



مرکز پژوهش‌های اتاق ایران

تنظیم‌گری اقتصاد دیجیتال

بررسی حقوقی و اقتصادی

لایحه مقابله با محتوای خلاف واقع در فضای مجازی در بستر جهانی



مرداد ۱۴۰۴



مرکز پژوهش‌های اتاق ایران

تنظیم‌گری اقتصاد دیجیتال:

بررسی حقوقی و اقتصادی لایحه مقابله با محتوای خلاف واقع در فضای مجازی در بستر جهانی

تهیه و تدوین: محمدعبده ابطحی

ناظران علمی: عیسی منصوری، فرزانه نادری، مجتبی قاسمی

تاریخ انتشار: مرداد ۱۴۰۴

واژگان کلیدی: تنظیم‌گری اقتصاد دیجیتال، محتوای خلاف واقع، اخبار جعلی، فضای مجازی، مقررات‌گذاری محتوا، قانون‌گذاری اینترنت، حقوق دیجیتال، آزادی بیان آنلاین، اقتصاد دیجیتال، قوانین بین‌المللی فضای مجازی

نشانی: تهران، خیابان طالقانی، نبش خیابان شهید موسوی (فرصت)، پلاک ۱۷۵

مرکز پژوهش‌های شبکه‌های اجتماعی:

Instagram: rc.iccima.ir@

Telegram: rc_iccima@

Twitter: rc_iccima@

فهرست مطالب

خلاصه مدیریتی.....	۴
۱- کالبدشکافی «لایحه مقابله با انتشار محتوای خلاف واقع»	۵
۱-۱- اهداف اعلامی	۵
۲-۱- دامنه شمول و تعاریف: معماری ابهام	۵
۳-۱- چارچوب تکالیف پیشگیرانه و مسئولیت سکوها	۶
۴-۱- معماری اجرایی: یک مدل دولت‌محور	۶
۵-۱- چارچوب تنبیهی: جرم‌انگاری	۶
۲- موج‌های اقتصادی: تأثیر بر اکوسیستم دیجیتال ایران	۷
۱-۲- هزینه بالای انطباق و فعالیت	۷
۲-۲- فضای نوآوری، استارت‌آپ‌ها و سرمایه‌گذاری	۷
۳-۲- آینده اقتصاد محتوا و اشتغال دیجیتال	۸
۳- اکوسیستم جهانی: تحلیل تطبیقی قوانین تنظیم‌گری محتوا	۸
۱-۳- اتحادیه اروپا: مدل هم‌تنظیم‌گری و مبتنی بر ریسک	۸
۲-۳- آلمان: مدل «برون‌سپاری اجرا»	۹
۳-۳- فرانسه: مدل «مداخله جراحی‌وار»	۹
۴-۳- بریتانیا: مدل «وظیفه مراقبت»	۹
۵-۳- ایالات متحده آمریکا: مدل «مصونیت سکو»	۹
۶-۳- چین: مدل «کنترل کامل دولتی»	۱۰
۷-۳- ترکیه: مدل «اجبار فزاینده»	۱۰
۸-۳- عربستان سعودی: مدل «ممنوعیت‌های مبهم»	۱۰
۹-۳- امارات متحده عربی: مدل «نظم عمومی»	۱۱
۱۰-۳- جمهوری کره: مدل «دموکراتیک مناقشه‌برانگیز»	۱۱
۱۱-۳- سایر کشورها	۱۱
۴- سنتز تطبیقی: ماتریس مقایسه جهانی تنظیم‌گری دیجیتال	۱۱
۱-۴- جدول تطبیقی جامع قوانین تنظیم‌گری محتوای آنلاین	۱۱
۲-۴- شناسایی مدل‌ها: طیفی از کنترل	۱۵
۵- توصیه‌های راهبردی و تحلیل نهایی	۱۵
۱-۵- راهکارهای کاهش اثرات منفی اقتصادی	۱۵
۲-۵- تقویت رویه‌های عادلانه و حاکمیت قانون	۱۵
۳-۵- ملاحظات نهایی	۱۶
۶- فهرست منابع	۱۶

خلاصه مدیریتی

این گزارش به تحلیل جامع «لایحه مقابله با انتشار محتوای خلاف واقع در فضای مجازی» می‌پردازد و تأثیرات حقوقی و اقتصادی آن را در چارچوب روندهای جهانی تنظیم‌گری اینترنت ارزیابی می‌کند. یافته‌های کلیدی این گزارش به شرح زیر است:

- **ویژگی‌های اصلی لایحه:** لایحه حاضر با تعاریف گسترده و مبهم، مسئولیت‌های سنگین و پیشگیرانه برای سکوها، مجازات‌های کیفری شدید و یک ساختار اجرایی دولت‌محور مشخص می‌شود. این ویژگی‌ها در مجموع، فضایی از عدم قطعیت حقوقی ایجاد کرده و زمینه را برای محدودیت گسترده آزادی بیان و خودسانسوری فراهم می‌سازند.
- **تحلیل تطبیقی:** در مقایسه با مدل‌های بین‌المللی، لایحه ایران بیشترین شباهت را به مدل «کنترل دولتی» دارد که در کشورهای نظیر چین، ترکیه و عربستان سعودی مشاهده می‌شود. این مدل در تضاد کامل با مدل «مصونیت سکو» در آمریکا (ذیل بخش ۲۳۰) و مدل «هم‌تنظیم‌گری مبتنی بر ریسک» در اتحادیه اروپا (ذیل قانون خدمات دیجیتال) قرار می‌گیرد که بر حفظ فرآیندها، شفافیت و حقوق کاربر تأکید دارند.
- **ریسک‌های اقتصادی حیاتی:** این لایحه با تحمیل هزینه‌های سنگین انطباق، ایجاد موانع ورود برای استارت‌آپ‌ها و تضعیف امنیت سرمایه‌گذاری، پتانسیل از بین بردن نوآوری در اقتصاد دیجیتال ایران را دارد. جرم‌انگاری فعالیت تولیدکنندگان محتوا و اینفلوئنسرها، اقتصاد نوپای محتوا را مستقیماً هدف قرار داده و می‌تواند به فرسایش این بخش مهم از اشتغال‌زایی دیجیتال منجر شود.
- **توصیه‌های کلیدی:** برای کاهش اثرات منفی، پیشنهاد می‌شود تعاریف کلیدی در لایحه به صورت دقیق و محدود بازنویسی شوند، برای کسب‌وکارهای کوچک و متوسط (SMEs) معافیت‌های موقت در نظر گرفته شود، مجازات‌های کیفری (به‌ویژه حبس) با جرائم مدنی متناسب جایگزین گردند و یک نهاد تنظیم‌گر مستقل به جای نهادهای سیاسی-امنیتی فعلی، مسئولیت نظارت و اجرا را بر عهده گیرد.

در مجموع، هرچند مقابله با انتشار اطلاعات نادرست یک هدف مشروع است، اما رویکرد اتخاذ شده در این لایحه، به دلیل عدم تناسب و فقدان سازوکارهای حمایت از حقوق بنیادین، تهدیدی جدی برای آینده اقتصاد دیجیتال و فضای مدنی آنلاین در ایران محسوب می‌شود.

۱. کالبدشکافی «لایحه مقابله با انتشار محتوای خلاف واقع»

این بخش به تحلیل دقیق حقوقی لایحه می‌پردازد تا بنیانی برای ارزیابی‌های اقتصادی و تطبیقی بعدی فراهم آورد.

۱-۱- اهداف اعلامی

لایحه حاضر با یک مقدمه توجیهی آغاز می‌شود که اهداف آن را «مقابله با تبعات منفی ناشی از نشر و بازنشر محتوای خبری تحریف شده و خلاف واقع» اعلام می‌کند. این اهداف شامل مواردی چون جلوگیری از ضربه زدن به حیثیت اشخاص، آسیب به امنیت روانی، عوام‌فریبی، بی‌اعتبارسازی نهادهای حاکمیتی، ایجاد ترس و وحشت عمومی و تضعیف انسجام ملی است.

۲-۱- دامنه شمول و تعاریف: معماری ابهام

یکی از چالش‌برانگیزترین جنبه‌های لایحه، تعاریف گسترده و مبهم آن است که دامنه شمول قانون را به شکل چشمگیری افزایش می‌دهد.

- **تعریف فراگیر «محتوا»:** بر اساس ماده ۱، بند ۱، «محتوا» شامل هرگونه داده خبری دیجیتال درباره «امور عمومی اثرگذار بر عموم جامعه» می‌شود که طیف وسیعی از موضوعات امنیتی، سیاسی، اقتصادی، فرهنگی و اجتماعی را در بر می‌گیرد. این تعریف آن‌قدر گسترده است که تقریباً هر نوع گفتمان عمومی، از گزارش‌های خبری حرفه‌ای گرفته تا نقد و نظر شخصی درباره اقدامات دولتی را شامل می‌شود.
- **تعریف مسئله‌ساز «محتوای خلاف واقع»:** چالش اصلی در ماده ۱، بند ۳ نهفته است. «محتوای خلاف واقع» نه تنها به محتوایی که «ما به ازایی در واقعیت نداشته» باشد اطلاق می‌شود، بلکه «شکل تحریف شده‌ای از یک واقعیت» یا «انعکاس ناقص واقعیت مانند پنهان کردن عمدی بخش‌هایی از آن» را نیز در بر می‌گیرد. معیار تشخیص، این است که آیا محتوا «عرفاً موجب تشویش اذهان، شبهه یا فریب مخاطب یا هتک حیثیت دیگران شود» یا خیر. این معیار «عرفی» و ذهنی، فاقد هرگونه شاخص عینی است و به نهادهای اجرایی و قضایی این اختیار را می‌دهد که هر محتوای منتقدانه‌ای را به سادگی ذیل این عنوان طبقه‌بندی کنند.
- **تعریف گسترده «سکو» و «درگاه»:** بر اساس ماده ۱، بندهای ۴ و ۵، «سکو» به زیرساخت‌های اصلی مانند اینستاگرام یا تلگرام و «درگاه» به بسترهایی مانند کانال‌های تلگرامی یا صفحات اینستاگرامی اطلاق می‌شود. حد نصاب یک «درگاه» برای مشمول شدن در این قانون، داشتن بیش از «یک هزارم جمعیت کشور» به عنوان عضو است. این حد نصاب نسبتاً پایین، تعداد بسیار زیادی از جوامع آنلاین، صفحات پرمخاطب و کانال‌های خبری را ذیل این قانون قرار می‌دهد. علاوه بر این، ماده ۲ به صراحت دامنه شمول قانون را به تمام سکوهایی داخلی و خارجی، صرف‌نظر از محل ثبت یا استقرار تجهیزات فنی، گسترش می‌دهد که نشان‌دهنده رویکرد فرامرزی و حداکثری قانون‌گذار است.

این ساختار مبتنی بر ابهام، عملاً یک «فرض تقصیر» برای محتوای آنلاین ایجاد می‌کند. برخلاف نظام‌های حقوقی که در آن آزادی بیان اصل است مگر آنکه ضرر آن در دادگاه اثبات شود، این لایحه سکوها و کاربران را وادار می‌کند تا دائماً ثابت کنند محتوایشان طبق استانداردهای مبهم و تعریف‌شده توسط دولت، «خلاف واقع» نیست. این وارونگی بار اثبات، به خودی خود یک اثر بازدارنده و

سردکننده^۱ قدرتمند ایجاد می‌کند.

۳-۱- چارچوب تکالیف پیشگیرانه و مسئولیت سکوها

لایحه مجموعه‌ای از تکالیف سنگین و پیشگیرانه را بر دوش مدیران سکوها و درگاه‌های نشر قرار می‌دهد که فراتر از مدل‌های واکنشی^۲ است.

- **تکالیف سکوها و درگاه‌ها (ماده ۴):** این تکالیف شامل موارد زیر است:
 - ✓ ثبت‌نام و به‌روزرسانی مداوم اطلاعات در یک «سامانه» دولتی.
 - ✓ ایجاد نقاط تماس برای دریافت دستورات از مراجع قضایی، کارگروه و سامانه.
 - ✓ «تلاش برای راستی‌آزمایی محتوا» هنگام نشر؛ تکلیفی مبهم که هزینه و مسئولیت بالایی را به سکوها تحمیل می‌کند.
 - ✓ برچسب‌گذاری محتوای مشکوک با عناوینی چون «محتوای مشکوک».
 - ✓ حذف فوری محتوا پس از دریافت ابلاغ از نهادهای ذی‌صلاح.
- **تکالیف مضاعف برای سکوها (ماده ۵):** سکوهاى اصلی موظفند ابزارهای لازم را برای درگاه‌ها فراهم کنند، «ضوابط و مرامنامه رفتار حرفه‌ای» تدوین و اجرا کنند، سازوکار احراز هویت برای کاربران متقاضی تیک تأیید یا تراکنش مالی فراهم آورند و مهم‌تر از همه، «سازوکار رصد و پایش محتوای خلاف واقع با استفاده از فناوری‌های نوین» را ایجاد کنند. این بند عملاً سکوها را به بازوی نظارتی دولت تبدیل می‌کند.

۴-۱- معماری اجرایی: یک مدل دولت‌محور

ساختار نظارت و اجرای این لایحه کاملاً در اختیار نهادهای دولتی، قضایی و امنیتی است و هیچ اثری از یک نهاد تنظیم‌گر مستقل در آن دیده نمی‌شود.

- **نقش محوری وزارت فرهنگ و ارشاد اسلامی:** این وزارتخانه مسئولیت ایجاد و مدیریت «سامانه» مرکزی، صدور مجوز برای مؤسسات راستی‌آزمای خصوصی و ارجاع تخلفات به قوه قضائیه را بر عهده دارد. قرار دادن یک وزارتخانه سیاسی در مرکز تنظیم‌گری گفتمان، استقلال این فرآیند را به کلی از بین می‌برد.
- **«کارگروه تعیین مصادیق محتوای مجرمانه»:** این کارگروه که سابقه‌ای طولانی در فیلترینگ گسترده دارد، به عنوان یکی از مراجع اصلی تشخیص «محتوای خلاف واقع» تعیین شده است. این امر قدرت یک نهاد امنیتی-قضایی را در این زمینه رسمیت می‌بخشد.
- **قوه قضائیه:** این قوه به عنوان مرجع نهایی برای صدور احکام کیفری عمل می‌کند.
- **تکالیف دستگاه‌های اجرایی:** بر اساس ماده ۱۰، تمام نهادهای دولتی موظفند در حوزه خود به رصد محتوای خلاف واقع پرداخته و از طریق سامانه، دستور تکذیب یا اصلاح صادر کنند. این ماده عملاً کل بدنه دولت را به یک دستگاه عظیم پلیس محتوا تبدیل می‌کند.

۵-۱- چارچوب تنبیهی: جرم‌انگاری

- شدت مجازات‌های پیش‌بینی‌شده در لایحه، نشان‌دهنده رویکرد کیفری و امنیتی آن به مسئله انتشار اطلاعات نادرست است.
- **مجازات برای کاربران و سکوها (ماده ۱۲):** انتشار «عالمانه و عامدانه» محتوای خلاف واقع، علاوه بر جبران خسارت، مستوجب حبس درجه شش (بیش از شش ماه تا دو سال)، جزای نقدی سنگین (از ۱۶۵ میلیون تا ۳۳۰ میلیون تومان) و محرومیت از فعالیت آنلاین تا دو سال است. این ماده مستقیماً عمل به اشتراک‌گذاری اطلاعات را جرم‌انگاری می‌کند.

1. chilling effect
2. notice and takedown

- **تشدید مجازات‌ها:** لایحه مجموعه‌ای از شرایط را برای تشدید مجازات در نظر گرفته است:
 - ✓ **ماده ۱۳:** اگر محتوا علیه «امنیت داخلی یا خارجی» یا «نظم عمومی» باشد، مجازات به حبس یا جزای نقدی درجه پنج (حبس بیش از دو تا پنج سال و جزای نقدی از ۸۰ تا ۱۶۵ میلیون تومان) افزایش می‌یابد. مرتکب ممکن است دو تا شش سال نیز از فعالیت یا اشتغال در امور مرتبط با نشر محتوا محروم گردد.
 - ✓ **ماده ۱۴:** انتشار محتوای خلاف واقع در «مواقع بحرانی» یا «وضعیت جنگی» مجازات را یک درجه تشدید می‌کند.
 - ✓ **ماده ۱۵:** اگر جرم توسط یک «شخص دارای قدرت تأثیرگذاری» (اینفلوئنسر)، یا حساب کاربری جعلی، یا به صورت سازمان‌یافته ارتکاب یابد، مجازات یک درجه تشدید می‌شود. این ماده به وضوح می‌تواند روزنامه‌نگاران، فعالان مدنی و منتقدان را هدف قرار دهد.
- **مجازات برای مقامات دولتی:** مواد ۱۷ و ۱۸ برای مدیران دستگاه‌های اجرایی که تکذیبیه خلاف واقع منتشر کنند یا از درج تکذیبیه خودداری ورزند، مجازات‌هایی مانند انفصال از خدمت در نظر گرفته است. هرچند این مواد ظاهری از پاسخگویی دولت را ایجاد می‌کنند، اما در عمل، با توجه به ساختار قدرت، احتمال اجرای آنها علیه مقامات دولتی بسیار کم است. در نهایت، ترکیب تعاریف مبهم، تکالیف پیشگیرانه، ساختار اجرایی غیرمستقل و مجازات‌های کیفری شدید، این لایحه را نه به ابزاری برای مقابله با اطلاعات نادرست، بلکه به یک مکانیزم جامع برای کنترل فضای اطلاعاتی و سرکوب هرگونه صدای مخالف یا منتقد تبدیل می‌کند.

۲. اثرات اقتصادی: تأثیر بر اکوسیستم دیجیتال ایران

این بخش با بهره‌گیری از مدل‌های تطبیقی، به پیش‌بینی تأثیرات اقتصادی لایحه بر اکوسیستم دیجیتال ایران می‌پردازد.

۱-۲- هزینه بالای انطباق و فعالیت

اجرای این لایحه هزینه‌های مستقیم و غیرمستقیم هنگفتی را بر کسب‌وکارهای دیجیتال تحمیل خواهد کرد.

- **هزینه‌های مستقیم برای سکوها:** سکوها برای اجرای تکالیف مواد ۴ و ۵، نیازمند سرمایه‌گذاری عظیم در فناوری‌های پایش، فیلترینگ و برچسب‌گذاری محتوا هستند. این امر شامل استخدام تیم‌های بزرگ انسانی برای بازبینی محتوا و خرید یا توسعه سیستم‌های هوش مصنوعی پیچیده می‌شود.
- **تحلیل هزینه تطبیقی:** تجربیات جهانی نشان‌دهنده هزینه‌های سرسام‌آور چنین قوانینی است. قانون NetzDG آلمان سالانه حدود ۲۰۴ میلیون یورو برای اقتصاد این کشور هزینه داشته و هزینه نیروی انسانی برای هر مورد حذف محتوا به بیش از ۵,۱۱۶ دلار رسیده است. قانون ایمنی آنلاین بریتانیا نیز هزینه‌ای چند صد میلیون پوندی برای کسب‌وکارها به همراه دارد و پیش‌بینی می‌شود هزینه‌های جاری تعدیل محتوا طی ده سال به ۱.۳۴ تا ۲.۵ میلیارد پوند برسد. اعمال چنین هزینه‌هایی بر اقتصاد دیجیتال نوپای ایران، که فاقد زیرساخت‌ها و منابع مالی اقتصادهای توسعه‌یافته است، می‌تواند فلج‌کننده باشد.
- **هزینه نمایندگی محلی:** الزام ضمنی سکوها خارجی به داشتن نماینده محلی برای پاسخگویی به مراجع قضایی و دولتی، مشابه الزامات قانون ترکیه، هزینه‌های عملیاتی قابل توجهی را به آنها تحمیل کرده و ممکن است به خروج برخی از آنها از بازار ایران منجر شود.

۲-۲- فضای نوآوری، استارت‌آپ‌ها و سرمایه‌گذاری

این لایحه فضایی نامساعد برای رشد استارت‌آپ‌ها و جذب سرمایه ایجاد می‌کند.

- **موانع ورود:** هزینه‌های بالای انطباق و ریسک‌های حقوقی، موانع ورود غیرقابل عبوری برای استارت‌آپ‌های فناوری ایرانی ایجاد می‌کند. آنها توانایی مالی و حقوقی برای برآورده ساختن این الزامات پیچیده را از روز اول فعالیت ندارند. این امر

مستقیماً با هدف اعلامی حمایت از اقتصاد دیجیتال داخلی در تضاد است.

- **اثر دلسردکننده بر سرمایه‌گذاری خطرپذیر:** عدم قطعیت قوانین و ریسک بالای مسدود شدن یک پلتفرم یا زندانی شدن مدیران آن، سرمایه‌گذاری خطرپذیر داخلی و خارجی در بخش محتوا و رسانه‌های اجتماعی ایران را به شدت پریسک می‌سازد. داده‌های مربوط به آلمان پس از اجرای NetzDG، که شاهد کاهش چشمگیر سرمایه‌گذاری در رسانه‌های اجتماعی در مقایسه با فرانسه و بریتانیا بود، یک هشدار جدی در این زمینه است.
- **«خالی شدن» اقتصاد دیجیتال:** این لایحه احتمالاً به انحصار بازار توسط بازیگران بزرگ، دولتی یا خارجی که توانایی تحمل هزینه‌ها و ریسک‌ها را دارند، منجر خواهد شد. این امر رقابت و نوآوری را که خون جاری در یک اکوسیستم دیجیتال پویاست، از بین می‌برد.

۳-۲- آینده اقتصاد محتوا و اشتغال دیجیتال

- **تهدید مستقیم برای تولیدکنندگان محتوا:** ماده ۱۵ به طور خاص افراد تأثیرگذار، شامل روزنامه‌نگاران، شهروند-خبرنگاران، اینفلوئنسرهای رسانه‌های اجتماعی و فعالان آموزشی را هدف قرار می‌دهد. تهدید به حبس برای انتشار محتوایی که «خلاف واقع» تشخیص داده شود، می‌تواند اقتصاد محتوا را نابود کند.
- **چرخه معیوب خودسانسوری:** با افزایش ریسک‌گریزی تولیدکنندگان محتوا، کیفیت و تنوع محتوای آنلاین کاهش می‌یابد. این امر جذابیت سکوها را برای کاربران کم کرده و به نوبه خود درآمد تبلیغاتی و پایداری مالی فعالیت به عنوان یک تولیدکننده محتوای تمام‌وقت را کاهش می‌دهد. این چرخه بازخورد منفی، به کوچک شدن اقتصاد دیجیتال منجر می‌شود. این قانون، الزامات تنظیم‌گری دیجیتال قرن بیست و یکمی را که حتی برای اقتصادهای پیشرفته نیز پرهزینه است، بر یک اقتصاد دیجیتال در حال توسعه تحمیل می‌کند و همزمان، یک محیط ریسک حقوقی تمرکزگرایانه قرن بیستمی را به وجود می‌آورد. این ترکیب، از نظر اقتصادی به شدت ناکارآمد است و به احتمال زیاد به فرار سرمایه، فرار مغزهای حوزه فناوری و انزوای اکوسیستم دیجیتال ایران منجر خواهد شد و اهداف اعلامی کشور برای توسعه اقتصادی را تضعیف می‌کند. در نهایت، این لایحه از منظر اقتصادی یک حرکت متناقض است.

۳. اکوسیستم جهانی: تحلیل تطبیقی قوانین تنظیم‌گری محتوا

این بخش به تحلیل روایی قوانین در مناطق و کشورهای منتخب می‌پردازد که داده‌های آن در جدول بخش بعد ترکیب خواهد شد.

۳-۱- اتحادیه اروپا: مدل هم‌تنظیم‌گری و مبتنی بر ریسک

- **قانون:** قانون خدمات دیجیتال (DSA)، لازم‌الاجرا از فوریه ۲۰۲۴.
- **مفاد کلیدی:** این قانون یک رویکرد لایه‌بندی شده و مبتنی بر ریسک دارد. تکالیف پایه برای همه واسطه‌های آنلاین تعریف شده و این تکالیف برای سرویس‌های میزبانی، سکوه‌های آنلاین و به ویژه سکوه‌های آنلاین بسیار بزرگ (VLOPs) تشدید می‌شود. تمرکز بر شفافیت فرآیندهاست، نه سانسور پیش از انتشار. این قانون «الگوهای تاریک»^۱ و برخی تبلیغات هدفمند را ممنوع می‌کند.
- **نظام نظارتی:** ساختاری دوگانه دارد. «هماهنگ‌کنندگان خدمات دیجیتال» ملی بر اکثر سکوها نظارت می‌کنند و کمیسیون اروپا مستقیماً بر VLOPs نظارت دارد.
- **مجازات‌ها:** جریمه تا ۶ درصد از گردش مالی سالانه جهانی برای VLOPs.
- **سازوکار اعتراض:** حقوق کاربری قدرتمندی پیش‌بینی شده که شامل حق شکایت مؤثر، سیستم اعتراض داخلی سکو و

1. Very Large Online Platforms یا VLOPs

2. dark patterns

دسترسی به نهادهای مستقل حل اختلاف خارج از دادگاه می‌شود.

۲-۳- آلمان: مدل «برون‌سپاری اجرا»

- **قانون:** قانون اجرای شبکه (NetzDG)، مصوب ۲۰۱۸.
- **مفاد کلیدی:** شبکه‌های اجتماعی بزرگ را ملزم می‌کند محتوای «آشکارا غیرقانونی» را ظرف ۲۴ ساعت و سایر محتوای غیرقانونی را ظرف ۷ روز حذف کنند. تمرکز این قانون بر اجرای آنلاین قوانین کیفری موجود آلمان است.
- **نظام نظارتی:** اداره فدرال دادگستری می‌تواند برای عدم انطباق سیستمی جریمه وضع کند. اما اجرای قانون عمدتاً به خود سکوها واگذار شده است.
- **مجازات‌ها:** جریمه تا ۵۰ میلیون یورو برای عدم انطباق سیستمی.
- **سازوکار اعتراض:** خود قانون یک فرآیند اعتراض قضایی برای کاربرانی که محتوایشان حذف شده پیش‌بینی نکرده که این یکی از انتقادات اصلی به آن است. کاربران باید به دادگاه‌های عمومی مدنی مراجعه کنند.

۳-۳- فرانسه: مدل «مداخله جراحی‌وار»

- **قانون:** قانون مبارزه با دستکاری اطلاعات، مصوب ۲۰۱۸.
- **مفاد کلیدی:** این قانون به طور خاص بر دوره‌های انتخاباتی (۳ ماه قبل از انتخابات) متمرکز است. یک رویه قضایی مدنی سریع برای مسدود کردن اطلاعات نادرستی که به صورت انبوه، مصنوعی و با هدف تأثیرگذاری بر نتیجه رأی‌گیری منتشر می‌شوند، ایجاد می‌کند. همچنین سکوها را به شفافیت در مورد محتوای سیاسی پولی ملزم می‌کند.
- **نظام نظارتی:** قوه قضائیه (برای دستورات حذف) و نهاد تنظیم‌گر رسانه (CSA/Arcom) برای تعلیق پخش‌کنندگان تحت کنترل دولت‌های خارجی.
- **مجازات‌ها:** جریمه نقدی و حبس برای عدم رعایت تکالیف شفافیت.
- **سازوکار اعتراض:** رویه قضایی آن ذاتاً خشک است و حق استیناف (تجدیدنظر)، هرچند در بازه زمانی بسیار کوتاه، در آن پیش‌بینی شده است.

۳-۴- بریتانیا: مدل «وظیفه مراقبت»

- **قانون:** قانون ایمنی آنلاین، مصوب ۲۰۲۳.
- **مفاد کلیدی:** یک «وظیفه مراقبت»^۱ بر سکوها برای محافظت از کاربران، به ویژه کودکان، در برابر محتوای غیرقانونی و مضر تحمیل می‌کند. یک سیستم لایه‌بندی شده از سکوها با وظایف فزاینده ایجاد می‌کند و آنها را ملزم به ارزیابی ریسک و اقدامات پیشگیرانه می‌کند.
- **نظام نظارتی:** یک تنظیم‌گر مستقل و قدرتمند به نام آفکام (Ofcom) که آیین‌نامه‌های اجرایی را تدوین کرده و اختیارات اجرایی قوی دارد.
- **مجازات‌ها:** جریمه تا ۱۸ میلیون پوند یا ۱۰ درصد از درآمد کل، و مسئولیت کیفری بالقوه برای مدیران ارشد.
- **سازوکار اعتراض:** سکوها باید سازوکارهای گزارش‌دهی و رسیدگی به شکایات شفاف برای کاربران داشته باشند. آفکام به عنوان نهاد نظارتی نهایی عمل می‌کند.

۳-۵- ایالات متحده آمریکا: مدل «مصونیت سکو»

- **قانون:** بخش ۲۳۰ قانون نجابت (نزاکت) ارتباطات^۲، مصوب ۱۹۹۶.

1. duty of care

2. Communications Decency Act

- **مفاد کلیدی:** مصونیت گسترده‌ای را برای «سرویس‌های کامپیوتری تعاملی» در برابر مسئولیت ناشی از محتوای منتشر شده توسط اشخاص ثالث فراهم می‌کند. آنها نمی‌توانند به عنوان «ناشر یا گوینده» تلقی شوند. این مصونیت از تصمیمات آنها برای تعدیل محتوا (میزبانی یا حذف) محافظت می‌کند.
- **نظام نظارتی:** وجود ندارد. اجرا از طریق دادگاه‌ها صورت می‌گیرد که به طور مداوم مصونیت بخش ۲۳۰ را تأیید کرده‌اند.
- **مجازات‌ها:** برای سکوها در قبال محتوای شخص ثالث (به جز موارد استثنایی مانند جرائم فدرال و مالکیت فکری) مجازاتی وجود ندارد.
- **سازوکار اعتراض:** شکایت علیه تولیدکننده اصلی محتوا صورت می‌گیرد، نه سکو.

۳-۶- چین: مدل «کنترل کامل دولتی»

- **قانون:** قانون امنیت سایبری (۲۰۱۷) و مقررات مرتبط.
- **مفاد کلیدی:** یک چارچوب مسئولیت مطلق را تحمیل می‌کند که در آن سکوها باید به طور پیشگیرانه طیف وسیعی از محتوای ممنوعه، از جمله هر چیزی که به «امنیت ملی» یا «نظم عمومی» آسیب برساند را رصد، فیلتر و حذف کنند.
- **نظام نظارتی:** چندین نهاد دولتی، از جمله اداره فضای سایبری چین (CAC) و وزارت امنیت عمومی، نقش‌های اجرایی قدرتمند و همپوشانی دارند.
- **مجازات‌ها:** جریمه، لغو مجوز کسب‌وکار و مسئولیت کیفری برای افراد و شرکت‌ها.
- **سازوکار اعتراض:** فرآیند اعتراض در درون سیستم اداری و قضایی دولت انجام می‌شود که فاقد استقلال است. این سیستم عمدتاً برای اجرای اراده دولت طراحی شده، نه برای رسیدگی به شکایات کاربران.

۳-۷- ترکیه: مدل «اجبار فزاینده»

- **قانون:** قانون شماره ۵۶۵۱ (اصلاحی ۲۰۲۰) و «قانون ضد اطلاعات نادرست» (۲۰۲۲).
- **مفاد کلیدی:** سکوها را ملزم به تعیین نماینده محلی، پاسخ به دستورات حذف ظرف ۴۸ ساعت و ذخیره داده‌های کاربران در داخل کشور می‌کند. قانون «ضد اطلاعات نادرست» انتشار «اطلاعات گمراه‌کننده» را با مجازات حبس تا ۳ سال جرم‌انگاری می‌کند.
- **نظام نظارتی:** اداره فناوری اطلاعات و ارتباطات (BTK) و قوه قضائیه که هر دو تحت نفوذ سیاسی قابل توجهی هستند.
- **مجازات‌ها:** یک نردبان تحریم فزاینده: جریمه‌های سنگین، ممنوعیت درآمد تبلیغاتی و در نهایت، کاهش پهنای باند تا ۹۰ درصد.
- **سازوکار اعتراض:** اعتراض به دادگاه‌های ترکیه ارجاع می‌شود که به دلیل عدم استقلال و تأیید سانسور دولتی مورد انتقاد قرار گرفته‌اند.

۳-۸- عربستان سعودی: مدل «ممنوعیت‌های مبهم»

- **قانون:** قانون مبارزه با جرائم سایبری (۲۰۰۷).
- **مفاد کلیدی:** «تولید، تهیه، انتقال یا ذخیره مطالبی که به نظم عمومی، ارزش‌های دینی، اخلاق عمومی یا حریم خصوصی لطمه می‌زند» را جرم‌انگاری می‌کند. این اصطلاحات مبهم و به طور گسترده تفسیر می‌شوند.
- **نظام نظارتی:** وزارت کشور، سازمان داده و هوش مصنوعی عربستان (SDAIA) و دادگاه کیفری تخصصی (SCC) که برای محاکمه مخالفان استفاده می‌شود.
- **مجازات‌ها:** احکام حبس شدید (تا ۴۵ سال در موارد مستند) و ممنوعیت سفر.
- **سازوکار اعتراض:** فرآیند اعتراض در نظام قضایی تا دیوان عالی کشور وجود دارد، اما نشان داده شده که به افزایش احکام

منجر شده و فاقد شفافیت و انصاف است.

۹-۳ - امارات متحده عربی: مدل «نظم عمومی»

- **قانون:** فرمان-قانون فدرال شماره ۳۴ سال ۲۰۲۱.
- **مفاد کلیدی:** انتشار اطلاعات گمراه‌کننده، به ویژه محتوایی که «با منافع عمومی در تضاد باشد، ناآرامی عمومی را تحریک کند یا نظم و سلامت عمومی را مختل سازد» را ممنوع می‌کند.
- **نظام نظارتی:** مرجع قضایی و سایر نهادهای دولتی.
- **مجازات‌ها:** حداقل یک سال حبس و جریمه از ۱۰۰,۰۰۰ درهم که در زمان بحران افزایش می‌یابد.
- **سازوکار اعتراض:** سیستم تحت شرایط خاص اجازه اعتراض می‌دهد، اما در چارچوب قضایی تحت کنترل دولت عمل می‌کند.

۱۰-۳ - کره جنوبی: مدل «دموکراتیک مناقشه‌برانگیز»

- **قانون:** اصلاحیه‌های پیشنهادی به قانون دآوری مطبوعات (متوقف شده).
- **مفاد کلیدی:** این پیشنهاد به دادگاه‌ها اجازه می‌داد تا برای «اخبار جعلی» عمدی که توسط رسانه‌ها منتشر می‌شود، خسارت تنبیهی تا پنج برابر خسارت تخمینی وضع کنند.
- **نظام نظارتی:** قوه قضائیه به عنوان داور عمل می‌کرد.
- **مجازات‌ها:** جریمه‌های مالی قابل توجه برای شرکت‌های رسانه‌ای.
- **وضعیت:** این لایحه پس از انتقادات گسترده از سوی رسانه‌ها، جامعه مدنی و نهادهای بین‌المللی که معتقد بودند آزادی مطبوعات را محدود می‌کند، به تعویق افتاد و عملاً کنار گذاشته شد. این مورد یک مطالعه موردی کلیدی از عقب‌نشینی دموکراتیک در برابر چنین قوانینی است.

۱۱-۳ - سایر کشورها

- **سنگاپور:** قانون حمایت در برابر دروغ و دستکاری آنلاین (POFMA)، مصوب ۲۰۱۹. این قانون به دلیل «دستور اصلاح»^۱ مشهور است که به هر وزیر دولتی اجازه می‌دهد دستور دهد یک اطلاعیه اصلاحی در کنار محتوایی که آن را نادرست می‌داند، قرار گیرد. این قانون به دلیل استفاده علیه مخالفان سیاسی و ایجاد فرهنگ خودسانسوری مورد انتقاد قرار گرفته است.
- **استرالیا:** قانون ایمنی آنلاین، مصوب ۲۰۲۱. این قانون بیشتر بر ایمنی (آزار و اذیت سایبری، سوءاستفاده) تمرکز دارد تا اطلاعات نادرست. یک کمیسر ایمنی الکترونیکی قدرتمند ایجاد می‌کند که می‌تواند دستور حذف صادر کرده و بر آیین‌نامه‌های صنعتی نظارت کند.

۴. سنتز تطبیقی: تنظیم‌گری دیجیتال در سطح جهان

این بخش، یافته‌های تحلیل تطبیقی را در قالب یک جدول جامع ارائه می‌دهد و سپس الگوهای کلیدی آن را تحلیل می‌کند.

۱-۴ - جدول تطبیقی جامع قوانین تنظیم‌گری محتوای آنلاین

جدول ۱ به ارائه یک نمای کلی و قابل مقایسه از چشم‌انداز پیچیده جهانی تنظیم‌گری محتوا می‌پردازد. این جدول لایحه ایران را با نمونه‌های بین‌المللی در محورهای کلیدی مقایسه می‌کند. این مقایسه مستقیم، تفاوت‌های فاحش در رویکردهای مربوط به رویه‌های قانونی، تناسب و مبانی اقتصادی را آشکار می‌سازد.

جدول ۱ - مقایسه لایحه پیشنهادی ایران با سایر کشورها

عنوان	ایران (لایحه پیشنهادی)	اتحادیه اروپا	آلمان	فرانسه	بریتانیا	آمریکا	چین	ترکیه	عربستان سعودی	امارات متحده عربی	کره جنوبی (پیشنهاد متوقف شده)	سنگاپور
عنوان قانون	لایحه مقابله با انتشار محتوای خلاف واقع در فضای مجازی	قانون خدمات دیجیتال (DSA) (DSGA)	قانون اجرای شبکه (NetzDG)	قانون مبارزه با دستکاری اطلاعات	قانون ایمنی آنلاین (OSA)	بخش ۲۳۰ قانون حمایت ارتباطات	قانون امنیت سایبری و مقررات مرتبط	قانون شماره ۵۴۵۱ و قانون ضد اطلاعات نادرست	قانون مبارزه با جرائم سایبری	فرمان-قانون فدرال شماره ۲۴ سال ۲۰۲۱	اصلاحیه پیشنهادی قانون دآوری مطبوعات (POFMA)	قانون حمایت در برابر دروغ و دستکاری آنلاین (POFMA)
سال تصویب	در دست بررسی	۲۰۲۲ (لایحه اجرا) (۲۰۲۴)	۲۰۱۷ (اصلاحی) (۲۰۲۲)	۲۰۱۸	۲۰۲۳	۱۹۹۶	۲۰۱۷	۲۰۰۷ (اصلاحی) ۲۰۲۰ و ۲۰۲۲	۲۰۰۷	۲۰۲۱	(متوقف شده)	۲۰۱۹
نکات مهم قانون	تعاریف بسیار گسترده از «محتوای خلاف واقع»؛ تکالیف سنگین نظارت برگ (VLOP) و راستی‌آزمایی پیشگیرانه برای سکوها. جرم‌انگاری انتشار محتوا؛ دامنه مشمول فرامرزی	رویکرد لایم‌بندی شده بر مبنی بر ریسک، تکالیف سنگین‌تر برای سکوهایی بسیار بزرگ (VLOP) تمرکز بر شفافیت فرآیندها، حقوق کاربر و مدیریت ریسک‌های سیستمی	الزام سکوها به حذف محتوای «آشکارا غیرقانونی» ظرف ۲۴ ساعت، برون‌سپاری اجرای قوانین کف‌ی موجود به سکوهایی خصوصی	تمرکز بر دوره نظارت، ایجاد رويه قضایی سریع برای حذف اخبار جعلی تأثیرگذار بر انتخابات. الزام به شفافیت در تبلیغات سیاسی	ایجاد «وظیفه مراقبت» برای سکوها جهت محافظت از کاربران (به‌ویژه کودکان) در برابر محتوای مضر. الزام بر تمام محتوای آنلاین پیشگیرانه	اعطای مصونیت گسترده به سکوها در برابر مسئولیت ناشی از محتوای شخص ثالث. حفاظت از تضمینات تعدیل محتوا	مسئولیت مطلق سکوها برای نظارت و حذف پیشگیرانه محتوای مسموم، کنترل شدید دولتی بر تمام محتوای آنلاین	الزام به تعیین نماینده محل، دستورات حذف سریع (۴۸ ساعت)، جرم‌انگاری «اطلاعات نادرست»، تهدید به کاهش پهنای پند	جرم‌انگاری انتشار محتوایی که به «نظم عمومی» ارزش‌های دینی و اخلاقی عمومی، لطمه بزند. تعاریف بسیار مبهم	جرم‌انگاری انتشار شایعات و اخبار جعلی که «نظم سلامت عمومی» را مختل کند. تشدید مجازات در زمان بحران	پیشنهاد وضع خسارت تنبیهی تا ۵ برابر برای صدور «دستور اصلاح» با حذف محتوایی که جعلی منتشر کنند. هدف‌گیری رسانه‌های سنتی	اعطای اختیار به هر وزیر کابینه و دفتر POFMA در IMDA (اجرایی و دولتی)
سیستم نظارت	قوه قضائیه (دولت‌محور و قضایی-امنیتی)	اداره فدرال دادگستری (برای جرم‌های سیستمی)، عمدتاً خودتنظیم‌گری اجباری توسط سکوها	دادگستری (برای جرم‌های سیستمی)، عمدتاً خودتنظیم‌گری اجباری توسط سکوها	قوه قضائیه (برای دستورات حذف) و تنظیم‌گر (رسانه Arcom) (قضایی و نهاد مستقل)	اقلام (Ofcom) به عنوان یک تنظیم‌گر مستقل و قدرتمند	دادگاه‌ها (که معمولیت را تأیید می‌کنند) (بدون تنظیم‌گر)	اداره فضای سایبری چین (CAC) و وزارت امنیت عمومی (کنترل کامل دولتی)	اداره فناوری اطلاعات و ارتباطات (BTR) و قوه قضائیه، (تحت نفوذ دولت)	وزارت کشور و دادگاه کیفری تخصصی (امنیتی و قضایی)	اداره قضایی ایویتی و نهادهای دولتی، (قضایی و دولتی)	قوه قضائیه (قضایی)	هر وزیر کابینه و دفتر POFMA در IMDA (اجرایی و دولتی)
مجازات برای افراد	حبس تا ۵ سال، جرزی نقدی، محرومیت از فعالیت آنلاین، تعلیق، محدودیت، جذب کاربر، ممنوعیت تبلیغات، مسئولیت کیفری مدیران.	به طور مستقیم خبر، اما قوانین ملی ممکن است اعمال شود.	مشمول قوانین کیفری عمومی آلمان	حبس و جریمه برای عدم رعایت شفافیت	جرائم جدیدی مانند ارسال اطلاعات نادرست یا قصد آسیب‌رسانی	مسئولیت در برابر تولیدکننده محتوا (نه سکوها)	حبس و سایر مجازات‌های کیفری	حبس تا ۳ سال برای انتشار «اطلاعات گمراه‌کننده»	حبس‌های بسیار طولانی (تا ۴۵ سال) و ممنوعیت سفر	حداقل ۱ سال حبس و جریمه سنگین	به طور مستقیم خبر، هدف رسانه‌ها بودند	جریمه و/یا حبس برای عدم رعایت دستورات
مجازات برای سکوها	تعلیق، محدودیت، جذب کاربر، ممنوعیت تبلیغات، مسئولیت کیفری مدیران.	جریمه تا ۵۰ میلیون یورو برای عدم انطباق سیستمی.	جریمه تا ۵۰ میلیون یورو برای عدم انطباق سیستمی.	به طور مستقیم خبر، مگر در موارد عدم همکاری.	جریمه تا ۱٪ از درآمد جهانی یا ۱۸ میلیون یورو، مسئولیت کیفری مدیران.	مصونیت کامل (به جز موارد استثنا).	جریمه، تعلیق یا لغو مجوز فعالیت.	جریمه سنگین، ممنوعیت تبلیغات، کاهش پهنای پند تا ۹۰٪.	مسئودسازی وبسایت.	مسئولیت در صورت عدم همکاری.	خسارت تنبیهی سنگین.	جریمه برای عدم همکاری.





عنوان	ایران (لایحه پیشنهادی)	اتحادیه اروپا	آلمان	فرانسه	بریتانیا	آمریکا	چین	ترکیه	عربستان سعودی	امارات متحده عربی	کره جنوبی (پیشنهاد متوقف شده)	سنگاپور	
نقاط قوت و قوت قانون	قوت: (از دید حاکمیت) کنترل بالا بر فضای اطلاعاتی، ضعف: ابهام آزادی، نقض آزادی بیان، فقدان رویه عادلانه، آسیب به اقتصاد دیجیتال.	قوت: حفاظت از حقوق کاربر، شفافیت، رویکرد متناسب، ایجاد ضعف: پیچیدگی، هزینه‌های انطباق بالا برای VLOPs.	قوت: اجرای قوانین موجود، فشار بر سکوها برای مسئولیت‌پذیری، ضعف: ریسک حذف بیش از حد (over-block-ing)، فقدان سازوکار اعتراض قضایی، تبدیل سکوها به قاضی.	قوت: تمرکز محدود و هدفمند (انتخابات)، سرعت عمل، نقض محوری شفافیت، ضعف: ریسک عدم پاسخگویی، عدم پیچیدگی، هزینه‌های بالا.	قوت: (از دید حاکمیت) کنترل مطابق و مؤثر بر سکوها خارج، ضعف: استفاده از آزادی بیان، فقدان حاکمیت قانون، انزوای دیجیتال.	قوت: نوآوری و رشد اینترنت، حفاظت قوی از آزادی بیان، ضعف: سکوب کامل آزادی بیان، فقدان حاکمیت قانون، انزوای دیجیتال.	قوت: (از دید حاکمیت) ابزار قدرتمند برای سکوب هر نوع ترافیک، ضعف: انتقاد شدت سکوبگر، مجازات‌های نامتناسب، فقدان کامل رویه عادلانه.	قوت: (از دید حاکمیت) ابزار قدرتمند برای سکوب هر نوع ترافیک، ضعف: انتقاد شدت سکوبگر، مجازات‌های نامتناسب، فقدان کامل رویه عادلانه.	قوت: تلاش برای پاسخگو کردن رسانه‌ها، ضعف: به دلیل نگرانی از تحدید آزادی مطوعات و مخالفت گسترده، متوقف شد.	قوت: سرعت عمل دولت در مقابله با اطلاعات نادرست، ابزار اصلاح به جای حذف، ضعف: قدرت نامحدود وزیر، استفاده علیه مخالفان، اثر سکوبنده.	قوت: (پیشنهاد متوقف شده)	سنگاپور	
مقایسه با قانون ایران	لایحه ایران ترکیبی از ویژگی‌های مدل‌های تمرکزگراست: تعاریف مبهم مجازات‌های سکوبگر، مستقل، به نهاد سیاسی-امنیتی تکیه دارد و به جای حقوق کاربر، بر کنترل دولتی تأکید می‌کند.	مدل ایران در تضاد کامل با DSA است، به جای تأیید بر محتوا تمرکز دارد؛ به جای تنظیم‌گر مستقل، به نهاد سیاسی-امنیتی تکیه دارد و به جای حقوق کاربر، بر کنترل دولتی تأکید می‌کند.	Net2DG حداقل بر قوانین کفیری موجود و مشخص تکیه دارد. لایحه ایران با خلق مفاهیم جدید و مبهم مانند «انعکاس ناقص واقعیت»، بسیار گسترده‌تر و خودسرانه‌تر است.	مدل بریتانیا بر یک تنظیم‌گر مستقل (اقدام) و «وظیفه مراقبت» مشتمل است. مدل ایران فاقد تنظیم‌گر مستقل است و «وظیفه اطاعت» از دولت را تحمیل می‌کند.	شباهت زیادی در رویکرد کنترل دولتی و مسئولیت مطابق سکوها وجود دارد. هرچند لایحه ایران با جرم‌انگاری محدود حتی مدل ایران حتی سخت‌گیرانه‌تر به نظر می‌رسد.	شباهت زیادی در رویکرد کنترل دولتی و مسئولیت مطابق سکوها وجود دارد. هرچند لایحه ایران با جرم‌انگاری محدود حتی مدل ایران حتی سخت‌گیرانه‌تر به نظر می‌رسد.	هر دو بر «نظم عمومی» تأکید دارند، اما لایحه ایران با ایجاد یک سامانه موقوف شد. لایحه ایران بدون توجه به این نگرانی‌ها در حال پیشروی است.	هر دو بر «نظم عمومی» تأکید دارند، اما لایحه ایران با ایجاد یک سامانه موقوف شد. لایحه ایران بدون توجه به این نگرانی‌ها در حال پیشروی است.	مدل کره جنوبی به دلیل نگرانی‌های دموکراتیک متوقف شد. لایحه ایران بر حذف و مجازات کفیری (حبس) متمرکز است.	مدل کره جنوبی به دلیل نگرانی‌های دموکراتیک متوقف شد. لایحه ایران بر حذف و مجازات کفیری (حبس) متمرکز است.	مدل کره جنوبی به دلیل نگرانی‌های دموکراتیک متوقف شد. لایحه ایران بر حذف و مجازات کفیری (حبس) متمرکز است.	مدل کره جنوبی به دلیل نگرانی‌های دموکراتیک متوقف شد. لایحه ایران بر حذف و مجازات کفیری (حبس) متمرکز است.	سنگاپور
مفنی: افزایش هزینه‌های انطباق برای سکوها، اما ایجاد بزرگ، زمین‌بازی برابر و افزایش اعتماد کاربر که می‌تواند در بلندمدت مثبت باشد.	مختلط: افزایش هزینه‌های انطباق برای سکوها، بزرگ، زمین‌بازی برابر و افزایش اعتماد کاربر که می‌تواند در بلندمدت مثبت باشد.	مفنی: هزینه‌های انطباق بسیار بالا، مثبت (بلندمدت): دولت اعا می‌کند با جلوگیری از 71.۳٪ از آسیب‌های آنلاین، هزینه‌ها جبران می‌شود.	مفنی: خروج برخی شرکت‌ها، کاهش سرمایه‌گذاری، ایجاد فضایی عدم اطمینان برای کسب‌وکارهای دیجیتال.	مفنی: (از دید حاکمیت) ابزار قدرتمند برای سکوب هر نوع ترافیک، ضعف: انتقاد شدت سکوبگر، مجازات‌های نامتناسب، فقدان کامل رویه عادلانه.	مفنی: (از دید حاکمیت) ابزار قدرتمند برای سکوب هر نوع ترافیک، ضعف: انتقاد شدت سکوبگر، مجازات‌های نامتناسب، فقدان کامل رویه عادلانه.	مفنی: (از دید حاکمیت) ابزار قدرتمند برای سکوب هر نوع ترافیک، ضعف: انتقاد شدت سکوبگر، مجازات‌های نامتناسب، فقدان کامل رویه عادلانه.	مفنی: (از دید حاکمیت) ابزار قدرتمند برای سکوب هر نوع ترافیک، ضعف: انتقاد شدت سکوبگر، مجازات‌های نامتناسب، فقدان کامل رویه عادلانه.	مفنی: (از دید حاکمیت) ابزار قدرتمند برای سکوب هر نوع ترافیک، ضعف: انتقاد شدت سکوبگر، مجازات‌های نامتناسب، فقدان کامل رویه عادلانه.	مفنی: ایجاد ریسک برای کسب‌وکارهای محتوا محور و رسانه‌های اجتماعی.	مفنی: نگرانی از آسیب به صنعت رسانه یکی از دلایل توقف آن بود.	مفنی: ایجاد خودسانسوری و کاهش تمایل به مشارکت در گفت‌وگوهای عمومی که می‌تواند بر پویایی پلتفرم‌ها تأثیر بگذارد.	سنگاپور	

عنوان	ایران (لایحه پیشنهادی)	اتحادیه اروپا	آلمان	فرانسه	بریتانیا	آمریکا	چین	ترکیه	عربستان سعودی	امارات متحده عربی	گروه جنوبی (پیشنهاد متوقف شده)	سنگاپور
راهکار اعتراض به معمولات قانون	در لایحه به صراحت پیش‌بینی نشده است. تنها راه، توسل به رویه‌های عمومی قضایی است که به نتیجه رسیدن آن در زمان کوتاه مورد تردید است.	سیستم اعتراض داخلی سنگو، نهادهای مستقل حل اختلاف خارج از دادگاه (ODS) و در نهایت دادگاه‌های اروپایی.	توسل به دادگاه‌های عمومی مدنی آلمان، خود قانون سازوکار مستقلی ندارد.	فرآیند قضایی سریع با حق استیناف فوری در دادگاه تجدیدنظر.	سیستم‌های رسیدگی به شکایات داخلی سکوها که توسط آکادم نظامی می‌شود.	شکایت از تولیدکننده محتوا در دادگاه. راهی برای اعتراض به تصمیم سکو وجود ندارد.	اعتراض به نهادهای اداری و قضایی دولتی که فاقد استقلال هستند.	اعتراض به دادگاه‌های ترکیه که استقلال آنها مورد انتقاد شدید است.	فرآیند اعتراض در نظام قضایی وجود دارد اما در عمل به تشدید احکام منجر شده و باعادلانه است.	اعتراض در چارچوب نظام قضایی کشور.	(نامشخص)	ابتدا درخواست تجدیدنظر از وزیر صادرکننده دستور و سپس مراجعه به دادگاه عالی.

۲-۴- مقایسه کلی مدل‌ها: طیفی از تنظیم و کنترل

تحلیل جدول فوق نشان می‌دهد که قوانین تنظیم‌گری محتوا در جهان بر روی یک طیف قرار می‌گیرند:

- مدل مصونیت (آمریکا): در یک سوی طیف، آمریکا با بخش ۲۳۰ قرار دارد که با اعطای مصونیت به سکوها، نوآوری و آزادی بیان را در اولویت قرار می‌دهد و بار مسئولیت را بر دوش تولیدکننده محتوا می‌گذارد.
- مدل هم‌تنظیم‌گری (اتحادیه اروپا و بریتانیا): این مدل یک «راه سوم» است که تلاش می‌کند بین ایمنی و حقوق، تعادل برقرار کند. این مدل از یک تنظیم‌گر مستقل برای نظارت بر فرآیندهای سکوها استفاده می‌کند و بر مدیریت ریسک و شفافیت تمرکز دارد، نه تصمیم‌گیری در مورد محتوای فردی.
- مدل قضایی (فرانسه): این مدل مداخله دولت را به شرایط خاص (مانند انتخابات) محدود کرده و آن را از طریق قوه قضائیه مستقل مدیریت می‌کند.
- مدل کنترل دولتی (چین، ترکیه، عربستان، امارات و ایران): در سوی دیگر طیف، این مدل قدرت را در قوه مجریه و نهادهای امنیتی متمرکز می‌کند، از قوانین مبهم بهره می‌برد، مجازات‌های کیفری شدید اعمال می‌کند و فاقد نظارت مستقل یا سازوکار اعتراض معنادار است. هدف اصلی در این مدل، کنترل فضای اطلاعاتی است. لایحه ایران به وضوح، در این دسته قرار می‌گیرد.

۵. توصیه‌های راهبردی و تحلیل نهایی

بر اساس تحلیل‌های حقوقی، اقتصادی و تطبیقی فوق، توصیه‌های زیر برای اصلاح لایحه و کاهش اثرات مخرب آن ارائه می‌شود.

۱-۵- راهکارهای کاهش اثرات منفی اقتصادی

- **توصیه ۱: محدود و دقیق کردن تعاریف.** ماده ۱ لایحه به طور کامل بازنویسی شود. اصطلاحات مبهمی مانند «انعکاس ناقص واقعیت» و «عرفاً موجب تشویش اذهان» با تعاریف دقیق، عینی و با آستانه بالا برای اطلاعات نادرست مضر جایگزین شوند، مشابه استاندارد «آشکارا غیرقانونی» در آلمان یا معیارهای مشخص قانون فرانسه.
- **توصیه ۲: ایجاد «بندرگاه امن» برای استارت‌آپ‌ها.** کسب‌وکارهای کوچک و متوسط (SMEs) و استارت‌آپ‌های نوپا برای یک دوره گذار از سنگین‌ترین تکالیف نظارتی و گزارش‌دهی معاف شوند، مشابه رویکردی که در قانون خدمات دیجیتال اتحادیه اروپا اتخاذ شده است. این کار به آنها اجازه رشد و رقابت می‌دهد.
- **توصیه ۳: جرم‌زدایی.** مجازات حبس برای کاربران و مدیران سکوها (مواد ۱۲، ۱۳ و ۱۵) به کلی حذف شود. این مجازات‌ها با یک سیستم جرائم مدنی متناسب برای سکوهایی که به طور سیستمی در انجام وظایف خود کوتاهی می‌کنند، جایگزین شود؛ رویکردی که به مدل‌های آلمان و بریتانیا نزدیک‌تر است. این مهم‌ترین گام برای جلوگیری از اثر دلسردکننده بر اقتصاد محتوا و مشارکت کاربران است.

۲-۵- تقویت رویه‌های عادلانه و حاکمیت قانون

- **توصیه ۴: تأسیس یک نهاد تنظیم‌گر مستقل.** به جای وزارت ارشاد و «کارگروه»، یک مرجع ارتباطات مستقل یا شبه‌مستقل، با الگوبرداری از آفکام بریتانیا یا هماهنگ‌کنندگان خدمات دیجیتال اتحادیه اروپا، برای نظارت بر این چارچوب ایجاد شود. این نهاد به صورت شفاف عمل کرده و در برابر قوه مقننه پاسخگو باشد، نه قوه مجریه.
- **توصیه ۵: ایجاد یک فرآیند اعتراض شفاف و در دسترس.** لایحه فعلی در مورد سازوکار اعتراض سکوت کرده است. یک مکانیزم اعتراض چندلایه و قوی ایجاد شود که هم برای کاربرانی که محتوایشان حذف شده و هم برای افرادی که هدف محتوا قرار گرفته‌اند، در دسترس باشد. این فرآیند شامل اعتراض داخل سکو، گزینه‌ای برای حل اختلاف خارج از دادگاه (مانند ODS در قانون DSA اروپا) و یک اعتراض نهایی در یک نهاد قضایی مستقل و تخصصی باشد. فقدان این سازوکار،

یکی از نقص‌های حیاتی در سیستم‌های آلمان و ترکیه است.

هم‌چنین لازم به ذکر است هم اکنون دستگاه قضایی با معضل جدی «حجم بالای پرونده‌های ورودی» دست و پنجه نرم می‌کند که منجر به فرسایش قضات و سایر پرسنل غیرقضایی شده است. این لایحه با تشدید این معضل، این فرآیند استهلاک و فرسایش را تشدید خواهد کرد. این موضوع دغدغه بسیاری از قضاتی است که در صورت تصویب لایحه مذکور باید به این پرونده‌ها رسیدگی کنند. در صورتی که بخواهیم قضات بیشتری نیز استخدام کنیم تصویب این لایحه منجر به ایجاد یک هزینه اجتماعی جدید و معنادار خواهد شد که در جای خود قابل تأمل است.

در نهایت، مفاد این لایحه در بخش تعیین مجازات برخلاف روح سیاست‌های کلی قوه قضائیه در کاهش مجازات حبس تعزیری یا اعمال مجازات‌های جایگزین حبس در سالیان اخیر بوده است.

۵-۳- ملاحظات نهایی

این گزارش نشان می‌دهد که «لایحه مقابله با انتشار محتوای خلاف واقع در فضای مجازی» در شکل کنونی خود، کنترل دولتی را بر تمام ملاحظات دیگر، از جمله پویایی اقتصادی و حقوق بنیادین، ارجحیت می‌دهد. هرچند مقابله با پدیده اطلاعات نادرست یک چالش جهانی و هدفی مشروع است، اما راه‌حل پیشنهادی در این لایحه به دلیل عدم تناسب، ابهام در قوانین و فقدان سازوکارهای حمایتی از رویه‌های عادلانه، احتمالاً آسیب بیشتری به جامعه و اقتصاد دیجیتال ایران وارد خواهد کرد تا رفع مشکلی که ادعای حل آن را دارد. یک اقتصاد دیجیتال شکوفا نمی‌تواند بر پایه‌های عدم قطعیت حقوقی و هراس بنا شود؛ چنین اقتصادی نیازمند پیش‌بینی‌پذیری، حاکمیت قانون و احترام بنیادین به آزادی بیانی است که سوخت اصلی نوآوری دیجیتال محسوب می‌شود.

۶. فهرست منابع

- متن لایحه مقابله با انتشار محتوای خبری خلاف واقع در فضای مجازی، ۱ مرداد ۱۴۰۴

<https://dotic.ir/news/18798/%D9%84%D8%A7%DB%8C%D8%AD%D9%87-%D9%85%D9%82%D8%A7%D8%A8%D9%84%D9%87-%D8%A8%D8%A7-%D8%A7%D9%86%D8%AA%D8%B4%D8%A7%D8%B1-%D9%85%D8%AD%D8%AA%D9%88%D8%A7%DB%8C-%D8%AE%D8%A8%D8%B1%D-B%8C-%D8%AE%D9%84%D8%A7%D9%81-%D9%88%D8%A7%D9%82%D8%B9-%D8%AF%D8%B1-%D9%81%D8%B6%D8%A7%DB%8C-%D9%85%D8%AC%D8%A7%D8%B2%DB%8C>

- Amnesty International. (2022, October). Turkey: 'Disinformation' law a new, dark chapter for online censorship. EUR4461432022ENGLISH.
- Annenberg Public Policy Center. (2019, April). The German Network Enforcement Act (NetzDG): A Transatlantic Working Group Report.
- Appeals Centre Europe. (n.d.). Rules of Procedure. Retrieved July 26, 2025, from <https://www.appealscentre.eu/rules-of-procedure/>
- Australian Government, eSafety Commissioner. (2024, March 18). Learn about the Online Safety Act. Retrieved from <https://www.esafety.gov.au/newsroom/whats-on/online-safety-act>
- Business & Human Rights Resource Centre. (2021, October 6). Human rights experts warn that EU's Digital Services Act could repeat regulatory mistakes & negatively impact fundamental rights.
- CCIA Research Center. (2025, March). EU Digital Regulation Factsheet.
- CCIA Research Center. (n.d.). Costs to U.S. Companies from EU Digital Regulation. Retrieved July 26, 2025, from <https://ccianet.org/research/stats/costs-to-us-companies-from-eu-digital-regulation/>
- Centre for European Policy Studies (CEPS). (n.d.). The impact of the German NetzDG law. Retrieved July 26,



2025, from <https://www.ceps.eu/ceps-projects/the-impact-of-the-german-netzdg-law/>

- Centre for European Policy Studies (CEPS). (2018) Germany's NetzDG: A key test for combatting online hate.
- CIVICUS Monitor. (2023, September 22). Singapore: Anti-fake news POFMA law used to block news outlet, target critics as another law to regulate online content is passed.
- Coda Story. (2022, September 20). How Saudi Arabia's cybercrime laws are being used to stifle dissent.
- Columbia Global Freedom of Expression. (2023, November 29). The Case of Salma bint Sami bin Abdulmo-hsen al-Shehab and Nourah bint Saeed al-Qahtani (Saudi Arabia).
- Computer & Communications Industry Association (CCIA). (2023, April 19). Greater Internet Regs Hurt Investment, Innovation, and Free Speech. Project DisCo.
- Cour de cassation. (2025, March 12). Clarification on price manipulation in financial markets and directors' liability.
- Craufurd Smith, R. (2019) Fake News, French Law and the Fight for the Truth. Journal of Media Law.
- CSIS. (2025, February 20). The EU's Perspective on Digital Regulations with the Lead Negotiator on the Digital Services Act.
- Democratic Erosion Consortium. (2022, May 27). Singapore's 'Fake News' Law: For or Against Democracy ?
- DGSI, Ministère de l'Intérieur. (2024, November 26). La lutte contre la manipulation de l'information.
- Discord Support. (n.d.). What's Changing for UK Users Due to the UK Online Safety Act. Retrieved July 26, 2025, from <https://support.discord.com/hc/en-us/articles-33362401287959/What-s-Changing-for-UK-Users-Due-to-the-UK-Online-Safety-Act>
- East Asia Forum. (2023, October 24). Singapore's 'fake news' fixer risks undermining public confidence.
- Electronic Frontier Foundation (EFF). (2021, November 16). UN Human Rights Committee Criticizes Germa-ny's NetzDG for Letting Social Media Companies Censor Speech.
- Electronic Frontier Foundation (EFF). (2023, September 19). The UK Online Safety Bill is a Massive Threat to Online Privacy, Security, and Speech.
- Electronic Frontier Foundation (EFF). (2023, September 20). UK Online Safety Bill Will Mandate Dangerous Age Verification for Much of the Web.
- Electronic Frontier Foundation (EFF). (2025, July 15). We Support Wikimedia Foundation's Challenge to UK's Online Safety Act.
- Entekhab.ir. (2025, July 19). Details of the government's bill on combating false content.
- EU DisinfoLab. (n.d.). France. Retrieved July 26, 2025, from <https://www.disinfo.eu/resources/france/>
- European Commission. (n.d.). The Digital Services Act. Retrieved July 26, 2025, from https://commission.europa.eu/strategy-and-policy/priorities/2019-2024-europe-fit-digital-age/digital-services-act_en
- European Commission. (2022, December 15). Questions and Answers: Digital Services Act.
- European Commission. (2025, March 31). Annual report on costs incurred for the fulfilment of the Commis-sion's tasks under the Digital Services Act (DSA) for 2024.
- European External Action Service (EEAS). (n.d.). Information Integrity and Countering Foreign Information Manipulation & Interference (FIMI). Retrieved July 26, 2025, from https://www.eeas.europa.eu/eeas/infor-mation-integrity-and-countering-foreign-information-manipulation-interference-fimi_en
- Fararu. (2025, July 19). Penalties for users who publish false content in cyberspace.
- Freedom House. (2021) Freedom on the Net 2021: Turkey.
- Freedom House. (2024) Freedom on the Net 2024: Turkey.

- Government of the United Kingdom. (2023, October 26). Online Safety Act 2023.
- Government of the United Kingdom. (2024, October 23). Online Safety Act: Enactment impact assessment.
- Government of the United Kingdom. (2025, April 24). Online Safety Act: Explainer.
- Government of the United Kingdom, Department for Science, Innovation and Technology. (2024, October 23). Potential impact of the Online Safety Bill.
- Government of the United Kingdom, Department for Science, Innovation and Technology. (2025) Impact Assessment: Data Use and Access Bill.
- Heinrich Böll Stiftung. (2025, February 18). Trump vs. Europe: The Role of the Digital Services Act.
- Hogan Lovells. (2025, February 10). When AI and Copyright clash: Chinese courts find AI platform liable for contributory copyright infringement based on AI generated images.
- House of Commons Library. (2025, February 14). The Online Safety Act 2023.
- Human Rights Watch. (2018, February 14). Germany: Flawed Social Media Law.
- Human Rights Watch. (2021, January 13). Singapore: 'Fake News' Law Curtails Speech.
- Human Rights Watch. (2021, November 10). How the EU's Flawed Artificial Intelligence Regulation Endangers the Social Safety Net.
- Human Rights Watch. (2022, January 7). EU: Put Fundamental Rights at Top of Digital Regulation.
- Human Rights Watch. (2022, October 14). Turkey: Dangerous, Dystopian New Legal Amendments.
- Internet Society. (2025, January 20). UK Online Safety Act – 2025 and beyond.
- JDSupra. (2023, October 11). China Proposes Amendments to the Cybersecurity Law.
- Légifrance. (2018, December 22). LOI n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information.
- Lee Kuan Yew School of Public Policy. (2019) Between Surveillance and Security: The POFMA Bill.
- Lexis Middle East. (2025, May 20). Abu Dhabi: Strict Penalties for Spreading Fake News.
- Latham & Watkins. (2023, November). UK Online Safety Act 2023: A Guide for In-Scope Service Providers.
- Park, A. & Youm, K. H. (2019) Fake News from a Legal Perspective: The United States and South Korea Compared. Southwestern Journal of International Law.
- Planet Compliance. (2024, September 19). Understanding the Implications of the Digital Services Act.
- Policy Review. (2018, December 10). Reading between the lines and the numbers: An analysis of the first NetzDG reports.
- Politico. (2025, July 11). France launches criminal investigation into X over algorithm manipulation.
- Protiviti. (2023) The Global Consequences of Europe's New Digital Regulatory Regime.
- Public Media Alliance. (2021, October 8). Update: South Korean lawmakers back down on controversial 'fake news' bill.
- Radio Farda. (2025, July 24). Government's defense of the controversial 'false content' bill.
- Rouse. (2021, October 28). Overview of administrative copyright enforcement in China.
- RSIS. (2022, August 1). POFMA: Why and How.
- RSIS. (2024, October 4). How Effective is POFMA in Battling Online Falsehoods ?
- S. Rajaratnam School of International Studies (RSIS). (2022) Looking Beyond POFMA to Combat Fake News and Misinformation in Singapore. Harvard Kennedy School Student Review.
- Sampi. (2022, August 2). China Cybersecurity Law: A summary of the first comprehensive data protection law in China.
- Saudi Arabia Ministry of Justice. (n.d.). Freedom of Information. Retrieved July 26, 2025, from <https://www.>



moj.gov.sa/English/Ministry/Pages/Info-Rights.aspx

- Saudi Arabia, Bureau of Experts at the Council of Ministers. (2007) Anti-Cyber Crime Law.
- Saudi Arabia, My.gov.sa. (2025, June 2). Report Fake News.
- Singapore Statutes Online. (2019) Protection from Online Falsehoods and Manipulation Act 2019.
- SMU Institutional Knowledge. (2019) Understanding Singapore's POFMA in its legal context.
- The Brookings Institution. (2022, October 14). Turkey's new media law is bad news, but don't report it.
- The GWU International Law & Policy Brief. (2021, December 8). Online Content Regulation: An International Comparison.
- The Hani. (2023, September 12). Korean media regulator's "one strike" policy for "fake news" denounced as censorship.
- The Korea Times. (2021, August 22). Fake news' law revision draws concern from international journalists.
- Twitch Help. (n.d.). Digital Services Act. Retrieved July 26, 2025, from <https://help.twitch.tv/s/article/digital-services-act>
- Two Birds. (2019, March 20). ISP Liability: China's internet court said Wechat is not obliged to disconnect portal to a Mini-Program upon notification of copyright infringing content.
- UK Parliament. (2025) Data Use and Access Bill: Impact Assessment.
- UK Parliament, Public Accounts Committee. (2024, May 15). Online Safety Act: A report.
- UN Human Rights Council, Working Group on Arbitrary Detention. (2023) Opinion No. 27/2023 concerning Salma al-Shehab (Saudi Arabia).
- U.S. Congressional Research Service. (2024, January 4). Section 230: An Overview.
- U.S. Congressional Research Service. (2024, February 29). An Introduction to Section 230.
- Verfassungsblog. (2017, July 5). The German NetzDG: A Risk Worth Taking ?
- Vista.ir. (2025, July 19). The new government bill is a copy of the Cyberspace Protection Bill.
- VOA News. (2021, September 8). South Korea Fights 'Fake News,' But Critics Claim It's Gagging the Press.
- Wikipedia. (n.d.). Internet regulation in Turkey. Retrieved July 26, 2025, from https://en.wikipedia.org/wiki/Internet_regulation_in_Turkey
- Wikipedia. (n.d.). Loi contre la manipulation de l'information. Retrieved July 26, 2025, from https://fr.wikipedia.org/wiki/Loi_contre_la_manipulation_de_l'information
- Wikipedia. (n.d.). Online Safety Act 2023. Retrieved July 26, 2025, from https://en.wikipedia.org/wiki/Online_Safety_Act_2023
- Wikipedia. (n.d.). Protection from Online Falsehoods and Manipulation Act 2019. Retrieved July 26, 2025, from https://en.wikipedia.org/wiki/Protection_from_Online_Falsehoods_and_Manipulation_Act_2019
- Yale Law School, Media Freedom & Information Access Clinic. (2018) Germany's NetzDG and the Threat to Online Free Speech.
- Zhang, C. (2012) Internet Intermediary Liability for Illegal Content in China. International Journal of Law and Information Technology.