تأثیر این محدودیت‌ها با نقدهای طولانی‌مدتِ CDA ۲۳۰ هم‌راستاست. منتقدان از زمان تصویب آن استدلال می‌کنند که سپر فراهم‌شده توسط CDA ۲۳۰ باعث می‌شود سکوهای برخط در مقایسه با حالتی که این سپر وجود نداشت در برخورد با محتوای افتراآمیز، کمتر پاسخگو و فعال‌اند.[2] در مواردی که اطلاعات مربوط به ارتکاب شونده افترا کم است، ممکن است قربانیان افترا بدون راه‌های کافی برای بهبودی باقی بمانند.[3] بحث‌هایی مشابه در چهارچوب اجرای قوانینی علیه آزار و اذیت در فضای سایبر انجام شده است.[4] این چالش در مواردی که مرتکبان این فعالیت، همانند انتخابات ریاست‌جمهوری سال ۲۰۱۶ ایالات متحده، در خارج از ایالات متحده فعالیت می‌کند ممکن است وخیم‌تر شود.

باید توجه داشت که CDA ۲۳۰ فقط برای جلوگیری از طرح نوعی شکایت علیه سکو تلاش می‌کند که آن شکایت سکو را مسئول بداند، طوری که انگار آن سکو انتشاردهنده محتوای افتراآمیز است. حتی اگر نمی‌توانست مانع از مسئولیت سکو شود، این واقعیت که بسیاری از اقدامات اطلاعات کاذب سیاسی انواع مختلف چهره‌های عمومی را هدف قرار می‌دهد، می‌تواند به این معنی باشد که ادعاهایی مانند افترا و وهن ممکن است تا حالا ابزارهای قانونی نسبتاً ضعیفی برای اعمال باشند. به عنوان مثال، حتی بدون CDA ۲۳۰، یک شکایت موفق توسط شخصیتی عمومی باید مطابق با استاندارد تعیین شده تحت نیویورک‌تایمز کو. مقابل سولیوان[5] باشد، که مستلزم اثبات

۱. نگاه کنید به California A.B. 1104 Opposition Letter, Electronic Frontier Foundation (2017), opposition-letter. This notes a number of First-1104-www.eff.org/document/california-ab Amendment challenges to this type of legislation

2. Reidenberg et al. 2012, p. 26; Brown-Barbour 2015

۳. برای مروری بر ادبیات وسیع درباره این موضوع، نگاه کنید به Reidenberg et al. (2012), pp. 29–31.

۴. نگاه کنید به Reidenberg et al. (2012), pp. 26-27; Jeong (2015).

5. New York Times Co. v. Sullivan

«سوء نیت بالفعل» است. این یک وظیفه چالش‌برانگیز است که مستلزم این است که شاکیان نشان دهند که این عمل با «شواهد کافی برای رسیدن به این نتیجه که متهم در واقع در مورد صدق آنچه منتشر کرده است در شک و تردید جدی بوده» انجام شده است.[1]

حتی با توجه به محدودیت‌های اعمال شده توسط CDA ۲۳۰، تأکید این نکته مهم است که قانون در عمل مانع از همه مداخلات قانونی یا تنظیم‌گرانه که می‌تواند سکوها را در جهت مبارزه با اطلاعات کاذب سیاسی برخط تشویق کند نیست. دو مسیر زمینه بالقوه‌ای را برای تغییر وضعیت بازی در اطراف این موضوع فراهم می‌کند.

گزینه یک: تنظیم‌گری دادگاه - محور از طریق CDA ۲۳۰

از زمان زران، دادگاه‌ها پیوسته دریافته‌اند که CDA ۲۳۰ محافظت‌هایی گسترده در برابر مسئولیت‌های سکوهای برخط برای فعالیت‌های کاربران خود فراهم می‌کند. با این حال، مجموعه‌ای از پرونده‌ها حاکی از آن‌اند که، تحت شرایط خاص، دادگاه‌ها مایل‌اند دامنه اعمالِ سپر فراهم‌شده توسط CDA ۲۳۰ را محدود کنند.

شورای اسکان منصفانه‌ی دره سانفرانسیسکو در مقابل Roommates.com[2] به ادعایی علیه وب‌سایتی مربوط بود که خدمتِ متصل کردن اجاره‌کننده‌های بالقوه به آپارتمان‌ها و اتاق‌های باز را فراهم می‌کرد.[3] شاکیان پرونده ادعا کردند که این سکو قانون اسکان عادلانه فدرال (FHA)[4] را با استخراج اطلاعات مربوط به ترجیحات اجاره‌کنندگان در مورد جنسیت، گرایش جنسی و وضعیت خانوادگی، نقض کرده است. با انتشار این ترجیحات و اجازه دادن به کاربران برای انتخاب

1. New York Times Co. v. Sullivan, 376 U.S. 1964) 254).
2. Fair Housing Council of San Fernando Valley v. Roommates.com
3. Fair Housing Council of San Fernando Valley v. Roommates.com, 521 F. 3d 1157.
4. The federal Fair Housing Act

اجاره‌کنندگان بر اساس این معیارها، دعویِ نقض قیود FHA مطرح شد که تبعیض توسط مالکان و مستأجران را منع می‌کرد. [مسئولان وب‌سایتِ] Roommates.com به CDA ۲۳۰ استناد کردند، با این استدلال که این اتهام سکو را به عنوان مشارکت‌کننده در فعالیت تبعیض‌آمیز تلقی می‌کند.

حوزه نهم - با اتخاذ منطقی مشابهِ حوزه هفتم - معتقد بود که Roommates.com از CDA ۲۳۰ مصونیت دریافت نمی‌کند زیرا نقش «ارائه دهنده محتوای اطلاعات» را داشته.[1] با طراحی یک فرایند ثبت نام در وب‌سایت که شامل سؤالاتی در مورد دسته‌بندی‌هایی مانند جنسیت و گرایش جنسی است و ارائه خدماتی که بر اساس این گرایشات فیلتر می‌شود، دادگاه اعلام کرد که Roommates.com «به طور عمده در رفتار غیرقانونی» مشارکت داشته.[2]

نتیجه‌ی نهایی قضاوت درباره Roommates.com این است که تصمیماتِ طراحی خاص ایجاد شده در یک وب‌سایت می‌تواند در تعیین این‌که آیا آن وب‌سایت تحت CDA ۲۳۰ می‌تواند مصونیت داشته باشد یا خیر مؤثر باشد. قابل توجه است که حوزه نهم ادعای شاکیان را مبنی بر اینکه سکو باید در قبال پست‌های تبعیض‌آمیز توسط کاربران در فیلد متنی «نظرات اضافیِ» اختیاری و بدون محدودیت در قسمت پروفایل‌های کاربر مسئول باشد رد کرد.[3] از آنجا که Roommates.com نوع خاصی از محتوا را در این فیلد متنی تقاضا نکرده و آنها را به همان صورت که نوشته شده منتشر کرده است، ایجادکننده محتوا نبوده و بنابراین مصونیت CDA ۲۳۰ را برای آن فعالیت‌ها دریافت کرده است.[4]

1. Quist 2012
2. Roommates.com, 521 F.3d at 1168.
3. Id. at 1175–1173.
4. Id. at 1175.

قضاوت در مورد Roommates.com در سال‌های پس از حکم به طور ناسازگاری در سراسر حوزه‌های قضایی اعمال شده است، و باعث شده برخی از محققان اظهار کنند که این پرونده به لحاظ قانونی حل نشده است و در واقع به اصطلاح دارای «میراث صفحه شطرنجی»[1] است.[2] حوزه دهم در افتی‌سی در مقابلِ اکوسرچ[3] این استدلالِ ارائه شده درباره Roommates.com در سال ۲۰۰۹ را برگرفت، و در نتیجه چنین دریافت که سایتی که سوابق تلفنیِ به نحو غیرقانونی به دست آمده را می‌فروشد، از مصونیت CDA ۲۳۰ برخوردار نیست، زیرا آن سایت «بخصوص توسعه آنچه درباره محتوا توهین‌آمیز [بوده] را [تشویق کرده]».[4] در مقابل، قانون‌گذاری مربوط به Roommates.com توسط حوزه اول در دو در مقابل بک‌پیج،[5] در سال ۲۰۱۶ به یک سایت انتشار آگهی‌های مربوط به روسپی‌گری اجازه داد مصونیت CDA ۲۳۰ را به دست آورد، با اشاره به این‌که تصمیمات یک سکوی برخط در «ساختار]مند[کردن وب‌سایت و الزامات پست گذاشتن در آن از کارهای ناشر است که از محافظت بخش ۲۳۰(c) (۱) برخوردار است».[6] به نظر می‌رسد چنین استدلالی به شکل قابل‌توجهی حکم مربوط به Roommates.com را محدود می‌کند.[7] این قاعده‌گذاری‌های متفاوت، تردیدهایی را در مورد اینکه آیا سابقه‌ی قانونی موجود مبنایی پایدار برای مبارزه با اطلاعات کاذب سیاسی برخط خواهد بود، برمی‌انگیزاند.[8]

1. Checkered legacy.
یعنی به صورت یکنواخت و سازگار در گذشته وجود نداشته و به طرق متفاوتی با آن رفتار شده‌است. م.
2. Goldman 2017, p. 2
3. FTC v. Accusearch
4. Federal Trade Commission v. Accusearch, Inc., 570 F.3d 10) 1199 ,1187th Cir. 2009)
5. Doe v. Backpage
6. Jane Doe No. 1 v. Backpage.com, LLC, 817 F.3d 1) 22 ,12st Cir. 2016).
۷. باید توجه کرد که قانونی در جهت معکوس حکم بک‌پیج به تصویب رسیده است. نگاه کنید به
Allow States and Victims to Fight Online Sex Trafficking Act of 2017, Pub. L. No. ,164-115 132 Stat. 2018) 253).
8. Feuerman 2016

با این وجود، قضاوت Roommates.com، در صورت اعمال، اظهار می‌کند که - حتی بدون اصلاح قانون - مصونیت‌های ارائه‌شده توسط CDA ۲۳۰ ممکن است به طور مؤثر توسط دادگاه‌های ارزیابی‌کننده‌ی اینکه آیا فعالیت‌های مرتبط با کارزارهای اطلاعات کاذب سیاسی باید مسئولیتی را متوجه سکوهای برخط کند یا خیر محدود شود. این موضوع محل بحث است که آیا طراحی خاص سکو آن را «به طور کامل یا جزئی برای ایجاد یا توسعه» محتوای توهین‌آمیز «مسئول کرده است» یا نه.[1] در حالی که این پرسشی است که به ادعایی خاص، خدمت مورد بحث، و نوع فعالیت اطلاعات کاذب، وابسته خواهد بود، پرونده [Roommates.com] برخی از رهنمودهای کلی درباره آنچه ممکن است نامصون از مزایای CDA ۲۳۰ باشد را ارائه می‌دهد.

در پایه‌ای‌ترین سطح، تحت قضاوتِ Roommates.com بعید به نظر می‌رسد که صرفاً به‌خاطر فراهم‌کردن فضایی که از طریق آن اقدامات غیرقانونی پیرامون اطلاعات کاذب سیاسی صورت گیرد، سکوها در معرض مسئولیت قرار گیرند. ایجاد یک جعبه برای پست‌کردن محتوای نامحدود به معنی همراهی در توسعه [ی آن محتوا] نیست، که این به Roommates.com این امکان را داد که حداقل برای برخی عناصر سکو خود از CDA ۲۳۰ بهره‌مند شود. با این حساب، به احتمال زیاد در دسترس قرار دادن ابزارهای پست‌کردن - حتی اگر توسط ترول، بات‌ها و عوامل خارجی برای انتشار اطلاعات کاذب استفاده شود - نکته‌ای خواهد بود که سکوها می‌توانند از آن طریق مصونیت خود را حفظ کنند.

1. Roommates.com, 521 F.3d at 1174.

با این حال، در صورت در نظر گرفتن سایر ویژگی‌های مشترک درخدمات وب، نتیجه مبهم‌تر است. تا حدی که کارزارهای اطلاعات کاذب از طریق کانال‌های تبلیغاتی ارائه‌شده توسط سکوها انجام می‌شود، ممکن است ادعا شود که شرکت‌هایی مانند فیسبوک و گوگل به طور عمده در امر غیرقانونی سهیم‌اند. پرونده‌هایی که از قضاوت Roommates.com استفاده کردند، گاهی مصونیت مبتنی بر CDA ۲۳۰ را در زمینه تبلیغات رد کرده‌اند. صرف سود بردن از تبلیغاتی که خدمات غیرقانونی را ترویج می‌کنند یا خود غیرقانونی‌اند، به خودی خود برای مسئولیت‌پذیری سکو ناکافی است.[۱] اما ترتیب قیمت‌گذاری‌ای که فعالیت مورد بحث را تشویق کند، می‌تواند به عنوان یک مشارکت عمده در کار غیرقانونی شناخته شود. دادگاه‌ها چند سناریوی احتمالی را در اینجا بیان کرده‌اند، از جمله ارائه تخفیف به تبلیغات مشکل‌دار و ساختارهای متغیر قیمت‌گذاری که متناسب با ارزش و حجم فعالیت غیرقانونی، سود سکو را افزایش می‌دهند.[۲] قیمت‌گذاریِ متغیر واقعیتی برخط است. بیشتر سکوهای بزرگ برای ارائه تبلیغات به سیستم‌های مبتنی بر حراج متکی‌اند، به این شکل که بسیاری از خریداران برای تحویل محتوای خود به یک کاربر معین رقابت می‌کنند.[۳] تاحدی‌که بتوان نشان داد که سکوها به

۱. نگاه کنید مثلا به
Jane Doe No. 1 v. Backpage.com, LLC, 817 F.3d 1) 17 ,12st Cir. 2016)
(مصونیت ناشی از CDA ۲۳۰ وجود دارد حتی زمانی‌که سکو به‌طور خاص برای تبلیغات روسپی‌گری درخواست پول کند.)
۲. نگاه کنید به
Chicago Lawyers' Committee for Civil Rights under the Law v. Craigslist, ۵۱۹ ۳d.F ۶۶۶, ۶۷۲
(که CDA ۲۳۰ را به‌طور بخشی اعمال می‌کند، زیرا سکو «قیمتی پایین‌تر به کسانی‌که گزاره‌های تبعیض‌آمیز در پست‌گذاری‌شان داشته‌اند ارائه نکرده»؛ و
NPS LLC v. StubHub, Inc ,Mass. L. Rptr ۲۵ ,۴۷۸ (Super. Ct. ۲۰۰۹)
(که مصونیت ناشی از CDA ۲۳۰ را به‌طور بخشی رد می‌کند زیرا «عایدی [سکو] در نسبتی مستقیم با قیمت بلیت فروخته‌شده افزایش یافته، در مقابل روزنامه، که به‌طور کلی قیمتی ثابت را درخواست می‌کند.)
3. See, e.g., Google's "About the ad auction – AdSense Help," (https://support.google.com/adsense/answer/160525?hl=en), which explains the Google auction system; see also Facebook's Help Center (www.facebook.com/business/help/430291176997542), which explains the Facebook auction system.

طور سیستماتیک تبلیغاتی را که نقض قانون می‌کنند با نرخ کمتری ارائه می‌دهند، در آنجا به طور بالقوه ادعای مشارکت در نقض قانون مطرح است که مانع استفاده از مصونیت مبتنی بر CDA ۲۳۰ می‌شود.

همچنین، محتوای تولیدشده به نحو الگوریتمی از طریق یک «خوراک»[1] برای کاربران مرتب می‌شود، شکل می‌گیرد و شخصی‌سازی می‌شود.[2] این ممکن است زمینه‌ای برای ایجاد استدلال در مورد همراهی در توسعه [محتوا] باشد، به ویژه هنگامی که این واقعیت را در نظر بگیریم که - در پاسخ به علاقه به یک محتوای منفرد افتراآمیز - سکو ممکن است خود محتوای افتراآمیز بیشتری را توصیه کند. در این معنا، این موضوع با قابلیت جستجو در Roommates.com مطابقت دارد، که در آن ارائه سازوکاری که مطالب را بر اساس معیارهای تبعیض‌آمیز برجسته می‌کند، به‌عنوان تسهیل فعالیت غیرقانونی در نظر گرفته می‌شود، به‌نحوی‌که مصونیت تحت CDA ۲۳۰ را حذف می‌کند.[3] بر اساس موضوعاتی که در زمینه هدف‌گذاری تبلیغات نیز به وجود آمده است، که در آن تولید الگوریتمی معیارهای هدف‌گذاری فعالیت غیرقانونی بالقوه را تسهیل می‌کند، ادعاهای مشابهی نیز ممکن است مطرح شود.[4]

علیرغم این موضوع، Roommates.com همچنین فرصت فراخی برای چهارچوب‌بندی مجدد نحوه ترتیب‌بندی و خلقِ مشترک محتوای موجود در یک خوراک را با نگاهی آسان‌گیرانه‌تر فراهم می‌کند. طبق قضاوت دادگاه، یک «اپراتور وب‌سایت که محتوای ایجاد شده توسط کاربر را ویرایش می‌کند . . . مصونیت خود را برای هرگونه

1. Feed

۲. نگاه کنید به «به خوراک خبری خوش آمدید» فیسبوک (Facebook's, "Welcome to News Feed," https://newsfeed.fb.com/?lang=en)، که این را که سیستم چگونه محتوا را برای کاربران سازماندهی می‌کند مرور می‌کند.

۳. همچنین نگاه کنید به Tremble (۲۰۱۷).

4. Angwin, Varner, and Tobin 2017

غیرقانونی بودن محتوای ایجاد شده توسط کاربر حفظ می‌کند، به‌شرطی که ویرایش‌ها با غیرقانونی بودن ارتباط نداشته باشند» – مثال‌ها شامل ویرایش به خاطر طول نوشته، تصحیح املاء یا از بین بردن فحاشی است.[1] می‌توان نشان داد که سکوهایی چون فیسبوک دقیقاً چنین می‌کنند، محتواها را به هم می‌چسبانند و آنها را همان‌طور که پست شده‌اند نمایش می‌دهند، و در مقابل تغییر معنای واقعی یا «[مشارکت] در امری که ادعاشده غیرقانونی است» را انجام نمی‌دهند.[2]

همچنین خیلی واضح نیست که صرفاً توصیه به محتوای افتراآمیزِ اضافی بر اساس علاقه کاربر به محتوای افتراآمیز، به سطحِ «همراهی در توسعه»[3] برسد. در Roommates.com، دادگاه بر این واقعیت متمرکز بود که این سکو در فیلترکردن و تحویل لیست آپارتمان‌ها به کاربران از معیارهای تبعیض‌آمیز غیرمجاز استفاده کرده‌است. با این حال، دادگاه در تلاش برای تمایز دادن این پرونده از سایر سکوهایی که ممکن است عملکردی مشابه داشته باشند، چنین نظر داد که استفاده از یک «[ابزار] خنثی برای انجام جستجوهای غیرقانونی یا غیرمجاز» در «موتور جستجوی معمولی» خودِ سرویس [سکو] را در معرض مسئولیت قرار نمی‌دهد.[4] در این مورد مستدل به نظر می‌رسد که این گونه نیست که سکویی مانند فیسبوک به صراحت درخواست یا وسوسه‌ای کند و سپس بر اساس محتوای افتراآمیز فیلتری انجام دهد. این موضوع مورد فیسبوک را از طراحی موجود در Roommates.com متمایز می‌کند، که در آن سکو مجموعه‌ای از دسته‌بندی‌های از پیش تعریف‌شده را ارائه

1. Fair Housing Council of San Fernando Valley v. Roommates.com, 521 F. 3d 1169 ,1157.
2. Id.
3. Codevelopment
4. Id.

می‌دهد که خود ویژگی‌های غیرقانونی‌اند و تبعیض ایجاد می‌کنند. در عوض، در سکویی چون فیسبوک، کاربر به طور مؤثر با استفاده از ابزاری خنثی و بر اساس رفتار مرورگرانه خود «جستجو می‌کند»، و خوراک، بدون توجه به موضوع خاص، در پاسخ محتواهایی را متناسب با آن رفتار بر می‌گرداند.

همان‌طور که این تحلیل مختصر برجسته می‌کند، نتیجه نهایی قضاوت Roommates.com مبهم است و بستگی زیادی به سکوی مورد نظر دارد، این انتقادی است که در آن پرونده توسط مخالفان مطرح شد.[1] اما به نظر می‌رسد که در شرایط خاص روشن است که سکوها ممکن است از مزایای مصونیت CDA ۲۳۰ برخوردار نباشند، و به نظر می‌رسد که حداقل ادعایی ظاهراً درست وجود دارد که طبق آن این اجازه وجود دارد که مسئولیت، حداقل برای برخی از تاکتیک‌های استفاده‌شده توسط کارزارهای اطلاعات کاذب سیاسی، بر عهده سکوها باشد.

گزینه دوم: اقدامات قانون‌گذارانه فراتر از اصلاح CDA ۲۳۰

CDA ۲۳۰ به طور هم‌زمان هم قانونی گسترده و هم قانونی محدود است. گسترده است در این معنا که سکوها در برابر مسئولیت طیف وسیعی از اعمال غیرقانونی که ممکن است کاربران آنها مرتکب شوند محافظت می‌شوند. در عین حال، از این نظر محدود است که مانع طیف گسترده‌ای از اقدامات که ممکن است به علاج کارزارهای اطلاعات کاذب سیاسی، خارج از اهرم اعمال مسئولیت سطح کاربر به سطح سکو، بپردازد نمی‌شود. سه پیشنهاد متأخر ارائه‌شده توسط

1. Id. at 1189–1176.

محققـان و سیاسـت‌گذاران بـا تمرکـز بـر ایـن موضـوع، نمونه‌هایـی از انـواع فعالیت‌هایـی کـه از طریـق چهارچـوب تعیین‌شـده توسـط CDA ۲۳۰ و سـابقه قانونیِ تفسـیر ایـن مـاده منـع نشـده اسـت، ارائـه می‌دهـد.

اول، CDA ۲۳۰ مانـع از اعمـال الزامـات مربـوط بـه شـفافیت نمی‌شـود، کـه ایـن احیانـاً موجـب می‌شـود سـکوها اطلاعـات مربـوط بـه ارزیابـی اعتبـار اطلاعـات را آشـکار کننـد. ایـن [آشکارسـازی] ممکـن اسـت شـامل مداخـلات در سـطح کاربـر باشـد - کمـک بـه اطلاع‌رسـانی بـه کاربـران در مـورد منشـأ و تأییـد محتـوا. ایـن [آشکارسـازی] ممکـن اسـت بـه عنـوان قوانینـی مشخص‌شـده در مجموعـه‌ای از اسـتانداردها در اطـراف «پرچم‌هـای مناقشـه»[1] خـود را نشـان دهـد کـه در کنـار پسـت‌های برخـط علامـت می‌دهنـد کـه یـک داسـتان توسـط یـک سـازمان صحت‌سـنج[2] مـورد چـون و چـرا قـرار گرفتـه اسـت، ماننـد مـواردی کـه همیـن حـالا هـم اسـتفاده می‌شـود.[3] ایـن [آشکارسـازی] ممکـن اسـت شـامل افشـای گسـترده‌تری بـرای تنظیم‌گـران خـاص یـا گروه‌هـای تحقیقاتـی متخصـص باشـد کـه ممکـن اسـت سـپس بـرای اجـرای قوانیـن و اطلاع‌رسـانی بـه مـردم بـه طـور گسـترده کار کننـد.[4] ایـن [آشکارسـازی] می‌توانـد داده‌هـای موضعـی[5] بیشـتری را کـه توسـط فیسـبوک و سـایر شـرکت‌ها در مـورد فعالیت‌هـای تبلیغاتـی در جلسـات کنگـره ۲۰۱۷ دربـاره ایـن موضـوع ارائـه شـد سـاختارمند کنـد.[6]

دوم، فراتـر از شـفافیت بیشـتر در مـورد داده‌هایـی کـه سـکوها «در دسـت» دارنـد، CDA ۲۳۰ مانـع اقدامـات لازم سـکوها بـرای آشکارسـازی بیشـتر از سـوی کاربـران خـود نمی‌شـود. پیشـنهادها در ایـن جنبـه بـه فراینده‌ـای مربـوط بـه تبلیغـات برخـط متمرکـز شـده اسـت، کـه بـه

1. dispute flags
2. Fact-checking organization
3. Kafka 217
4. Diresta and Harris 2017
5. Ad hoc
6. Seetharaman and Wells 2017; Hwang and Woolley 2017

نظـر می‌رسـد یکـی از کانال‌هـای اطلاعـات کاذب سیاسـی در انتخابـات ریاسـت‌جمهوری ۲۰۱۶ ایـالات متحـده بـوده اسـت. محققـان الزامـات مربـوط بـه «مشـتری خـود را بشناسـید»[1] بـرای تبلیغ‌گـران برخـط بـه مـوازات قوانیـن مشـابه وضع‌شـده در بخـش مالـی و همچنیـن قوانیـن دقیق‌تـر در مـورد برچسـب‌گذاری حسـاب‌های ناشـناس و خـودکار پیشـنهاد کرده‌انـد.[2] قانـون تبلیغـات صادقانـه - قانـون دو طرفـه‌ای کـه در ابتـدا در اکتبـر ۲۰۱۷ پیشـنهاد شـد، امـا اقدامـات متعاقـب کمـی پـس از آن مشـاهده شـد – سـکوهای برخـط بـزرگ را ملـزم می‌کنـد کـه یـک پرونـده عمومـی از تمـام ارتباطـات انتخاباتـی کـه فراتـر از یـک آسـتانه پولـی خاص‌انـد داشـته باشـند.[3] ایـن پرونـده شـامل یـک کپـی از تبلیغـات، داده‌هـای هدف‌گیـری شـده، و همچنیـن اطلاعـات مربـوط بـه خریـدار تبلیغـات اسـت.[4] رویکردهـای مشـابه خـارج از زمینـه تبلیغـات ممکـن اسـت بـا اعمـال الزامـات سـخت‌گیرانه‌تر در ایجـاد حسـاب‌های کاربـری و پروفایل‌هـای جدیـد در یـک خدمـت، از بات‌هـا و اسـتروترفینگ [یعنـی تبلیغـات مبتنـی بـر نظـرات جعلـی][5] جلوگیـری کنـد.

سـوم، CDA ۲۳۰ مانـع مداخـلات چشـمگیرتر دیگـری کـه جریـان واقعـی اطلاعـات را از طریـق سـکوها تغییـر می‌دهـد نمی‌شـود. بـه عنـوان ابـزاری بـرای محـدود کـردن تأثیـر سـکوهای برخـط در شـکل‌دهی بـه گفتمـان عمومـی، سیاسـت‌گذاران خواسـتار نوعـی «بـی طرفـی شـبکه‌ای» بـرای اعمـال در لایـه محتوایـی وب شـده‌اند، بـه طـوری کـه سـکوهایی چـون «فیسـبوک، گـوگل و آمـازون - ماننـد ISPهـا - بایـد در رفتـار خـود بـا جریـان اطلاعـات قانونـی و تجـارت در سـکوهای خـود «بی‌طـرف» باشـند».[6] رویکردهـای دیگـر ممکـن اسـت ایجـاب کنـد کـه الگوریتم‌هـا

1. know your customer
2. Diresta and Harris 2017, p. 82
3. The Honest Ads Act, S. 115 ,1989th Cong. (2017)
4. Id. at §8.
5. Astroturfing
6. Franken 2017

باید شاخص‌های مشخص قابل خواندن توسط ماشین درباره «اعتبار»[1] در ارتقا و رتبه‌بندی اطلاعات را در نظر بگیرند.[2]

هر سه‌ی این رویکردها در ساختار CDA ۲۳۰ عمل می‌کنند و به سیاست‌گذاران امکان می‌دهند تا به مسئله تاکتیک‌های استفاده‌شده توسط کارزارهای اطلاعات کاذب سیاسی بپردازند بدون اینکه لزوماً مسئولیت اَعمال فردی را به سکو متوجه سازند. این به این معنی نیست که آنها در غیر این‌صورت فاقد اعتبار نخواهند شد. دادگاه‌ها در مواردی تأیید کرده‌اند که خروجی‌های الگوریتمی، اِعمال حقوق متمم اول خود سکوها است.[3]

مقرراتی که این خروجی‌ها را شکل خواهند داد، متعاقباً با این حفاظت‌های قانونی مواجه خواهد شد. جالب توجه اینکه، همان‌طور که تیم وو[4] (۲۰۱۳) استدلال کرده است، حفاظت‌های متمم اول، خروجی‌های الگوریتمی سکوهای «کارکردی» را که «درگیری آنها با اطلاعات برای این‌که گفتار باشد بیش از حد دور یا مکانیکی است» را پوشش نمی‌دهد. این شرایطی است که در آن مصونیت CDA ۲۳۰ به احتمال زیاد تحت مورد Roommates.com اعمال خواهد شد زیرا این سکوها «به طور عمده مشارکتی» در محتوای توهین‌آمیز نمی‌کنند. برای این منظور، آموزه‌ها تا حدودی مکمل یکدیگرند زیرا مقرراتی که مستقیماً برای شکل‌دهی خروجی الگوریتمی به کار می‌روند احتمالاً از چالش مبتنی بر متمم اول، در شرایطی که آموزه Roommates.com احتمالاً جلوی تلاش‌ها برای تحمیل مسئولیت به سکو را می‌گیرد، جان سالم به در می‌برند.

1. Credibility

۲. نگاه کنید مثلا به Mina (2017)، که که یک ابتکار برای توسعه «نشانگرهای اعتبار» را بحث می‌کند.

۳. نگاه کنید مثلا به
Search King, Inc. v. Google Tech., Inc., No. 2003 ,1457-02 WL 21464568, at *4 (W.D. Okla. May 2003 ,27).
همچنین نگاه کنید به Volokh and Falk (2012)، که این پرونده‌هایی را در زمینه‌ی نتایج جستجو مرور می‌کند.

4. Tim Wu

با فرض اینکه یک مداخله مطابق با این الزامات قانونی باشد، این سه روش ممکن است بتوانند علیه این تهدیدها، بدون اصلاح قانون زیربنایی، در کنار استثنایی که در پرونده Roommates.com بیان شده است، اقدامی انجام دهند.

نتیجه: برخی مسیرها بسته است، دیگر مسیرها باز می مانند

CDA ۲۳۰، سازگار با انتقادات طولانی مدت از مقررات مربوط به مسائلی مانند افترا و آزار و اذیت، ممکن است انگیزه‌هایی مشکل‌دار برای سکوها فراهم کند تا در مقابله با اطلاعات کاذب، آن‌طور که باید، فعال نباشند. همچنین ممکن است سکوهای برخط فعالیت کمتری در جمع‌آوری و به اشتراک‌گذاری اطلاعات در مورد مرتکبین جرایم داشته باشند، به طوری که مانع تلاش برای تعقیب مستقیم این بازیگران شود.[1]

درعین حال، CDA ۲۳۰ به‌عنوان یک مانع مطلق برای عمل در این فضا عمل نمی‌کند. تحت قضاوت در مورد Roommates.com، اقدامات قضایی ممکن است در جهت تحمیل مسئولیت به سکوها تا حدی باشد که طراحی خاص آنها به سطح «همراهی در توسعه [ی جرم]» برسد، که آنها را در ارتکاب اعمال غیرقانونی، شریکِ جرم می‌کند. بعلاوه، از آنجا که CDA ۲۳۰ در مورد ادعاهایی که سکو را به‌عنوان «ناشر یا سخنگوی» محتوا تلقی می‌کنند به طور محدود اعمال می‌شود، پس با مداخلات قانونی که مستقیماً تعهداتی را بر روی دوش سکوها قرار می‌دهد، منافاتی ندارد. بسیاری از پیشنهادهایی که به شفافیت بیشتر، آشکارسازی کاربر، و اصلاحات الگوریتم‌های محتوای زیربنایی

1. Reidenberg et al. 2012

نیاز دارند، همچنان تحت ساختار CDA ۲۳۰ گزینه‌هایی قابل طرح‌اند.

بنابراین این سؤال که آیا CDA ۲۳۰ برای مقابله با تهدیدات اطلاعات کاذب اصلاح شود یا خیر، به بررسی دقیق بستگی دارد. مسئله این است که آیا این گزینه‌های باقیمانده برای پاسخگویی به تهدیدات ناشی از اطلاعات کاذب سیاسی کافی است یا خیر - و به همین ترتیب، عملی بودن بالقوه، و سود و هزینه اصلاح CDA ۲۳۰ برای تحمیل مسئولیت فردی به طور مستقیم به سکوها [باید دقیقاً مشخص شود].

بخش سوم

بخش سوم

آیا باید CDA ۲۳۰ اصلاح شود تا اطلاعات کاذب سیاسی را برطرف کند؟

با ادامه بحث عمومی پیرامون چالش ناشی از اطلاعات کاذب برخط، تعداد فزاینده‌ای از کسانی که اظهار نظر می‌کنند طرفدار اصلاح یا حذف CDA ۲۳۰ اند. یکی از اظهارات اخیر در فایننشیال تایمز،[1] این ماده قانونی را «خلأ قانونی»[2] توصیف کرده است، و در نتیجه به صراحت استدلال کرده است که اپراتورهای سکو «دیگر مستحق نوعی معافیت کامل از مسئولیت‌هایی نیستند که در هر صنعت دیگری به عنوان هزینه تجارت به شرکت‌ها متحمل می‌شود».[3] مجله اکونومیست این ماده قانونی را به عنوان «یارانه ضمنی» برای سکوهای برخط توصیف و استدلال کرده که «دادن مجوز رایگان به سکوها به طور فزاینده‌ای برای تنظیم‌گران و دادگاه‌ها دشوار شده است: آنها به طور کلی برای اقتصاد و جامعه بیش از اندازه مهم شده‌اند».[4]

رابطه بین CDA ۲۳۰ و تلاش برای مبارزه با اطلاعات کاذب پیچیده است. این بخش به دنبال ارزیابی استدلال برای تغییر یا حذف CDA ۲۳۰ با پاسخ دادن به سؤالات زیر است. اول، با توجه به وضعیت موجود، آیا دامنه مداخلات ممکن برای رفع تهدیدهای ناشی از کارزارهای اطلاعات کاذب سیاسی کافی است؟ دوم،

1. Financial Times
2. Loophole
3. Foroohar 2017
4. The Economist 2017

تأثیرات مثبت و منفی بالقوه حاصل از چنین اصلاحی چه خواهد بود؟ سوم، به طور عملی، اگر قرار باشد کسی CDA ۲۳۰ را اصلاح کند، چه اصلاحاتی برای رفع چالش ناشی از اطلاعات کاذب سیاسی مناسب است؟

آیا مداخلات در چهارچوب CDA ۲۳۰ کافی است؟

همان‌طور که در «بخش ۲: چگونه CDA ۲۳۰ تلاش‌ها برای مبارزه با اطلاعات کاذب سیاسی برخط را شکل می‌دهد؟» بحث شد، CDA ۲۳۰ به‌عنوان یک سدّ قطعی برای مداخلات قانونی بالقوه برای حل چالش‌های اطلاعات کاذب سیاسی عمل نمی‌کند. تأثیر آن به طور قابل ملاحظه‌ای خاص‌تر است: این مداخلاتی که می‌تواند سکو را، به‌عنوان ناشر یا سخنگوی یک اقدام، تهدید کند و مسئولیت کاربر معینی را برای کل سکو اعمال کند، محدود می‌کند. این قانون مانع از انجام طیفی از اقدامات قانونی بالقوه برای الزام‌بخشی به ایجاد شفافیت بیشتر در سکوها، اَعمال آشکارگرانه‌ی قوی‌تر از سوی کاربران، یا حتی اصلاح سازوکارهای نحوه توزیع اطلاعات توسط خدمت‌هایی مانند فیسبوک یا گوگل نمی‌شود. CDA ۲۳۰ همچنین مانع اقدامات احتمالی دادگاه‌ها با استفاده از الگوی قبلی در Roommates.com برای حذف گزینشی مصونیت قانونی نمی‌شود. یک سؤال که فوراً پیش می‌آید این است که آیا CDA ۲۳۰ صرفاً حالت سرگرمی[1] دارد. آیا ابزارهای بالقوه‌ای که بدون اصلاح CDA ۲۳۰ در دسترس‌اند، به تنهایی کافی نیستند که بتوانند با کارزارهای جدید اطلاعات کاذب سیاسی مقابله کنند؟

1. Distraction

یک چالش مهم برای اقدامات تنظیم‌گرانه یا دادگاه-محور در این فضا مربوط به سرعت رشد و نمو کارزارهای اطلاعات کاذب برخط است. تاکتیک‌های اطلاعات کاذب سیاسی روسیه به طور مداوم از تکنیک‌های جدیدی استفاده می‌کنند و مداخله آنها در سال ۲۰۱۶ نشان‌دهنده اوج سال‌ها آزمون و خطای قبلی در این فضا است.[1] برای این منظور، حتی اگر راهکاری مشخص در کاهش تأثیر این تاکتیک‌ها در کوتاه مدت موفقیت‌آمیز باشد، با تغییر رویکردِ مرتکبان جرم، ممکن است آن راهکار به سرعت منسوخ شود. یک راه حل قدرتمند قادر خواهد بود به سرعت با پیشرفت چشم‌انداز استراتژی‌ها سازگار شود؛ و از این نظر، مشخص نیست که آیا گزینه‌های مورد بحث در «گزینه اول: تنظیم‌گری مبتنی بر دادگاه از طریق CDA ۲۳۰» یا «گزینه دوم: اقدامات قانون‌گذارانه فراتر از اصلاح CDA ۲۳۰» پاسخ کاملاً چابکی را ارائه دهند.

به‌عنوان مثال، قوانینی که به موجب آن سکوها لازم است افشای اطلاعات بیشتری از کاربران و تبلیغ‌کنندگان انجام دهند، ممکن است به سرعت منسوخ شوند زیرا مرتکبان این کارزارها روش‌های جدیدی برای پوشاندن هویت خود پیدا می‌کنند. به ویژه در مورد کارزارهای پیچیده اطلاعات کاذبی که بیشترین نگرانی را ایجاد می‌کنند، مانند مواردی که در انتخابات ریاست‌جمهوری ۲۰۱۶ مشاهده شدند، مرتکبان این تلاش‌ها ممکن است ابزارهایی داشته باشند که بتوانند از طریق سپرهای شرکتی و سایر نام‌های مستعار، مشارکت خود را مخفی کنند.[2] در این حالت، می‌توان انتظار داشت که تعریف یک مجموعه ثابت از الزاماتِ گزارش‌دهی به راحتی گریزپذیر خواهد شد.

1. Chivvis 2017
2. Lapowsky 2017

تمرکز فعلی روی تبلیغات نیز ممکن است خیلی محدود باشد. اگرچه درست است که ابزارهایی برای مانع شدنِ استفاده مرتکبان اطلاعات کاذب سیاسی از سکوهای تبلیغاتی ممکن است دسترسی آسان به ابزارهای قدرتمند برای هدف قرار دادن یک پیام را محدود کند، توجه به این نکته مهم است که این کارزارها حتی بدون دسترسی به تبلیغات پولی نیز می‌توانند پیش بروند. کارزارهای دارای منابع کافی ممکن است به قابلیت‌های توزیع زیرساخت‌های رسانه‌ای دولتی، روابط تبلیغاتی غیررسمی موجود در خارج از ابزار تبلیغاتی یک سکو، و طرف‌داران «شبه مردمی» که می‌خواهند یک پیام بخصوص را گسترش دهند، دسترسی داشته باشند.[1] حتی روش‌های محدودتری که بر محدودیت‌های تبلیغات سیاسی تمرکز کرده‌اند، به طور ویژه تلاش‌هایی را که در صدد هدف قرار دادن و تولید کشمکش خارج از متن انتخابات یا کارزارند فراموش می‌کنند. به عنوان مثال، اتفاقات داخل فیسبوک که توسط روسیه برای ایجاد کشمکش بین گروه‌های «جان سیاهان مهم است» و «جان آبیان مهم است» ایجاد شد، ممکن است فعالیت‌هایی باشد که به‌وسیله‌ی قوانینی به سبکِ «مشتری خود را بشناسید» مانع نشود.[2]

به نظر می‌رسد مداخله توسط دادگاه‌ها برای اعمال گزینشی مصونیت CDA ۲۳۰ بدون اصلاح ادبیاتِ زیربنایی به همین ترتیب ضعیف است. مورد Roommates.com و موارد مشابه به تحقیق بسیار ویژه‌ای بستگی دارند که طراحی دقیق یک سکوی برخط را روشن می‌کند. این شیوه احتمالاً تعدادی از کانال‌هایی را که از طریق آنها ممکن است کارزارهای اطلاعات کاذب سیاسی جریان داشته و

1. See the section “Part 1: The Disinformation Challenge” in this chapter.
2. For examples of these kinds of tactics, see Seetharaman (2017).

همچنان مؤثر باقی بمانند، دست نخورده باقی می‌گذارد. به یاد آورید که در آن حکم، تهیه جعبه متنی بی‌انتها برای ارسال محتوا به اندازه کافی «دست-نخورده»[1] بود که سرویس Roommates.com همچنان قادر به دریافت مصونیت CDA ۲۳۰ برای محتوای تبعیض‌آمیز در آن قسمت از سایت شد. تعمیم چنین قانونی به متن سیاسی به معنای این است که سکوها، برای مثال برای فعالیت‌هایی که در ویژگی‌های ارسال فرم آزاد آن‌ها اتفاق می‌افتد، مصونیت دارند، اما برای خوراک‌های الگوریتمی که سکو نقش «همراهی در توسعه» فعال‌تری دارد، مجاز نیستند. نتیجه ممکن است این باشد که سکوها اقدامات ابتدا به ساکن بیشتری را برای مقابله با اطلاعات کاذب در برخی از بخش‌های خدمات خود، بیش از دیگر بخش‌ها، انجام دهند، و این مشکل کلی را کنترل‌ناشده رها می‌کند.

سکوها ممکن است با ابهام قانونی قابل توجهی در مورد محدودیت‌هایی که ممکن است موجب مسئولیت واسطه‌ای آنها شود، مواجه باشند، و این باعث ایجاد اجرای ناسازگار سیاست در سراسر سکوها می‌شود. فارغ از ماهیت مبتنی بر واقعیتِ خاص تصمیمات گرفته‌شده پس از مورد Roommates.com، دادگاه‌ها نیز این قاعده را به طور ناسازگار در [دیگر] حوزه‌های قضایی اعمال می‌کنند و گاهی دلیل‌هایی ارائه شده که دلایلِ آن پرونده را زیر سؤال برده است.

دشواری دوم این است که چیزهای زیادی در مورد تأثیرات اجتماعی کارزارهای اطلاعات کاذب سیاسی ناشناخته مانده است، که باعث می‌شود فراهم ساختنِ یک پاسخ مؤثر در کوتاه‌مدت یک چالش باشد. به عنوان

1. hands-off

مثال، پیشنهادهایی که سکوهای برخط را ملزم می‌کند تا علامت‌دهی بهتری به کاربران در مورد کیفیت و منشأ محتوایی که روبرو می‌شوند بدهند گسترش یافته است.[1] اما هنوز مشخص نیست که آیا برچسب‌هایی که نشان می‌دهد که آیا یک محتوا توسط یک سازمانِ صحت‌سنج زیر سؤال رفته است یا نه واقعاً مؤثر است. مطالعه‌ای اخیر نشان می‌دهد که تکرار ساده عناوین «اخبار جعلی» برای افزایش حساسیت کاربران به دقت، کافی است، حتی اگر برچسب غلط یا مورد مناقشه باشد.[2] همچنین شواهدی وجود دارد که اثرِ «حقیقت ضمنی»[3] را نشان می‌دهد، که در آن برچسب «اخبار جعلی» دقت درک‌شده از آن مطلب را تا حد کمی کاهش می‌دهد، در حالی که دقت درک شده از اطلاعات کاذبی را که برچسب نخورده‌اند، تا حد زیادی افزایش می‌دهد.[4] در زمینه سیاسی، نتایج اخیر آزمایشگاهی گویای این است که حتی وقتی نشان داده می‌شود که اظهارات یک رهبر سیاسی اطلاعات کاذب است، اثر این افشای کاذب بودن بر قصد بالفعل رأی‌دهندگان محدود است.[5] برای دستیابی به یک واکنش معنی‌دار در برابر این تهدیدات، مطالعه‌ی بیشتر لازم است.

نهایتاً، مشخص نیست که آیا نهادهای قانون‌گذاری و قضایی صلاحیت فنی برای اجرای مؤثر این مداخلات را دارند یا خیر. اتخاذ رویکرد مبتنی بر Roommates.com، دادگاه‌ها را ملزم می‌کند که نقش اصلی را در بازجویی از تصمیمات خاص طراحی و ارزیابی میزان کمک آنها به رفتارهای غیرقانونی داشته باشند. با توجه به اینکه حتی متخصصان صنعت اعتراف می‌کنند که

1. Santa Clara University 2017
2. Pennycook, Cannon and Rand 2017
3. implied truth
4. Pennycook and Rand 2017
5. Swire et al. 2017

خطرات و پیچیدگی مدیریت این سیستم‌ها باعث می‌شود آنها در تلاش برای حل چالش‌های اطلاعات کاذب محافظه‌کار باشند، دادگاه‌های عمومی ممکن است آن‌چنان به خوبی عمل نکنند.[1]

تدبیرِ مداخله قانون‌گذارانه با موانع مشابهی روبرو است. بسیاری از پیشنهادهای مطرح شده در «گزینه دوم: اقدامات قانون‌گذارانه فراتر از اصلاح CDA ۲۳۰» از عدم پوشش کافی رنج می‌برند، و برخی از تکنیک‌های اطلاعات کاذب را دشوارتر می‌کنند، در حالی که بقیه را برای بهره‌برداری باز می‌گذارند. یک گزینه برای غلبه بر این محدودیت، گسترش دامنه قانون‌گذاری برای مقابله جامع‌تر با اطلاعات کاذب است، به عنوان مثال، با تجویز الگوریتم‌هایی خاص که عناصر تعریف‌شده از کیفیت اطلاعات را در نظر می‌گیرند یا بررسی منظم رفتار الگوریتمی را الزام می‌بخشند. با این وجود افزایش دامنه‌ی]قانون‌گذاری[به طور هم‌زمان سطح پیچیدگی را گسترش می‌دهد و قانون‌گذاران را ملزم می‌کند که با طراحی فنی سکوها در سطحی جزئی تعامل بیشتری داشته باشند. همان‌طور که در پرونده قضایی صادق است، مشخص نیست که فرایند قانون‌گذاری قادر به انجام چنین چیزی به طور مؤثر و به موقع باشد.[2]

مزایا و هزینه های بالقوه اصلاحیه چیست؟

اصلاحیه CDA ۲۳۰ بر بسیاری از نقایصی که احتمالاً مانع رویکرد تنظیم‌گرانه یا دادگاه-محور در برابر چالش‌های ناشی از اطلاعات کاذب سیاسی می‌شود غلبه می‌کند. نکته مهم اینکه قرار دادن «خدمت رایانه‌ای تعاملی» در معرض مسئولیت به‌خاطر اقدامات غیرقانونی

۱. برای یک مثال از این‌که چگونه «فهمی از خطرات یادگیری ماشین (ML) محافظه‌کاری [small-c conservatism]» در شرکتهایی چون فیس‌بوک را «پیش می‌راند» نگاه کنید به Constine (2017).
۲. مقایسه کنید با Metz (2015)، که زیرساخت پیچیده برای مدیریت کردن کد گوگل (Google's code) را توصیف می‌کند.

انجام‌شده توسط کاربران، ساختار کلی مشوق‌ها را با انتقال بارِ مسئولیت به دوش سکو تغییر می‌دهد. در واقع، حکومت به جای تعیین مجموعه‌ای دقیق از اقدامات لازم برای مقابله با اطلاعات کاذب، مجموعه‌ای اولویت درباره فعالیت‌هایی که باید کمینه شوند تنظیم می‌کند و تصمیمات در مورد چگونگی دستیابی به این هدف را به سکوها می‌سپارد.

چنین آرایشی از چالش‌هایی که رویکردهای تنظیم‌گرانه یا دادگاه-محور با آن روبرویند جلوگیری می‌کند. سکوها قادرند به سرعت اقداماتی را برای کاهش تأثیر اطلاعات کاذب سیاسی تدوین و اجرا کنند. مهم‌تر این‌که آنها می‌توانند تاکتیک‌ها را با چابکی، همین‌طور که فضای این کارزارها تغییر می‌کند تغییر دهند، و در نتیجه اطمینان خاطر به عمل آورند که سنگر مستحکم‌تری در برابر این تهدیدها ایجاد می‌شود. علاوه بر این، سکوها همچنین برای ارزیابی کارایی برخی از راه‌حل‌های پیشنهادی و برای روشن کردن ابهامات فعلی در مورد تأثیر و مکانیسم‌های رفتاری زمینه‌ساز اطلاعات کاذب، بهترین موقعیت را دارند. وضع خطر جریمه مالی با عدم رسیدگی به این چالش موجب افزایش سرمایه‌گذاری در این کار تحقیقاتی و مداخلات تجربی مبتنی بر آن می‌شود. سرانجام، تغییر CDA ۲۳۰ مسئولیت را متوجه عاملانی می‌کند که تخصص فنی و شناخت عمیق از محصولات لازم برای توسعه‌ی پاسخی دقیق به اطلاعات کاذب سیاسی را دارند.

به‌رغم آنچه گفته شد، دامنه وسیع CDA ۲۳۰ به این معنی است که اصلاحات، طیف وسیعی از اثرات بعدی را ایجاد خواهد کند.

اگرچه اصلاحیه یا حذف کلی می‌تواند نفوذ اطلاعات کاذب سیاسی را محدود کند، ممکن است مجموعه‌ای از آسیب‌ها را ایجاد کند که مجموعاً چنین تغییری را غیرعاقلانه می‌کند.

اول، سرایت مسئولیت در سطح کاربر به سکوها ممکن است این خدمات را در رفع این مسئولیت دچار مشکل یا بیش از حد واکنشی کند به نحوی که به آزادی بیان آسیب وارد نماید. اینها به نوعی استدلال‌های «کلاسیک» علیه ایجاد استثنا در چهارچوب CDA ۲۳۰ اند.[۱] از یک طرف، مسئولیت در قبال اَعمال هر یک از خیل کاربران ممکن است قابلیت مالی برخی از سکوها را تهدید کند.[۲] این مطلب به ویژه با توجه به دامنه وسیع «خدمت رایانه‌ای تعاملی» تحت سابقه قانونی، شامل همه موارد از یک وبلاگ کوچک یا لیست‌سروها تا بزرگترین سکوهایی که توسط شرکت‌هایی مانند گوگل و فیسبوک اداره می شوند، صادق است.[۳] سکوهای بزرگتر، برای رفع این خطر، از منابع مالی و تخصص حقوقی برخوردار خواهند بود، درحالی‌که مشاغل کوچک‌تر و خدمت‌هایی که توسط داوطلبان اداره می‌شوند، نمی‌توانند بر اساس اقدامات کاربران خود، دعاوی قضایی را مدیریت کنند. یک نتیجه احتمالی تسریع بیشتر و تقویتِ ادغام در مجموعه بزرگ‌ترین شرکت‌هاست چنان‌که سکوها با منابع کمتر از بازار خارج می‌شوند یا با رقبای با موقعیت بهتر ادغام می‌شوند.

از طرف دیگر، سکوها ممکن است بیش از حد نسبت به حتی مقدار کمی تهدیدِ مسئولیت حقوقی واکنش نشان دهند، و حذف محتوای بالقوه توهین‌آمیز را به طور پیش‌فرض، به جای سنجش بررسی‌شده خطر، ترجیح دهند.[۴] از آنجا که اصلاح CDA ۲۳۰ برای

1. Reidenberg et al. 2012, pp. 37-35
2. Reidenberg et al. 2012, p. 36
۳. نگاه کنید به Batzel v. Smith, 333 F.3d 1018 (9th Cir 2003)
4. Reidenberg et al. 2012, p. 36

مقابلـه بـا چالـش اطلاعـات کاذب تـلاش می‌کنـد، انگیـزه بـرای بـه حداقـل رسـاندن ریسـک قانونـی ممکـن اسـت باعـث شـود کـه سـکوها محتوایـی را کـه درسـت و ارزشـمند اسـت امـا احتمـال دارد منبـع بحـث و جـدل باشـد پیش‌دسـتانه حـذف کننـد. ایـن حذف‌کردن‌هـا همچنیـن می‌توانـد منافـع افـرادی را کـه تمایـل و توانایـی پیگیـری ادعـای حقوقـی علیـه ایـن سـکوها را دارنـد، بـه صـورت نامتناسـب نشـان دهـد. پـس، از قضـا، ایجـاد مسـئولیت در سـکو در قبـال اطلاعـات کاذب ممکـن اسـت مسـیر دیگری را ایجـاد کنـد کـه از طریـق آن اطلاعـاتِ درسـت سـرکوب می‌شـود.

دوم، اصـلاح CDA ۲۳۰ ممکـن اسـت سـکوها را اساسـاً، در مقایسـه بـا حالـت دیگـر، کمتـر شـفاف و مشـارکت‌پذیر کنـد. یکـی از نگرانی‌هـای ایجـاد انگیـزه در تصویـب CDA ۲۳۰ در دهـه ۱۹۹۰ ایـن تصـور بـود کـه هیـچ وسـیله عملـی وجـود نـدارد کـه توسـط آن شـرکت‌ها بتواننـد بـر جریـان گسـترده محتـوای تولیـد شـده توسـط کاربـر کـه هـر روز از طریـق خدمـات آنهـا منتشـر می‌شـود، نظـارت کننـد.[۱] بـا ایـن حـال، همان‌طـور کـه دیگـران اشـاره کرده‌انـد، ایـن محدودیـت، بـا توجـه بـه این‌کـه بـا پیشـرفت در یادگیـری ماشـین و قـدرت پـردازش، نظـارت و کنتـرل مطالـب در مقیـاس گسـترده ممکن‌تـر شـده اسـت، بـه تدریـج کمتـر مشـکل‌آفرین می‌شـود. در واقـع، بسـیاری از ایـن سیسـتم‌ها امـروزه بـرای مدیریـت نظـارت بـر پورنوگرافـی کـودکان و نقض‌هـای مالکیـت معنـوی اسـتفاده می‌شـوند، قوانینـی کـه از حـدود صلاحیـت CDA ۲۳۰ مسـتثنی شـده‌اند. تـا آنجـا کـه اصلاحـات CDA ۲۳۰ سـکوها را در معـرض مسـئولیت فعالیت‌هـای اطلاعـات کاذب ارتکاب‌شـده توسـط کاربـران آنهـا قـرار می‌دهـد، بـه احتمـال زیـاد همـان روش الگوریتمـی خـودکار بـرای بـه

۱. نگاه کنید به
Zeran v. America Online, Inc., 129 F.3d 4) 331 ,327th Cir. 1997):
«در نتیجـه، مقـدار اطلاعـات رد و بـدل شـده از طریـق خدمـات رایانـه ای تعاملـی تعجب‌برانگیـز اسـت ... ایـن بـرای فراهم‌کننـدگان خدمـت غیرممکـن اسـت کـه هـر یـک از میلیون‌هـا پسـت‌گذاری‌ها را بـرای مشـکلات ممکـن غربـال کننـد.»

حداکثر رساندن و تسریع شناسایی و حذف محتوای وهن‌آمیز نیز اعمال خواهد شد.[1] روش‌های مقابله با سؤالات مربوط به حقیقت، نادرستی و کیفیت اطلاعات ممکن است مانع مدل‌های جایگزین دیگری شود که از مشارکت کاربر و جامعه برای فیلتر کردن این معیارها استفاده می‌کنند.[2] ویکی‌پدیا، دائرةالمعارف ویرایش شونده به نحو همکاری جمعی، در مقاومت در برابر تأثیر «اخبار جعلی» از طریق نظارت انسانی نسبتاً موفق بوده است.[3] تحقیقات نشان می‌دهد که کاربران با احساس مالکیت و هویت جمعی انگیخته می‌شوند تا در بحث و گفتگو در مورد حقایق و از بین بردن دروغ، نقش فعالی داشته باشند.[4] وجود الگوریتم‌های خودکار که بر محتوا کنترل دارند می‌توانند این انگیزه‌ها را از بین ببرد و سهم داوطلبان را کاهش دهد.[5] از این نظر، سیستم‌های خودکار با رویکردهای مبتنی بر اجتماع برای مسئله اطلاعات کاذب در تنش هستند.

خصوصیاتی در فیلتر کردنِ اطلاعات کاذب مبتنی بر جامعه هست که آن را نسبت به رویکردهای الگوریتمی خودکار مرجّح می‌کند. الگوریتم‌ها غیرشفاف و دارای سوگیری‌های پنهانی‌اند که تشخیص آنها برای کاربر دشوار است. به همین ترتیب، الگوریتم‌ها توسط سکو طراحی و نگهداری می‌شوند و به طور مؤثری تصمیمات مربوط به تشخیص صدق و کذب را به شرکت مجری این خدمت اعطا می‌کنند. در مقابل، یک روش فیلتر کردن که از بحث و گفتگو و نظارت در جامعه استفاده می‌کند، می‌تواند به شیوه‌ای شفاف‌تر به کار آید و تصمیم‌گیری در مورد اطلاعات کاذب را به کاربران بسپارد.

۱. نگاه کنید مثلا به چالش اختبار جعلی (www.fakenewschallenge.org/)، که رقابتی‌ست برای ساخت ماشینی برای تشخیص «اخبار جعلی».

2. Grimmelmann 2015; Rogers 2017

3. Rogers 2017, pp. 362–359

4. Rogers 2017, p. 363

۵. نگاه کنید به Halfaker (۲۰۱۳)، که این را توصیف می‌کند که چگونه خودکارسازی می‌تواند تاثیراتی خلاف داشته باشد که مشارکت‌های داوطلبانه را در طی زمان در زمینه‌ی ویکی‌پدیا کاهش می‌دهد.

اصلاح CDA ۲۳۰ ممکن است با اتخاذ رویکرد الگوریتمی، سکوها را برای به حداقل رساندن خطر تشویق کند، و بنابراین گزینه‌های مبتنی بر مشارکت مردم را محدود کند.[۱]

سوم، همان‌طور که نیکلاس برامبل[۲] (۲۰۱۲) نوشته است، مصونیت ناشی از CDA ۲۳۰ نشان‌دهنده یک استراتژی تنظیم‌گرانه برای جلوگیری از محصور کردن داده‌ها و ضبط تنظیم‌گرانه در زیرساخت اطلاعاتی است. به طور خاص، CDA ۲۳۰ - و مصونیت ارائه‌شده به سکوهای تحت بخش ۵۱۲ قانون حق نشر هزاره‌ی دیجیتال[۳] - واسطه‌های برخط را به عنوان یک نیروی توازن‌بخش در برابر تأثیر ارائه‌دهندگان شبکه مانند کمکاست[۴] و ای‌تی‌اندتی[۵] از یک طرف و تأثیر ارائه‌دهندگان محتوا مانند دیزنی،[۶] ویاکام،[۷] و نیویورک تایمز[۸] از طرف دیگر قرار می‌دهد.[۹] با محدودکردن قرارگیری سکوها در معرضِ مسئولیتِ سطح کاربر، «ارائه‌دهندگان شبکه و دارندگان محتوا دیگر تنها واحدهایی نیستند که تعیین کنند دسترسی، مشارکت، و نوآوری کاربر در چه شرایطی در این فضاهای [برخط] انجام می‌شود».[۱۰] این استثنائات همچنین مشوق‌های مالی را به گونه‌ای ترتیب می‌دهد که، حداقل از لحاظ نظری، واسطه‌های برخط را به عنوان مدافع منافع ارتباطی کاربران خود در برابر سایر عامل‌ها قرار دهد.[۱۱] اصلاح CDA ۲۳۰ توازن قدرت بین منافع مختلف را به نحوی بازنویسی می‌کند که می‌تواند زیرساخت اطلاعاتی گسترده‌تر را به روشی نامطلوب شکل دهد. این ممکن است بر منافع بالقوه حاصل از

۱. این به معنای زیرسؤال بردن این نیست که شرایطی وجود دارد که در آن خودکارسازی و بات‌ها می‌توانند با کارایی با مدل‌های مبتنی بر اجتماع کار کنند. نگاه کنید به Geiger (2017).

2. Nicholas Bramble
3. Digital Millennium Copyright Act
4. Comcast
5. AT&T
6. Disney
7. Viacom
8. New York Times
9. Bramble 2012, p. 364
10. Bramble 2012

۱۱. نگاه کنید به Bramble (۲۰۱۲)، pp. ۳۵۹–۳۶۱. اما محققان این تصور را که «تعادل قدرت» واقعا در عمل وجود دارد زیرسؤال برده‌اند. نگاه کنید به Pasquale and Bracha (2007).

پرداختن به تهدیدهای محدودتر ناشی از اطلاعات کاذب سیاسی بچربد. مواجهه با چالش خاص اطلاعات کاذب سیاسی با لغو عمده CDA ۲۳۰ با توجه به تأثیرات منفی گسترده‌تری که ممکن است به دنبال داشته باشد، فاقد توجیه است. برای این منظور، سؤال اصلی مربوط به نحوه متناسب‌کردن[1] است: دقیقاً چه نوع افعالی باید هدف اِعمال یک استثنا به CDA ۲۳۰ باشند؟ آیا انتساب علل فعلی دعوی به سکوها کافی خواهد بود یا این‌که به علل دعوی جدیدی نیاز خواهد بود؟

چه اصلاحاتی عملی اند؟

به ویژه در زمینه‌ی تنظیم‌گری نادرستی و کیفیت اطلاعات، تهیه یک استثناءِ مناسب برای CDA ۲۳۰ چالش‌برانگیز است. یک دلیل این است که، همان‌طور که پژوهشگر حقوقی کاس سونستاین[2] (۱۹۹۲) اشاره کرده، «ما نمی‌دانیم بازار ایده‌هایی که عملکرد خوبی دارد، چگونه است.» از آنجا که مشخص کردن یک حالت نهایی ایده‌آل با دقت دشوار است، شناسایی مجموعه مشوق‌هایی که جامعه باید برای پرداختن به اطلاعات کاذب برخط به سکوها تحمیل کند به همین ترتیب دشوار می‌شود.

دلیلی دیگر اینکه، یک انتخاب دشوار و عملی وجود دارد که دقیقاً مشخص کنیم به‌خاطر چه علل دعوی‌ای، وقتی توسط کاربری منفرد انجام می‌شود، باید سکو را در معرض مسئولیت قرار داد. قوانین مربوطِ زیادی وجود ندارد که انتشار مطالب کذب را غیرقانونی اعلام کند. افترا یک مصداق روشنِ خطای مدنی است که می‌توان آن را

1. Tailoring
2. Cass Sunstein

از CDA ۲۳۰ مستثنی کرد، زیرا اطلاعات کاذب سیاسی اغلب ناظر به شهرت یا شخصیت یک فرد خاص است. با این حال، همان‌طور که در «بخش ۱: چالش اطلاعات کاذب» بحث شد، ممکن است کارزارهای اطلاعات کاذب به دنبال گسترش مطالب غلط درباره موضوعات بسیار گسترده‌تری از موضوعات مربوط به اعتبار یک فرد باشند، و استاندارد اثبات افترا علیه چهره‌های عمومی خیلی بالا است.[1]

سایر فعالیت‌هایی که در گذشته با کارزارهای اطلاعات کاذب سیاسی همراه بوده‌اند، به طور بالقوه باعث خدشه‌دار شدن تعدادی از قوانین می‌شوند، از جمله اساسنامه‌ای علیه قلدریِ سایبری[2] و تحمیل عمدی پریشانی عاطفی.[3] تا آنجا که یک کارزار اطلاعات کاذب تلاش برای دستیابی و نشت اطلاعات دارد، همچنین ممکن است به تعرض به حریم خصوصی و نقض حقوق دولتی در مورد تبلیغات بینجامد.[4] اینها همه ادعاهایی است که اگر از CDA ۲۳۰ مستثنی شوند می‌توانند برای سکو مسئولیت‌آور باشد و با این کار آن‌ها را برای مبارزه با مرتکبان این کارزارها تشویق کند. اگرچه ایجاد استثناهایی پیرامون این اقدامات جانبی به طور غیرمستقیم می‌تواند مانعِ بهره‌وری یک تلاش برای نشر اطلاعات کاذب شود، ممکن است در پرداختن به چالش اصلی یعنی دست‌کاری رسانه‌ای و گسترش پروپاگاندا ناکام بمانند.

این کمبود علل دعوی علیه افرادی که اطلاعات کاذب را تداوم می‌بخشند جای تعجب ندارد. متمم اول مقررات مربوط به درستی، نادرستی یا کیفیت اطلاعات را به عنوان محدودیت‌های مبتنی بر محتوا به شدت

1. Brown 2015
2. Cyberbullying
3. Emotional Distress

نگاه کنید به‌طور کلی به Klein and Wueller (2017), pp. 7–9.

۴. حقوق قانون دولتی نسبت به تبلیغ (publicity) گاهی بعنوان ادعای مالکیت فکری طرح می‌شود، که تلاش دارد شاکیان از استثنا ذیل ۴۷ U.S.C. § ۲۳۰(e)(۲) استفاده کنند. نگاه کنید به Cross v. Facebook, CIV 2016 ,537384 WL 7785723 (Cal. Super. Ct. May 2016 ,31), aff 'd in part and rev'd in part, No. A2017 ,148623 WL 3404767 (Cal. Ct. App. Aug. 2017 ,9).

محدود می‌کند. قانون اساسی «خواستار این است که محدودیت‌های محتوایی گفتار غیرمعتبر فرض شود.»[1] در سال ۲۰۱۲، دیوان عالی سؤال ویژه درباره قوانین ضد اظهارات غلط را در ایالات متحده درمقابل آلوارز[2] بررسی کرد.[3] در آن پرونده قانون شجاعت مسروقه[4] که مربوطه به سال ۲۰۰۵ بود محل بحث قرار گرفت، که اظهارات غلط در مورد نشان‌های اعطاشده توسط نیروهای مسلح را قابل مجازات با جریمه نقدی یا حبس حداکثر تا شش ماه عنوان کرد.[5]

در ارزیابی تطابق آن قانون با قانون اساسی، کثیری از دادگاه‌ها متذکر شدند که «غلط بودن به تنهایی ممکن است برای خارج کردن گفتار از متمم اول کافی نباشد» و این استدلال را رد کردند که «علاقه‌ی» حکومت «به گفتمان درست به تنهایی برای ایجاد منعی بر گفتار کافی [است]».[6] دادگاه به مبارزه با اطلاعات کاذب به‌وسیله ضد گفتار استدلال کرده و اظهار داشت: «راه درمانِ گفتاری نادرست، گفتاری درست است. این طریقی معمول در جامعه آزاد است . . . [جامعه] وقتی حکومت بخواهد از طریق دستورالعمل‌های مبتنی بر محتوا برنامه‌ریزی عمومی انجام دهد، خدمات خوبی دریافت نمی‌کند.»[7] قوانینی که، پس از دقیق‌ترین بررسی‌ها، توزیع اطلاعات را به دلیل نادرست بودن آن مجازات می‌کنند، باید از سد بسیار بلند قانون اساسی بگذرند تا مجاز باشند.[8]

یک رویکرد ممکن است اجتناب از ضرورت تلاش برای تنظیم‌گری علیه کذب یا حتی کذب سیاسی فی‌نفسه باشد. همانند مورد آلوارز، «اگر قرار باشد اظهار نظر آزادانه و شدیدی در گفتگوی عمومی و خصوصی

1. Ashcroft v. American Civil Liberties Union, 542 U.S. 660 ,656.
2. v. Alvarez
3. United States v. Alvarez, 567 U.S. 709.
4. Stolen Valor Act
5. See id., at 715.
6. id., at 723 ,719.
7. id., at 727.
8. id., at 724 (citing Turner Broadcasting System, Inc. v. FCC, 512 U.S. 642 ,622).

صورت گیرد- اظهار نظری که متمم اول به دنبال تضمین آن است- برخی اظهارات غلط اجتناب‌ناپذیرند».[1] تهدید ناشی از کارزارهای هماهنگ اطلاعات کاذب مانند آنچه در انتخابات ریاست‌جمهوری ۲۰۱۶ ایالات متحده و جاهای دیگر دیده شده صرفاً انتشارِ اطلاعات نادرست در حوزه سیاسی نیست. توزیع کذب‌های سیاسی یکی از ویژگی‌های دیرینه تاریخ نهادهای مردم‌سالارانه ایالات متحده است.[2]

آنچه منحصر به فرد است این است که اطلاعات کاذب از طریق وسیله‌ای گسترش می‌یابد که به خودی خود اعتماد به نتایج فرایندهای مردم‌سالارانه را از بین می‌برد و مانع گفتمان مؤثر پیرامون سیاست می‌شود. بخشی از این موضوع سودی درک شده - و بالقوه واقعی - است که ابزارهایی مانند بات‌ها، تبلیغات با هدف‌گذاری خُرد،[3] منابع مالی دولتی خارجی، و سایر تاکتیک‌ها را به عاملانی اعطا می‌کنند که پیامی را گسترش دهند و عموم مردم را تحت تأثیر قرار دهند. این سود فارغ از درستی یا نادرستی اطلاعات منتشر شده است، گرچه در شرایط فوری باعث ایجاد این حس دراماتیک می‌شود که وضعیت کنونی شرایطی است که در آن جامعه «با تفنگ آب‌بازیِ صدق به مقابله با شیرفلکه‌ی کذب»[4] می‌رود.[5] اصلاح این توازن قدرت بر متناسب‌سازی بهتر ابزار گفتمان متمرکز است. چنین هدفی ممکن است از نظر سیاسی، قانونی و فکری قابل‌دسترس‌تر باشد تا تعیین اینکه آستانه «حقیقت» چه باید باشد و آن را برای تفسیر و اجرا به بازیگران خصوصی و دولت واگذاریم.

به طور خلاصه، گرچه ممکن است مشخص‌کردن دقیق اینکه یک بازار «ایده‌آل» ایده‌ها چگونه به نظر می‌رسد دشوار باشد، سرراست‌تر

1. id., at 718.

۲. نگاه کنید مثلا به Meacham (2013)، که دروغ‌های سیاسی حین کارزار ریاست‌جمهوری ایالت متحده ۱۸۰۰ را روشن می‌کند.

3. Advertisement microtargeting

4. counter[ing] a firehose of falsehood with a squirt gun of truth

5. Paul and Courtney 2016

این است که آنچه را که ممکن است به عنوان روش‌های رقابت ناعادلانه در بازار ایده‌ها باشد برشمرده و متوقف کنیم. اصلاحات CDA ۲۳۰ باید به این هدف معطوف شود، و نه به هدف گسترده‌ترِ تشویق سکوها برای از بین بردن کذب‌های سیاسی از وب. اتخاذ مورد دومی به‌عنوان هدف، ریسک استثناها در CDA ۲۳۰ را که کاملاً گسترده‌اند و لااقل ممکن است به ایجاد علل دعاوی جدیدی بینجامد، که به موجب متمم اول از نظر قانونی بودن محل تردیدند، افزایش می‌دهد.

این رویکرد باعث ایجاد استثناهایی در CDA ۲۳۰ برای تعدادی از قوانین موجود و مقررات جدید بالقوه می‌شود. بخش‌هایی از قانون کارزار انتخاباتی فدرال (FECA)[1] از CDA ۲۳۰ برای جلوگیری از مداخلات خارجی در گفتمان سیاسی مستثنی می‌شود.[2] FECA منافع و علایق خارجی را از ورود به مخارج مرتبط با انتخابات از طریق تبلیغات یا دیگر ارتباطات انتخاباتی شبیه آنچه در انتخابات ریاست‌جمهوری سال ۲۰۱۶ آمریکا رخ داد منع می‌کند. با استثنای این قاعده‌ها از مصونیت ارائه‌شده توسط CDA ۲۳۰، سکوها مسئول این اقدامات خواهند بود و مشوق‌هایی برای کاهش یا از بین بردن این فعالیت از سیستم‌های خود خواهند داشت.

طیف وسیعی از قوانین ارائه‌شده است که «هدف گذاری خرد»،[3] یعنی استفاده از داده‌های بسیار ریز برای هدف قرار دادن پیام‌های معطوف به کاربران در زمینه انتخابات و فراتر از آن، را محدود می‌کند.[4] برخی ایده‌ها شامل مقرراتی‌اند که کارگزاران داده[5] را که در جمع‌آوری و توزیع داده‌ی کاربر تخصص دارند ملزم می‌کند برای شهروندان قابلیت دسترسی به مجموعه‌ای که درباره آنها گرد آمده و به کار استفاده‌های خاص می‌آید،

1. Federal Election Campaign Act

۲. نگاه کنید به 52 U.S.C § 30121 and 11 C.F.R § 110.20.

3. Microtargeting

۴. برای نگاهی کلی به برخی از پیشنهادها درباره هدف‌گذاری خرد تبلیغاتی سیاسی، نگاه کنید به Rubinstein (۲۰۱۴).

5. Data broker

فراهم کنند.[1] پیشنهاد دیگر به تهیه «اطلاعیه‌های جامع ... [از] کنش‌های پردازش داده» از کسانی که درگیر جمع‌آوری داده‌های رأی‌دهندگان‌اند، الزام می‌کند.[2] در صورت اجرا، این قواعد ممکن است متعاقباً با تدوین استثنائی در CDA ۲۳۰ تقویت شود که مشوق‌های سکوها را با تقویت قانون همسو کند. این می‌تواند سطح شفافیت در دسترس مردم را در مورد اینکه چه انواعی از هدف‌گیری مورد استفاده قرار گیرد افزایش دهد و مانع از عاملانی شود که مایل به فراهم آمدن شفافیت سکوها نیستند.

استثناهایی محدود برای کلاهبرداری برای تعبیه در CDA ۲۳۰ نیز ممکن است به دلیل رواج بات‌های بدون برچسب یا عوامل پولی که برای اهدافِ ترغیب و تحریک، ادعا می‌کنند کاربر واقعی هستند، موجه شوند. چنین استثنایی همچنین برای همسو کردن سکوها با هدف کاهش یا از بین بردن ایجاد وب‌سایت‌هایی به کار می‌آیند که جعلی‌اند یعنی چنین تقلید یا ادعا می‌شود که انگار رسانه‌های خبری محلی‌اند، همان‌طور که در چرخه انتخابات ۲۰۱۶ مشاهده شد.[3]

اینکه چه تکنیک‌هایی «رقابت نامنصفانه در بازار ایده‌ها» محسوب شوند به درستی محلِ بحث عمومی است، و چنین پرسشِ بازی ممکن است نگرانی‌هایی را در مورد طیف گسترده‌ای از مسئولیت‌هایی که سکوها احیاناً درگیر آن‌اند برانگیزاند. حداقل، حذف مصونیت از سکوهایی که به طور فعال از این تکنیک‌ها در تأثیرگذاری بر گفتمان عمومی حمایت می‌کنند به نظر موجه و کمتر بحث‌برانگیز است. دانیل کیتس سیترون[4] و بنجامین ویتس[5] پژوهشگرانی‌اند که چنین روشی را پیشنهاد کرده‌اند،

۱. نگاه کنید به Rubinstein (2014), pp. 919–921؛ همچنین نگاه کنید به Executive Office of the President (2014)، که از رویکردهایی دفاع می‌کند که به افراد توانایی «شرکت در استفاده و توزیع اطلاعاتش پس از این‌که جمع‌آوری شد» را می‌دهد.

۲. نگاه کنید به Rubinstein (2014), p. 913.

3. Coler 2016

4. Danielle Keats Citron

5. Benjamin Wittes

یعنی اصلاحی را پیشنهاد می‌کنند که به صراحت از محدودیت مسئولیت وب‌سایت‌های «سامری بد»[1] و سایر میزبان‌های محتوایی که مجموعه‌ای تعریف شده از اقدامات غیرقانونی را «به طور هدفمند تشویق می‌کنند» جلوگیری کند.[2] در حالی که تمرکز آنها بر روی موضوعات قاچاق جنسی و پورنوگرافی بدون رضایت است، رویکردی مشابه برای مقابله با چالش‌های اطلاعات کاذب سیاسی می‌تواند در پیش گرفته شود.

مبارزه با اطلاعات کاذب احتمالاً نیاز به تنظیم ظریف و تدریجی CDA ۲۳۰ دارد. انگیزه شرکت در کارزارهای اطلاعات کاذب سیاسی با چالشی کردن بیشتر این تلاش‌ها برطرف نمی‌شود و آنها ممکن است مانند گذشته ادامه یابند. اگرچه ایجاد استثنائات CDA ۲۳۰ پاسخ‌ها را نسبت به نسخه‌های نظارتی یا قضایی سفت و سخت چابک‌تر خواهد کرد، این کارزارها احتمالاً کانال‌های جدیدی را برای فعالیت پیدا می‌کنند. همچنین ممکن است انتظار داشته باشیم که تأثیر این کارزارها با گذشت زمان تغییر کند. به عنوان مثال، عموم مردمی که به طور فزاینده‌ای نسبت به امکان کارزارهای اطلاعات کاذب برخط مراقب شده‌اند می‌توانند منجر به کاهش کلی تأثیر اقناعی آن کارزارها در آینده شوند. در عین حال، تکنیک‌های در حال بهبود برای ساخت جعل‌های قابل باور در ویدئو و سایر رسانه‌ها ممکن است به مرور زمان توانایی اقناع‌کننده این تاکتیک‌ها را افزایش دهند. ممکن ساختن تکامل باز این استثناها، به CDA ۲۳۰ اجازه می‌دهد تا خود را همان‌طور که فهم ما از این تکنیک‌ها و خطرشان در طول زمان تغییر می‌کند، تطبیق دهد.

1. Bad Samaritan
2. Citron and Wittes 2017
3. نگاه کنید مثلا به ویدئوی یوتیوبی متیاس نیزنر (Matthias Niessner)
"Face2Face: Real-time face capture and reenactment of RGB videos (CVPR 2016 Oral)," (www.youtube.com/watch?v=ohmajJTcpNk)
که نشان‌دهنده‌ی استفاده از یادگیری ماشین برای خلق شبیه‌سازی‌های قابل‌باور از سخنرانی رهبران سیاسی است.

جمع بندی

جمع‌بندی

سایه روشنِ جمع؟[1]

ظهـور اطلاعـات کاذب سیاسـی و فراگیـری اطلاعـات کاذب بـه طور کلی، نشـان‌دهنده یک شکسـت غیرمنتظـره در بازار برخـط تمثیلیِ ایده‌ها[2] اسـت. بسـیاری از صحبت‌هـا در اوایـل دوره رسـانه‌های اجتماعـی ایـن دیـدگاه را برجسـته می‌کردنـد کـه گفتمـان ارگانیـک بسـیاری از شـرکت‌کنندگان - «خِـرد» بسـیار ستایش‌شـده‌ی «جمعـی» - اطلاعـات غلـط را از ریشـه می‌خشـکاند و نمایشـی چنـد وجهـی از «حقیقـت» تولیـد می‌کنـد.[3] این امر همچنیـن در ایدئولـوژی کسـانی کـه سـکوها را طراحـی کردنـد، سـکوهایی کـه اکنـون به‌عنـوان بزرگ‌تریـن منابـع اطلاعـات کاذب قلمداد می‌شـوند، به صـورت ضمنـی وجود داشـت. همان‌طور کـه اِو ویلیامز،[4] یکـی از بنیان‌گذاران توییتـر، اظهـار داشـته کـه «مـن فکـر می‌کـردم وقتـی همـه بتواننـد آزادانـه صحبـت کننـد و اطلاعـات و ایده‌هـا را تبـادل کننـد، جهـان به طـور خودکار مـکان بهتـری خواهـد شـد . . . مـن در ایـن مورد در اشـتباه بـودم».[5]

موفقیت‌هـای اولیـه ماننـد ویکی‌پدیـا]در عمـل[به یک اصل گسـترده‌تر که جمـع افـراد می‌تواننـد به طور مؤثـر و قابل اعتماد به نفع حقیقـت و ضد کذب

1. the twilight of the crowd?
2. the figurative online marketplace of ideas
3. Surowiecki 2005; Taraborelli 2012
4. Ev Williams
5. Streitfeld 2017

مطالب را از صافی بگذرانند تعمیم نیافت.[1] صرف نظر از تأثیر علّی آن بر رفتار مربوط به رأی دادن و ادراکِ سیاسی، چرخه انتخابات ریاست‌جمهوری ۲۰۱۶ ایالات متحده حداقل نشان داد که تلاش‌های هماهنگ برای انتشار اطلاعات کاذب می‌تواند، به جای اینکه سریع از بین برود، در انتشار یافتن بسیار موفق باشد. تصفیه ارگانیک توسط خردِ جمعی آن‌قدر که ابتدا تصور می‌شد در برابر دست‌کاری عامدانه قوی نبود.[2]

تلاش‌ها برای اصلاح یا حذفِ CDA ۲۳۰ را باید در زمینه گسترده‌تری از عقب‌نشینی از رویکردهای باز مشارکتی به مسئله اطلاعات کاذب دیده شود. با توجه به نبود یا ضعف درک شده از یک جمع قوی، مداخلات به سمت مدیریت اطلاعات کاذب از طریق اقدامات قانونی یا قضایی یا قضاوت‌های مبتنی بر واسطه‌های سکوهای خصوصی تغییر یافته است. انجام این تغییر می‌تواند و باید نگرانی‌های طولانی‌مدت در مورد تأثیر و منافع سکوها در تنظیم‌گری بیان ایجاد کند.[3] این امر حتی نگرانی‌هایی طولانی‌مدت را درباره نقش دولت در تنظیم‌گری آزادی بیان برمی‌انگیزاند.[4]

با این وجود، تهدیدات ناشی از اطلاعات کاذب سیاسی، به ویژه کارزارهای پشتیبانی شده توسط دولت‌ها، همچنان در سراسر جهان گسترش می‌یابد. تلاش‌های روسیه برای استفاده از این تکنیک‌ها همچنان توسعه می‌یابد، و پیشرفت‌های اخیر نشان می‌دهد که کشورهای دیگر مانند چین در حال تجربه همان استراتژی‌ها برای پیشبرد منافع خودند.[5] به موازات این، دست‌کاری توسط بازیگران راست‌گرای داخلی در ایالات متحده نیز در حال پیشرفت است.[6]

۱. نگاه کنید مثلا به Tapscott and Williams (2010)، که کاربردی وسیع‌تر از مدل اشتراکی استفاده‌شده توسط ویکی‌پدیا را پیش‌بینی می‌کند.

2. Hwang 2017
3. Pasquale 2017
4. Pasquale 2017, pp. 15–14
5. Mozur 2017
6. Fang and Woodhouse 2017

با توجه به این، اصلاحاتِ سنجیده CDA ۲۳۰ ممکن است مسیری طولانی در کمک به جامعه مدنی و عمومی پیش رو داشته باشد تا به آن‌ها شانسِ مبارزه به‌وسیله تشویق سکوها برای تثبیت و متعادل کردن بازار ایده‌هایی که آن‌ها دارند و اجرا می‌کنند بدهد. کاهش یا حذف تکنیک‌های توزیعی که - صرف نظر از درستی یا نادرستی پیام‌های منتقل‌شده از طریق آن‌ها - اعتماد به گفتمان عمومی و فرایندهای مردم‌سالارانه را از بین می‌برد از اهمیت ویژه‌ای برخوردار است.

نهایتاً، هدف نهایی نباید تفویض کامل مسئولیت مربوط به ارزش صدق اطلاعات به حکومت یا سکوها باشد. در عوض، هدف اصلی باید تشویق عموم مردم باشد که خود در برابر ماهیت همیشه در حال توسعه اطلاعات کاذب قوی هستند. اگر خرد جمعی نسبت به یک دهه پیش از قوت کمتری برخوردار است، این امر تا حدی به این دلیل است که فضاهای برخط که مردم در آن فعالیت می‌کنند نتوانسته‌اند شرایط مناسبی را ایجاد کنند که تحت آن مردم بتوانند موفق عمل کنند. تنظیم دقیق مرزهای CDA ۲۳۰ نمایانگر گامی در تحقق و احیای مجدد این چشم‌انداز اصیل است.

منابع

• Alcindor, Y. (2017). Black lawmakers pressure Facebook over racially divisive Russian ads. New York Times, September 28. www.nytimes.com/28/09/2017/us/politics/facebook-russia-race-congressional-black-caucus.html

• Allcott, H., & Gentzkow, M. (2017). Social media and fake news in the 2016 election. Journal of Economic Perspectives, 236–211 ,(2)31.

• Angwin, J., Varner, M., & Tobin, A., (2017). Facebook enabled advertisers to reach «Jew haters." ProPublica, September 14. www.propublica.org/article/facebookenabled-advertisers-to-reach-jew-haters

• Arendt, H. (1971). Lying in politics: Reflections on the Pentagon Papers. The New York Review of Books, November 18. www.nybooks.com/articles/18/11/1971/lying-inpolitics-reflections-on-the-pentagon-pape/

• Barnouw, E. (1966). A Tower in Babel. New York: Oxford University Press.

• Barthel, M., & Mitchell, A. (2017). Democrats, Republicans Now Split on Support for Watchdog Role. Pew Research Center report. www.journalism.org/10/05/2017/ democrats-republicans-now-split-on-support-for-watchdog-role

• Belford, A., Cvetkovska, S., Sekulovska, B., & Dojc ˇinovic´, S. (2017). Leaked documents show Russian, Serbian attempts to meddle in Macedonia. OCCRP, June 4. www.occrp.org/en/spooksandspin/leaked-documents-show-russian-serbian-attemptsto-meddle-in-macedonia/

• Boxell, L., Gentzkow, M., & Shapiro, J. M. (2017). Greater Internet use is not associated with faster growth in political polarization among US demographic groups. Proceedings of the National Academy of Science, 10617–10612, (40)114.

• Bramble, N. W. (2012). Safe harbors and the national information infrastructure. Hastings Law Journal, 384–325 ,(2)64.

• Brown Barbour, V. S. (2015). Losing their license to libel: Revisiting § 230 immunity. Berkeley Technical Law Journal, 1560–1505 ,(2)30.

• Chen, A. (2015). The Agency. New York Times, June 2. www.nytimes.com/07/06/2015/ magazine/the-agency.html

• Chivvis, C. S. (2017). Understanding Russian «Hybrid Warfare": And What Can Be Done about It. RAND Corporation report. www.rand.org/pubs/testimonies/ CT468.html

• Citron, D., & Wittes, B. (2017). The Internet will not break: Denying bad Samaritans Section 230 immunity 17. SSRN. https://papers.ssrn.com/abstract=3007720

• Coleman, G. (2015). Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous. London: Verso.

• Coler, J. (2016). We tracked down a fake-news creator in the suburbs. Here's what we learned. NPR.org, November 23. www.npr.org/sections/alltechconsidered/503146770/23/11/2016/npr-finds-the-head-of-a-covert-fake-news-operation-in-the-suburbs

• Constine, J. (2017). Facebook security chief rants about misguided «algorithm" backlash. TechCrunch, October 7. http://social.techcrunch.com/07/10/2017/alexstamos/

• Diresta, R., & Harris, T. (2017). Why Facebook and Twitter can't be trusted to police themselves. POLITICO Magazine, November 1. http://politi.co/2zppJMA

• Dreyfuss, B. (2017). Seth Rich, conspiracy theorists, and Russiagate «Truthers." The Nation, August 25. www.thenation.com/article/seth-rich-conspiracy-theorists-andrussiagate-truthers/

• Dryzek, J. S. (2002). Deliberative Democracy and Beyond: Liberals, Critics, Contestations (1st ed.). New York: Oxford University Press.

• The Economist. (2017). Internet firms' legal immunity is under threat. The Economist, February 11. www.economist.com/news/business/-21716661platforms-havebenefited-greatly-special-legal-and-regulatory-treatment-internet-firms

• Epstein, D., & Graham, J. D. (2007). Polarized politics and policy consequences. Rand Corporation occasional paper. www.rand.org/content/dam/rand/pubs/ occasional_papers/2007/RAND_OP197.pdf

• Executive Office of the President. (2014). Big Data: Seizing Opportunities, Preserving Values. White House Washington report. https://obamawhitehouse.archives.gov/ sites/default/files/docs/big_data_privacy_report_may_2014_1.pdf

•Fang,L.,&Woodhouse,L.A.(2017).Howwhitenationalismbecamenormal online. The Intercept, August 25. https://theintercept.com/25/08/2017/video-how-whitenationalism-became-normal-online/

• Faris, R., Roberts, H., Etling, B. et al. (2017). Partisanship, Propaganda, and Disinformation: Online Media and the 2016 US Presidential Election. Cambridge: Berkman Klein Center.

• Feingold, R., Herman, L., Aravind, A. et al. (2017). Fake News & Misinformation: The Role of the Nation's Digital Newsstands

Facebook, Google, Twitter, and Reddit. Stanford Law School Law and Policy Lab report. https://www-cdn.law.stanford.edu/wp-content/uploads/10/2017/Fake-News-Misinformation-FINAL-PDF.pdf

• Feuerman, M. (2016). Court-side seats? The Communications Decency Act and the potential threat to StubHub and peer-to-peer marketplaces. Boston College Law Review, 260–227 ,(1)57.

• Finley, K. (2015). Pro-government Twitter bots try to hush Mexican activists. Wired, August 23. www.wired.com/08/2015/pro-government-twitter-bots-tryhush-mexican-activists/

• Foroohar, R. (2017). Facebook's self-policing needs an update. Financial Times, September 10. www.ft.com/content/f5d04d7e11-9481-e-7a9e-611d2f0ebb7f0

• Franken, A. (2017). We must not let Big Tech threaten our security, freedoms and democracy. The Guardian, November 8. www.theguardian.com/commentisfree/ 2017/nov/08/big-tech-security-freedoms-democracy-al-franken Amendment of Section 281 230

• Geiger, R. S. (2017). Beyond opening up the black box: Investigating the role of algorithmic systems in Wikipedian organizational culture. Big Data & Society. https://doi.org/2053951717730735/10.1177

• Goldman, E. (2017). The ten most important Section 230 rulings. SSRN. https://papers.ssrn.com/abstract=3025943

• Grimmelmann, J. (2015). The virtues of moderation. Yale Journal of Law and Technology, 109–42 ,(1)17.

• Halfaker, A., Geiger, R.S., Morgan, J.T. (2013). The rise and decline of an open collaboration system: How Wikipedia's reaction to popularity is causing its decline. American Behavioral Scientist, 688–664 ,(5)57.

• Howard, P., & Kollanyi, B. (2017). Social media companies must respond to the sinister reality behind fake news. The Observer, September 30. www.theguardian.com/ media/2017/sep/30/social-media-companies-fake-news-us-election

• Hwang, T. (2017). The madness of the crowd. Logic Magazine, March 15. https:// logicmag.io/-01the-madness-of-the-crowd/

• Hwang, T., & Woolley, S. (2017). The most important lesson from the dust-up over Trump's fake Twitter followers. Slate, June 2. www.slate.com/articles/technology/ future_tense/06/2017/the_lesson_of_the_dust_up_over_trump_s_fake_twitter_ followers.html

• Jeong, S. (2015). The Internet of Garbage. New York: Vox Media.

• Kafka, P. (2017). Facebook has started to flag fake news stories. Recode, March 4.www.recode.net/14816254/4/3/2017/facebook-fake-news-disputed-trumpsnopes-politifact-seattle-tribune

• Klein, D. O., & Wueller, J. R. (2017). Fake news: A legal perspective. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2958790

• Kollanyi, B., Bradshaw, S., & Neudert, L.-M. (2017). Social media, news and political information during the US election: Was polarizing content concentrated in swing states? Project on Computational Propaganda Data Memo No. 2017.8. http:// comprop.oii.ox.ac.uk/wp-content/uploads/sites/09/2017/89/Polarizing-Contentand-Swing-States.pdf

• Kosoff, M. (2017). The Russian troll farm that weaponized Facebook had American boots on the ground. The Hive, October 18. www.vanityfair.com/news/10/2017/the-russian-troll-farm-that-weaponized-facebook-had-americanboots-on-the-ground

• Lange-Ionatamishvili, E., Svetoka, S., & Geers, K. (2015). Strategic communication and social media in the Russia Ukraine conflict. In K. Geers (Ed.), Cyber War in Perspective: Russian Aggression Against Ukraine (pp. 111–103). Tallinn: NATO CCDCOE Publications.

• Lapowsky, I. (2017). Russia wouldn't need Trump's digital team to spread fake news. Wired, July 13. www.wired.com/story/russia-trump-targeting-fake-news/

• Lee, T. B. (2017). Dow Jones posts fake story claiming Google was buying Apple. Ars Technica, October 10. https://arstechnica.com/tech-policy/10/2017/dow-jonesposts-fake-story-claiming-google-was-buying-apple/

•Lessig,L.(1999).CodeandOtherLawsofCyberspace.NewYork:BasicBooks.

• Ling, J. (2017). Google chief says Google News will «engineer" Russian propaganda out of the feed. Motherboard, November 20. https://motherboard.vice.com/en_us/article/ pa39vv/eric-schmidt-says-google-news-will-delist-rt-sputnik-russia-fake-news

• Marantz, A. (2016). Trolls for Trump. The New Yorker, October 31. www.newyorker .com/magazine/31/10/2016/trolls-for-trump

• Marwick, A., & Lewis, R. (2017). Media Manipulation and Disinformation Online. Data & Society Research Institute report.

• Meacham, J. (2013). Thomas Jefferson: The Art of Power. New York: Random House.

• Metz, C. (2015). Google is 2 billion lines of code – and it's all in one place. Wired, September 16. www.wired.com/09/2015/google-2-billion-lines-codeand-oneplace/

• Mina, A. X. (2017). Knight Prototype Fund supports the Credibility Working Group. MisinfoCon, June 22. https://misinfocon.com/knight-prototype-fund-supports-thecredibility-working-group-c3dcc6667569

• Mozur, P. (2017). China spreads propaganda to U.S. on Facebook, a platform it bans at home. New York Times, November 8. www.nytimes.com/08/11/2017/technology/ china-facebook.html

• Mulford, C. (2008). Benjamin Franklin's savage eloquence: Hoaxes from the press at Passy, 1782. Proceedings of the American Philosophical Society, 530–490 ,(4)152.

• Museum of Hoaxes. Drunk Driving on the Internet. http://hoaxes.org/af_database/ permalink/drunk_driving_on_the_internet

• National Intelligence Council. (2017). Assessing Russian Activities and Intentions in Recent US Elections. Office of the Director of National Intelligence report, ICA 01-2017D.

• NCCIC (National Cybersecurity and Communications Integration Center). (2016). GRIZZLY STEPPE – Russian Malicious Cyber Activity. Department of Homeland Security report, Jar20296-16-a.

• Nielsen, R. K., & Graves, L. (2017). What do ordinary people think fake news is? Poor journalism and political propaganda. Columbia Journalism

Review, October 24. www.cjr.org/analysis/fake-news-study.php

• North, A. (2017). When a SWAT team comes to your house. New York Times, July 6. www.nytimes.com/06/07/2017/opinion/swatting-fbi.html

• NPR. (2017). Russian bots tweeting calls to fire McMaster, former FBI agent says. NPR.org, August 20. www.npr.org/544817844/20/08/2017/russian-bots-tweeting-callsto-fire-mcmaster-former-fbi-agent-says

• Oremus, W. (2016). Stop calling everything «fake news." Slate, December 6.www.slate.com/articles/technology/technology/12/2016/stop_calling_everything_fake_news.html

• Pasquale, F. (2017). The automated public sphere. SSRN. https://papers.ssrn.com/ abstract=3067552

• Pasquale, F., & Bracha, O. (2007). Federal Search Commission? Access, fairness and accountability in the law of search. SSRN. https://papers.ssrn.com/ abstract=1002453

• Paul, C., & Courtney, W. (2016). Russian propaganda is pervasive, and America is behind the power curve in countering it. Rand Corporation (blog), September 12. www.rand.org/blog/09/2016/russian-propaganda-is-pervasive-and-americais-behind.html

• Pennycook, G., Cannon, T. D., & Rand, D. G. (2017). Prior exposure increases perceived accuracy of fake news. SSRN. https://papers.ssrn.com/abstract=2958246

• Pennycook, G., & Rand, D. (2017). Assessing the effect of «disputed" warnings and source salience on perceptions of fake news accuracy. SSRN. https://papers.ssrn .com/abstract=3035384 Amendment of Section 283 230

• Prior, M. (2013). Media and political polarization. Annual Review of Political Science, 127–101 ,16.

• Quist, M. D. (2012). «Plumbing the depths" of the CDA: Weighing the competing Fourth and Seventh Circuit standards of ISP immunity under Section 230 of the Communications Decency Act. George Mason Law Review, 309–275 ,(1)20.

• Reidenberg, J. R., Debelak, J., Kovnot, J., & Miao, T. (2012). Section 230 of the Communications Decency Act: A survey of the legal literature and reform proposals. SSRN. https://papers.ssrn.com/abstract=2046230

• Robb, A. (2017). Pizzagate: Anatomy of a fake news scandal. Rolling Stone, November 16. www.rollingstone.com/politics/news/pizzagate-anatomy-of-afake-news-scandal-w511904

• Robertson, J., Riley, M., & Willis, A. (2017). How to hack an election. Bloomberg Businessweek, March 31. www.bloomberg.com/features/-2016how-to-hack-anelection/

• Rogers, J. (2017). Wikipedia and intermediary immunity: Supporting sturdy crowd systems for producing reliable information. Yale Law Journal Forum, 372–358 ,127.

• Rolling Stone. (2011). Musician Started Bon Jovi Death Hoax. Rolling Stone, December 28. www.rollingstone.com/music/news/musician-started-bon-jovideath-hoax20111228-

• Rubinstein, I. (2014). Voter privacy in the age of big data. SSRN. https://papers.ssrn.com/abstract=2447956

• Santa Clara University. (2017). Leading news outlets establish

transparency standards to help readers identify trustworthy news sources. The Trust Project, November 16. www.scu.edu/ethics/focus-areas/journalism-ethics/programs/the-trust-project/ trust-project-launches-indicators/

• Schreckinger, B. (2017). World war meme. POLITICO Magazine, March/ April. www .politico.com/magazine/story/03/2017/memes4-chan-trump-supporters-trolls-internet- 214856

• Seetharaman, D. (2017). Russian-backed Facebook accounts staged events around divisive issues. Wall Street Journal, October 30. www.wsj. com/articles/russian-backedfacebook-accounts-organized-events-on-all-sides-of-polarizing-issues1509355801-

• Seetharaman, D., & Wells, G. (2017). Tech giants disclose Russian activity on eve of congressional appearance. Wall Street Journal, October 30. www.wsj.com/articles/ facebook-estimates-126-million-people-saw-russian-backed-content1509401546-

• Silverman, C., & Singer-Vine, J. (2016). Most Americans who see fake news believe it, new survey says. BuzzFeed, December 6. www.buzzfeed. com/craigsilverman/fakenews-survey

• Streitfeld, D. (2017). «The Internet is broken": @ev is trying to salvage it. New York Times, May 20. www.nytimes.com/20/05/2017/technology/ evan-williamsmedium-twitter-internet.html

•Subramanian,S.(2017).InsidetheMacedonianfake-newscomplex.Wired, February 15. www.wired.com/02/2017/veles-macedonia-fake-news/

• Sullivan, M. (2017). It's time to retire the tainted term «fake news."

Washington Post, January 8. www.washingtonpost.com/lifestyle/style/its-time-to-retire-the-tainted-termfake-news/06/01/2017/a5a7516c-d11-375e945-6a76-f69a399dd5_story.html

• Sunstein, C. R. (1992). Free speech now. University of Chicago Law Review, 316–255 ,59.

• Surowiecki, J. (2005). The Wisdom of Crowds. New York: Anchor Books.

• Swire, B., Berinsky, A., Lewandowsky, S. et al. (2017). Processing political misinformation: Comprehending the Trump phenomenon. Royal Society OpenScience.http://doi.org/10.1098/rsos.160802

• Tapscott, D., & Williams, A. D. (2010). Wikinomics: How Mass Collaboration Changes Everything. New York: Penguin Group.

• Taraborelli, D. (2012). Seven years after Nature, pilot study compares Wikipedia favorably to other encyclopedias in three languages. Wikimedia Foundation (blog), August 2. https://blog.wikimedia.org/02/08/2012/seven-years-after-nature-pilotstudy-compares-wikipedia-favorably-to-other-encyclopedias-in-three-languages/

• Thompson, N. (2017). Our minds have been hijacked by our phones. Tristan Harris wants to rescue them. Wired, July 26. www.wired.com/story/our-minds-have-beenhijacked-by-our-phones-tristan-harris-wants-to-rescue-them/

• Tremble, C. (2017). Wild Westworld: Section 230 of the CDA and Social Networks' Use of Machine-Learning Algorithms, Fordham Law Review 82586.

• Tynan, D. (2016). How Facebook powers money machines for obscure political «news" sites. The Guardian, August 24. www.theguardian.com/

technology/2016/aug/24/ facebook-clickbait-political-news-sites-us-election-trump

• Volokh, E., & Falk, D. M. (2012). First Amendment protection for search engine search results. White Paper commissioned by Google. www.volokh.com/wp-content/ uploads/05/2012/SearchEngineFirstAmendment.pdf

• Wingfield, N., Isaac, M., & Benner, K. (2016). Google and Facebook take aim at fake news sites. New York Times, November 14. www.nytimes.com/15/11/2016/technology/ google-will-ban-websites-that-host-fake-news-from-using-its-ad-service.html

• Wintour, P. (2017). Russian hackers to blame for sparking Qatar crisis, FBI inquiry finds. The Guardian, June 7. www.theguardian.com/world/2017/jun/07/russianhackers-qatar-crisis-fbi-inquiry-saudi-arabia-uae

• Woolley, S. C., & Howard, P. N. (2017). Computational propaganda worldwide: Executive summary. Project on Computational Propaganda Working Paper No. 2017.11. http://comprop.oii.ox.ac.uk/publishing/working-papers/computationalpropaganda-worldwide-executive-summary/

• Wu, T. (2013). Machine speech. University of Pennsylvania Law Review, 1533–1495 ,161

csri.majazi.ir