مجله حقوقی دادگستری

دوره ۹۰/ ویژه‌نامه نودمین سال انتشار/ آذر ۱۴۰۵/ صفحات: ۷۸-۳۹
تاریخ دریافت: ۱۴۰۴/۰۵/۱۶ تاریخ پذیرش: ۱۴۰۴/۰۷/۱۹

مطالعه تطبیقی تنظیم‌گری مشارکتی در برابر مخاطرات سکوهای رایانه‌ای محتوایی

محمد یکرنگی،[۱] سید محمود قرقچیان[۲]

چکیده

رشد شتابان سکوهای رایانه‌ای و تأثیر عمیق آن‌ها بر زندگی افراد و پاسخ‌گو نبودن قوانین سنتی به جهت پیچیدگی‌های این حوزه، ضرورت بازبینی در رویکردهای تنظیم‌گری را نمایان ساخته است. امروزه بسیاری از مراودات اشخاص از طریق سکوهای رایانه‌ای صورت می‌گیرد. در این میان سکوهای رایانه‌ای تولید محتوایی که با محوریت کاربران فعالیت می‌کنند، اهمیت به سزایی یافته است؛ زیرا کاربران قادر به ارائه هرگونه محتوایی در آن می‌باشند. لذا پرسشی که مطرح می‌شود در زمینه مسؤولیت سکو، اعم از مدنی، اداری و حتی کیفری در قبال این محتواها می‌باشد. آیا سکوها مسؤولیتی دارا می‌باشند یا خیر و آیا مسؤولیت وی ناظر به حذف و محدودیت دسترسی محتواهای مضر و مجرمانه است یا بیش از آن می‌باشد؟ پژوهش حاضر که به روش توصیفی تحلیلی و بر پایه مطالعات کتابخانه‌ای انجام شده است، با تطبیق سه نظام حقوقی ناظر به فضای مجازی یعنی هم‌تنظیمی، خودتنظیمی و تنظیم‌گری دولتی، به تحلیل گذار از مصونیت مطلق سکوها به پذیرش مسؤولیت محدود و مشارکت آن‌ها در فرایند تنظیم‌گری می‌پردازد. در این چارچوب، دو رهیافت کلیدی هم‌تنظیمی و خودتنظیمی، نقش سکوها را از پیروی صرف به بازیگری فعال در تدوین و اجرای دستورالعمل‌ها تغییر می‌دهد؛ با این حال، چالش‌هایی نظیر قضاوت سلیقه‌ای، حذف حداکثری محتوا و تعارض منافع، ضرورت تدوین اصول راهنمای شفاف و تشکیل کمیسیون‌های نظارتی مستقل را دوچندان می‌کند. یافته‌های تحقیق نشان می‌دهد که تنظیم‌گری مشارکتی، با ایجاد توازن میان نظارت مؤثر و صیانت از آزادی بیان، می‌تواند پاسخی مناسب به چالش‌های تنظیم‌گری در فضای دیجیتال ارائه دهد.

واژگان کلیدی: سکوهای رایانه‌ای محتوایی، تنظیم‌گری مشارکتی، هم‌تنظیمی، خودتنظیمی، نظارت دولتی، مسؤولیت مدنی، مسؤولیت کیفری

---

۱. عضو هیات علمی گروه حقوق جزا و جرم‌شناسی، دانشکده حقوق و علوم سیاسی، دانشگاه تهران، تهران، ایران Yekrangi@ut.ac.ir

۲. دکتری حقوق جزا و جرم‌شناسی، دانشکده حقوق و علوم سیاسی، دانشگاه تهران، تهران، ایران (نویسنده مسؤول) ghoroghchian73@ut.ac.ir

درآمد

در دهه‌های اخیر، سکوهای رایانه‌ای[1] به‌عنوان یکی از بازیگران کلیدی در فضای دیجیتال، ساختارهای اجتماعی، اقتصادی و حتی فرهنگی را دگرگون کرده‌اند. سکوها به کمک فناوری دیجیتال که موانع زمانی و مکانی را از بین برده و از نرم‌افزارهای هوشمند و پیشرفته بهره می‌گیرد، با حذف مسؤولان واسطه و با ایجاد ارتباط میان کاربران خود تعامل و تبادل اطلاعات، کالا و خدمات را تسهیل و امکان ارزش‌آفرینی را برای همه آن‌ها میسر می‌سازند(غلامی و همکاران، ۱۳۹۶: ۱٤). تعریف و چارچوب‌بندی دقیق مفهوم سکوها همواره موضوعی چالش‌برانگیز و پیچیده بوده است. دلیل این پیچیدگی نه تنها به تنوع و گستردگی انواع آن‌ها برمی‌شود، بلکه به این واقعیت مرتبط است که سکوها در حوزه‌های مختلف از جمله فناوری اطلاعات، اقتصاد، حقوق و جامعه‌شناسی، تعاریف و مصادیق متفاوتی دارند (عبدالهی نیسیانی و قاسمی، ۱٤۰۰: ۲٦۹).[2] اما در یک تعریف کلی می‌توان سکوها را بسترهای مبتنی بر فناوری اطلاعات دانست که با ایجاد زیرساخت‌های تعاملی و شبکه‌ای، امکان تبادل ارزش، اطلاعات، کالا، خدمات یا نوآوری را میان گروه‌های مختلف کاربران و ذی‌نفعان فراهم می‌کنند و با بهره‌گیری از اثرات شبکه‌ای و مقیاس‌پذیری بالا، فضایی پویا و چندجانبه برای خلق ارزش ایجاد می‌نمایند.

یکی از چالش‌هایی که حاکمیت‌ها با ظهور سکوها با آن مواجه گشته‌اند، تنظیم‌گری آن‌ها به دلیل برهم خوردن مؤلفه‌ها و پارادایم‌های سنتی و عدم امکان نظارت و کنترل همانند گذشته است. در واقع تنظیم‌گری که به مجموعه‌ای از مداخلات حاکمیتی[3] در عرصه‌های اقتصادی و اجتماعی اطلاق می‌شود که از طریق

---

1. Digital Platform

۲. در تعاریف کلاسیک، سکوها معمولاً به عنوان بسترهای فیزیکی یا تکنولوژیکی تعریف می‌شوند که بر اساس آن‌ها محصولات یا خدمات دیگر ساخته و ارائه می‌شوند. این تعریف عمدتاً به دنیای صنعتی و تولیدات فیزیکی مرتبط است. چنان‌که در صنعت، سکو به عنوان یک مجموعه استاندارد از اجزاء و زیرساخت‌ها در نظر گرفته می‌شود که محصولات یا سیستم‌های مختلف می‌توانند بر اساس آن‌ها توسعه یابند و به آن پلتفرم محصول نیز اطلاق می‌شود. به عنوان مثال، گروه فولکس‌واگن از سکوی ام.کیو.بی (MQB) برای تولید خودروهای مختلفی از برندهای آئودی، اشکودا و سئات استفاده می‌کند.

۳. اطلاق حاکمیتی بودن لزوماً به این معنا نیست که صرفاً توسط حکومت اجرا می‌شود، بلکه

به‌کارگیری ابزارهای حقوقی، اقتصادی، اجتماعی و سایر شیوه‌ها، با هدف تحقق سیاست‌ها و تأمین منافع عمومی اعمال می‌شود (امامیان و همکاران، ۱۳۹۷: ۹) به جهت مسائلی همچون کیفیت، امنیت و حفاظت از حریم خصوصی کاربران، جلوگیری از انحصارطلبی و تنظیم فضای رقابتی، مدیریت محتوای نامناسب، اطمینان از کیفیت خدمات، احقاق حقوق کارگران و تأمین شرایط متناسب و مناسب کاری و ایمن‌سازی آن و امثال این موارد، ضرورت خود را آشکار ساخته است. افزون بر موارد فوق، از مقررات بیرونی که توسعه سکوها به دنبال داشته است نیز نباید غافل گشت؛ به عنوان مثال، توسعه استفاده از تاکسی‌های اینترنتی در حوزه اقتصاد پلتفرمی و کاهش استفاده از وسایل حمل و نقل عمومی، مستلزم ارائه راهکارهایی جهت تنظیم این بازار است (Wyman, 2018: 12).

با این حال به دلیل تنوع سکوها، تدوین و اجرای یک سیاست واحد و فراگیر برای تمامی آن‌ها امری دشوار و در برخی موارد ممتنع به نظر می‌رسد. امروزه انواع مختلفی از سکوها در فضای دیجیتال فعالیت دارند. در یک دسته‌بندی کلی می‌توان آن‌ها را به دو گروه سکوهای محتوامحور و سکوهای کالا و خدمات تقسیم کرد. سکوهای محتوامحور بر مبنای محتوای منتشر شده در آن‌ها شکل گرفته‌اند و خود به دو نوع سکوهای کاربرمحور و ناشرمحور قابل تفکیک می‌باشند (حسنی، ۱۴۰۳: ۳۶). سکوهای کاربرمحور همان شبکه‌های اجتماعی هستند؛ مانند شبکه‌هایی که برای یادداشت‌نویسی طراحی شده‌اند (مانند ویکی‌پدیا)[1] یا بر اشتراک‌گذاری محتوا تمرکز دارند (مانند اینستاگرام[2] و روبیکا) یا سکوهایی که برای برقراری ارتباط میان کاربران به‌کار می‌روند (مانند تلگرام،[3] سیگنال، بله و ایتا). در مقابل، سکوهای کالا و خدمات آن دسته از سکوهایی هستند که به‌منظور ارائه یا تسهیل دسترسی به کالا و خدمات ایجاد شده‌اند؛ خواه صرفاً معرفی کالا در آن‌ها انجام شود (مانند دیوار) یا امکان خرید و فروش فراهم باشد (مانند آمازون و ایمالز)[4] و یا برای ارائه خدمات

می‌تواند از سوی نهادهای مستقل، تنظیم‌گران بخشی یا در مواردی حتی با مشارکت نهادهای مدنی نیز انجام شود.

1. Wikipedia
2. Instagram
3. Telegram
4. Emalls

طراحی شده باشند (مانند اسنپ و اوبر).[1]

با این وصف، آنچه در کانون توجه این تحقیق قرار دارد، سکوهای تولید محتوایی بوده و چالش اصلی در ارتباط با آن‌ها، تعیین حدود و ضوابط مواجهه با محتواهای نامناسب، مضر یا غیر قانونی و اختیارات سکوها در زمینه حذف یا محدودسازی دسترسی به این‌گونه محتواها در چارچوب سه نظام کنترلی خودتنظیمی، هم‌تنظیمی و تنظیم‌گری دولتی می‌باشد. به عبارت دیگر، شیوه برخورد با این چالش‌ها نیز موضوعی است که نظام‌های حقوقی مختلف به‌طور جدی با آن مواجه شده‌اند. تنظیم‌گری کاملاً دولتی در دنیای دیجیتال به جهت حجم و پیچیدگی بالای فعالیت در سکوها، فرامرزی بودن آن‌ها و و ماهیت جهانی فعالیت‌های دیجیتال، حجم گسترده داده‌ها، نقش کاربران به عنوان تولیدکنندگان محتوا و تغییرات سریع فناوری با چالش‌های متعددی مواجه است و در بسیاری از موارد، دولت‌ها نمی‌توانند به تنهایی بر تمامی جزئیات و مسائل این سکوها نظارت داشته باشند و در نهایت نیازمند همکاری و تعامل با خود سکوها هستند. در واقع معمولاً ناظران با قواعد نظارتی ورود می‌کنند تا امنیت و کیفیت را تضمین نمایند و لذا با اعمال قواعد نظارتی پسینی به دنبال اهداف مذکور هستند؛ اما در فضای سکوها که تعداد زیادی کاربر اعم از مشتری (به معنای عام) و ارائه‌دهنده کالا و خدمات فعالیت دارند، چنین نظارتی کارایی تام ندارد و لذا الزاماً در چنین فضایی باید به سراغ تنظیم‌گری‌های اشتراکی و همکارانه رفت (Cannon & Chung, 2018: 13).

حال دولت‌ها با درک اثرگذاری بالای سکوها و ضرورت اولویت‌گذاری چنین تنظیم‌گری باز حسب سیاست اتخاذی خود در خصوص مسؤولیت سکوها با چالش‌های مختلفی در خصوص نحوه اجرای محدودیت و اعمال آن مواجه خواهند بود. درواقع، سیاست‌های متفاوت دولت‌ها در تعیین میزان مسؤولیت یا مصونیت سکوها از مصونیت گسترده‌ای که در ایالات متحده برقرار است، تا مسؤولیت مشروط در اتحادیه اروپا و مسؤولیت مطلق در برخی کشورها مانند چین و رهیافت‌های مختلف اندیشیده در راستای تنظیم‌گری، دو بُعد اساسی و مکمل در اعمال آن به شمار می‌آیند. از همین رو، با توجه به پیشرو بودن اروپا و آمریکا

1. Uber

در تدوین قوانین خاص و برخورداری از منابع پژوهشـــی غنی، بررسی رویکردهای تنظیم‌گـــری در این نظام‌ها می‌تواند چارچوب‌های مفیدی بـــرای تحلیل و اقتباس، فراهم آورد.

پژوهش حاضر بر آن است تا با تمرکز بر سکوهای تولید محتوایی و با روش توصیفی تحلیلی و با هدف ارائه پیشنهادهایی برای طراحی الگوی حقوقی مناسب در نظام حقوقی ایران برای تنظیم‌گری مؤثر، مشارکتی و متوازن در قبال سکوهای فوق، ابتدا به بررسی مبانی مسؤولیت سکوها در نظام‌های حقوقی مختلف (بند ۱) پرداخته و ســـپس ضوابط هم‌تنظیمی به‌عنوان چارچوب اصلی تنظیم‌گری سکوها در اتحادیه اروپـــا و ایالات متحده (بند ۲) تحلیل و در نهایت خودتنظیمی به‌عنوان مکملی برای این ساختار (بند ۳) بررسی شود.

۱. بررسی تطبیقی مبانی مســـؤولیت سکوها؛ از مصونیت گسترده[1] تا مسؤولیت مطلق[2]

مسأله تعیین مسؤولیت یا مصـونیت سـکوها برای کنترل محـتوا و فعالیـت‌های کاربران، به یکی از چالش‌های حقوقـــی و سیاست‌گذاری مهم در سطح جـــهانی تبدیل شده است. بسیاری از دولت‌ها به دنبـــال اعمال سیـاست‌هـای تنظـیم‌گرانه برای حفاظت از حقوق عمومی و جلوگیـــری از نشر محتوای نامناسب هســـتند و از سوی دیگر، سکوهـــای رایانه‌ای به دلیل ماهیت نوآورانه و گسـترده فعالیت‌های خود، از پذیرش مسؤولـــیت‌های سنگین و مستقیم در قبال محـتواها و فعالیت‌های کاربران اجتناب می‌کنند. در واقع یکی از چالش‌های اصلی این اســـت که ســـکوها که صرفاً بسترساز هستند تا چه اندازه باید در قبال مـــحتوا و فعالیـت‌های کاربران خود نظارت کرده و مسؤول شـــناخته شوند. برای پاسخ به این پرسـش، کشورهای مختلف با توجه به اولویت‌ها و دیدگاه‌های حقوقی خود، نظام‌هـــای متفاوتی را در زمینه تعیین مسؤولیت یا مصونیت سکوها اتخاذ نموده‌اند که به تبیین آن خواهـــیم پرداخت.

1. Broad immunity
2. Strict liability

۱-۱. مصونیت گسترده

ایـــن رویکرد در آمریـــکا طبق بخش ۲۳۰ «قانون حســـن ارتباطات مصوب ۱۹۹٦»[1] پذیرفته شـــده است و ملایم‌ترین رژیم محســـوب می‌شود. مصونیت ایجاد شـــده در بخش ۲۳۰ را می‌توان در دو قســـمت تحلیل کرد: اولاً سکوها نمی‌توانند در برابر محتوای کاربران خود مســـؤول شناخته شوند؛ زیرا آن‌ها صرفاً دسترسی به اینترنت و ســـایر خدمات را به عنوان یک بسترســـاز فراهم می‌کنند و در واقع آن‌ها به معنای حقوقی، ناشـــر محتوای کاربران خود نیستند؛ و ثانیاً اگر سکوها تصمیم بر نظارت بر محتوای کاربران خود داشته باشد از حفاظت و مصونیت پیش‌گفته خارج نمی‌شوند. به هر حال منطق چنین مصونیتی بر این است که اگر سکو مسؤول شناخته شـــود، موجب می‌شـــود تا کاربران را به طور فعال نظارت کند و لذا این امر نه‌تنها عملاً غیرممکن است، بلکه از نظر مالی غیرقابل تحمل و از لحاظ سیاسی نامطلوب خواهد بود؛ علی‌الخصوص که به دلیل ترس از مســـؤولیت، نوآوری‌های برخط[2] نیز متوقف خواهد شـــد. البته مواردی که مربوط به نقض حق نشـــر[3] یا علامت تجاری[4] اســـت، مشمول قوانین خاصی مانند «قانون حق نشـــر هزاره دیجیتال ایالات متحده مصوب ۱۹۹۸»[5] یا «قانون لنهام ایالات متحده مصوب ۱۹٤٦»[6] هستند. این قوانین به عنوان استثنا، سکوها را ملزم به اقدامات فعال‌تر در شناسایی و مقابله با نقض حقوق مالکیت معنوی می‌کنند (MacKinnon et al, 2015: 42).

سیاســـت اتخاذ شده از سوی آمریکا هرچند در راســـتای حراست از اصول آزادی بیان و حفظ حریـــم خـصوصـــی افراد و رشد و توســـعه سـکوها مثـبت ارزیابی گشته اســـت، اما این سیاســت به خـــصوص در سال‌های اخیر و پس از کشمکش بین توییتر و ترامپ[7] محل انتقـــادات فراوان بوده اســت؛ چنان‌کـه برخـی

1. Communications Decency Act (1996)
2. Online
3. Copyright
4. Trademark
5. Digital Millennium Copyright Act (DMCA)(1998)
6. Lanham Act (1946)
۷. ترامپ در ۲٦ می ۲۰۲۰ اعلام کرد که رای‌گیری پســـتی در انتخابات پیش روی آمریکا منجر به تقلب می‌شـــود. توییتر در واکنش به این اقدام ترامپ یک برچســـب زیر توییت وی اضافه کرد که «حقایق مربوط به رأی‌گیری پســـتی را دریافت کنید». این برچسب کاربران را به خواندن مطالبی که

در نقد آن گفته‌اند که «قاعده حسن نیتی است که مستلزم عمل با حسن نیت نیست» (Sevanian, 2014: 125)؛ زیرا حتی برخی دادگاه‌ها در جایی که سکو از محتوای غیر قانونی و ناقض مطلع گشته، اما نسبت به حذف آن اقدام ننموده؛ چه به نحو عمدی چه با فرض تقصیر، با استناد به چنین مصونیتی وی را مسؤول ندانسته‌اند. البته باید توجه داشت که تحت همین بخش ۲۳۰ نیز در صورت احراز برخی شرایط می‌توان قائل به مسؤولیت گشت؛ چنان‌که بند ٤ آن بیان می‌دارد که «هیچ چیز در این ماده نباید به گونه‌ای تفسیر شود که اعمال قانون محرمانگی ارتباطات[1] مصوب ۱۹۸٦ یا اصلاح راجع به آن یا مقررات ایالتی مشابه را محدود کند». به هر حال، سکوها در صورتی که حسن نیت آن‌ها مخدوش شود یا محتوای غیرقانونی و عمل زیان‌بار به نحوی به آن‌ها منتسب شود؛ یعنی مرتکب تقصیری شوند که ضرر ناشی از محتوا قابل انتساب به آن‌ها شود یا عملکرد سکو از واسطه به ناشر یا تولیدکننده تغییر یابد، مسأله مسؤولیت آن‌ها، قابل بررسی است (Boyle & Jenkins, 2014: 519).

۲-۱. مسؤولیت مشروط[2]

اکثر کشورهای اروپایی و بسیاری از کشورهای آمریکا جنوبی و همچنین روسیه به این رویکرد متمایل می‌باشند. این رژیم پیشنهادی که شبیه قوانین ایالات

مدافع رأی‌گیری پستی بود هدایت می‌کرد. ترامپ این اقدام توییتر را خلاف آزادی بیان و دخالت در انتخابات خواند و توییتر در اقدامی دیگر توییت دیگری از ترامپ که در آن بیان شده بود «اراذل و اوباش در حال اهانت به یاد و خاطره جورج فلوید هستند و من نیروهای گارد امنیتی آمریکا را می‌فرستم تا در صورت شروع شدن غارت‌ها، تیراندازی آغاز شود»، پنهان کرد و به آن برچسب خشونت‌آمیز زد و در صورت درخواست کاربر، قابل مشاهده برای وی می‌نمود. اینجا بود که ترامپ از صدور یک فرمان اجرایی برای حذف یا تغییر بخش ۲۳۰ در راستای جلوگیری از اقدامات توییتر و سکوهای دیگر سخن به میان آورد. توییتر در دفاع از اقدام خود مدعی بود که در راستای رویکرد جدید خود و در جهت دفاع از اخلاق مدنی، توییت‌های خطرناک و به طور کلی محتواهای مخرب و گمراه‌کننده را حذف می‌کند؛ چنان‌که توییت‌های رؤسای جمهور برزیل و ونزوئلا در تبلیغ داروهای مشکوک در خصوص کرونا را حذف کرد. ترامپ در فرمان اجرایی خود اعلام نمود که سکوها قدرتی مهارنشدنی جهت حذف، محدود کردن، شکل دادن، پنهان کردن، ویرایش یا تغییر بخش بزرگی از ارتباطات دارند و او این را غیر قابل قبول می‌دانست و امیدوار بود با چنین فرمانی زمینه اعمال مقررات تازه و نظارت بیشتر بر عملکرد سکوها از جمله توییتر و فیس‌بوک فراهم شود.

1. Electronic Communications Privacy Act (1986)
2. Conditional liability

متحده در حوزه حق نشـــر است، معتقد است که ســـکوها در قبال آنچه کاربرانشان بارگذاری و منتشر می‌کنند، مسؤولیتی ندارند تا زمانی که علم واقعی به خلاف بودن محتوا نداشـــته باشند و محتوای غیرقانونی را ایجاد نکرده و یا آغازگر و شروع‌کننده آن نباشـــند و به درخواست‌ها برای حذف محتوای غیرقانونی شخص ثالث نیز پاسخ دهند (Gillespie, 2018: 6-7). این رویکرد در قوانین جدیدی همچون دستورالعمل تجارت الکترونیک اتحادیه اروپا مصوب ۲۰۰۰ [1] و قانون خدمات دیجیتال [2] اتحادیه اروپا مصوب ۲۰۲۲ (لازم‌الاجرا از ۲۰۲٤)، به‌طور واضح دیده می‌شـــود که بر اساس آن‌ها، ســـکوها ملزم به رعایت اصول مشخصی هســـتند؛ اما همچنان آزادی بیان و حقوق کاربران مورد توجه قرار دارد. این نوع مســـؤولیت توازن مناسبی میان امنیت کاربران و آزادی بیان ایجاد کرده و به ســـکوها اجـــازه می‌دهد تا محتوا را تا حدی کنترل کنند، بدون آن که به‌طور کامل مسؤول باشند.

۳-۱. مسؤولیت مطلق

در نظام‌هایی با نظارتی مطلق بر فضـــای مجازی، ســـکوها موظف هســـتند مســـؤولیت کامل محتوای منـــتشرشده توســـط کاربران را بپذیـــرند؛ حتی اگر از غیرقانونی بودن یا وجـــود آن محتوا بی‌اطـــلاع باشند. برای اجتناب از پیامدهای قانونی، سکوها باید به‌طور مداوم محـــتوا را بررسی، پالایش و در صورت احتمال نقض قوانین، حذف کننـــد؛ با این حـال حتی در صورت انجام این اقـدامات، اگر محتوای ناقض قوانیـــن از دید آن‌ها پنـــهان بماند، مسـؤولیت آن هـمچنان متوجه آن‌ها خواهد بود. به‌عـــنوان نـمونه، دولـــت چین تمامی سکوها را ملزم به نظارت دقـــیق بر فعالیت کاربران، حذف محتوای نامناسب و گـزارش تخلفات کرده و در صورت کوتاهـی، مجـازات‌هـایی نظیر جـریمه، پیگـرد قانونـی یا لغو مجـوز برای

1. E-Commerce Directive
2. Digital Services Act (DSA)(2022)

ماده ۵ قانون خدمات دیجیتال مقرر می‌دارد: «۱- ارائه دهندگان خدمات واسطه‌ای در قبال اطلاعاتی که به درخواست دریافت‌کننده خدمات ذخیره می‌شود، مسؤول نخواهند بود، به شرط آن‌که: الف- ارائه‌دهنده از محتوای غیرقانونی آگاهی واقعی نداشـــته باشد و در خصوص ادعاهای خسارت، از حقایق یا شـــرایطی که فعالیت یا محتوای غیرقانونی را آشکار می‌سازد مطلع نباشد؛ یا ب- پس از کسب چنین آگاهی یا اطلاع، به‌سرعت برای حذف یا مسدود کردن دسترسی به محتوای غیرقانونی اقـــدام کند؛ ۲- بند ۱ در مواردی که دریافت‌کننده خدمـــات تحت اختیار یا کنترل ارائه‌دهنده عمل می‌کند، اعمال نخواهد شد».

آن‌ها در نظر می‌گیرد (MacKinnon et al, 2015: 40). در این نظام، تمرکز بر مسؤولیت سکوها موجب محدود شدن نقش کاربران و دولت خواهد شد و لذا تنظیم‌گری مشارکتی که به دنبال توزیع مسؤولیت است با اصول دو نظام مسؤولیت محدود و مصونیت مطلق سازگارتر خواهد بود که نیازمند تبیین و تدقیق رهیافت‌های مختلف موجود در راستای اعمال این تنظیم‌گری در بستر هریک از آن‌ها می‌باشد.

۲. هم‌تنظیمی به عنوان پایه

تنظیم‌گری مشارکتی، به‌عنوان رویکردی نوین در فضای دیجیتال، شامل مجموعه‌ای از ابزارها و مکانیسم‌هایی است که با همکاری دولت، بخش خصوصی و سایر ذی‌نفعان تلاش می‌کند تعادلی میان حمایت از کاربران، حفظ منافع عمومی و تقویت نوآوری برقرار کند. در این چارچوب، دو رهیافت کلیدی خودتنظیمی[1] و هم‌تنظیمی[2] به عنوان بنیان‌های اصلی این نوع تنظیم‌گری شناخته می‌شوند. این دو رهیافت به شکلی متقابل یکدیگر را تقویت می‌کنند و می‌توانند به ایجاد یک محیط دیجیتال منصفانه، شفاف و مؤثر کمک کنند؛ زیرا این دو، مدل‌های ترکیبی در تنظیم‌گری هستند که هم‌تنظیمی نقش پایه‌ای و چارچوب‌ساز دارد و قوانین و مقررات پایه‌ای را تعریف می‌کند که همه سکوها ملزم به رعایت آن‌ها هستند. در مقابل، خودتنظیمی به‌عنوان یک مکمل عمل می‌کند و به سکوها این امکان را می‌دهد که بر اساس شرایط خاص خود، استانداردها و سیاست‌های اجرایی را تطبیق داده و روزآمد کنند. در هم‌تنظیمی، دولت‌ها و قانون‌گذاران، اصول و الزامات کلی را تعیین می‌کنند، اما جزئیات اجرای این اصول بر عهده سکوها گذاشته می‌شود؛ به مانند مدیریت محتوای کاربران یا رعایت استانداردهای امنیتی (Finck, 2018: 16). این رهیافت به دولت‌ها این امکان را می‌دهد که به‌طور غیر مستقیم و از طریق همکاری با سکوها، نظارت مؤثری بر فضای دیجیتال اعمال کنند. قوانین اروپایی و آمریکایی نمونه‌های بارزی از چارچوب‌های هم‌تنظیمی هستند که از سکوها می‌خواهند در راستای اهداف عمومی عمل کنند؛ اما آزادی عمل قابل‌توجهی در نحوه اجرای این

1. Self-regulation
2. Co-regulation

قوانین به آن‌ها می‌دهند.

۱-۲. چارچوب‌های هم‌تنظیمی در اروپا: از «قانون تجارت الکترونیک» تا «قانون خدمات دیجیتال»

از نمونه‌های برجسته هم‌تنظیمی در اروپا، دستورالعمل تجارت الکترونیک است که به‌عنوان نقطه آغاز این رویکرد در فضای دیجیتال شناخته می‌شود. این دستورالعمل ضمن تعیین اصول کلی برای فعالیت سکوها، مسؤولیت آن‌ها را محدود به شرایط خاصی کرده و فضای لازم برای خودتنظیمی در چارچوب نظارت کلان دولت را فراهم نموده است. با مداقه در مواد ١٤ و ١٥ دستورالعمل، دو رکن به عنوان ارکان اساسی رژیم مسؤولیت محدود آن می‌توان در نظر گرفت: رکن نخست، یک معافیت را اعلام می‌کند که بستر میزبانی مشمول آن است و در سطح اروپا شرایط چنین معافیتی را هماهنگ می‌کند. یک سکوی رایانه‌ای می‌تواند از مسؤولیت محتوای غیرقانونی فرار کند که از غیرقانونی بودن اطلاع نداشته و در صورت اطلاع، فوراً برای حذف یا غیرفعال‌کردن دسترسی به آن اقدام کرده باشد؛ و رکن دوم، ممنوعیت کشورهای عضو اتحادیه اروپا برای تحمیل یک تعهد کلی بر سکوهای رایانه‌ای برای نظارت بر محتوا است.

این رژیم حقوقی اولاً، به دنبال تقسیم مسؤولیت برای اینترنت امن برای تمام بازیگران خصوصی درگیر و همکاری با مقامات دولتی است و لذا کاربران در صورت مشاهده هرگونه تخلف انتظار می‌رود سکوها را مطلع سازند و سکوها نیز باید هرگونه محتوای غیرقانونی که از آن مطلع می‌شوند، حذف یا مسدود نمایند؛ ثانیاً، توسعه تجارت الکترونیک را از طریق ایجاد اطمینان از این که میزبانی سکوها تعهدی به نظارت بر قانونی بودن تمامی محتواهای موجود و ذخیره شده در بستر آن‌ها ندارد، تشویق می‌کند؛ زیرا این امر بسیار پرهزینه است؛ ثالثاً، بین حقوق اساسی مختلف به ویژه حریم خصوصی، حفاظت از داده‌های شخصی، آزادی بیان و اطلاعات، آزادی انجام تجارت و حق مالکیت از جمله مالکیت معنوی، تعادل عادلانه ایجاد کرده است (Buiten et al, 2020: 3). البته رویه قضایی دیوان دادگستری اتحادیه اروپا[1] سکوها را به لحاظ این اطلاع از محتوای غیر قانونی

1. Court of Justice of the European Union (CJEU)

و تحمیل مسؤولیت بر آن‌ها به دو قسم فعال و منفعل تقسیم می‌کند. سکوهای منفعل صرفاً زیرساخت فنی برای ذخیره یا انتقال محتوا فراهم می‌کنند و هیچ‌گونه نقشی در گزینش، سازماندهی یا نمایش محتوای کاربران ندارند. در مقابل سکوهای فعال به نحوی در پردازش یا مدیریت محتوا دخالت می‌کنند؛ برای مثال از طریق الگوریتم‌های رتبه‌بندی، تبلیغات هدفمند، پیشنهادهای محتوایی یا ساختاردهی صفحات کاربران؛ به گونه‌ای که می‌توان برای آن‌ها نوعی کنترل یا آگاهی احتمالی نسبت به محتوای بارگذاری‌شده فرض کرد.[1] حال سکو برای معافیت از مسؤولیت تحت لوای این قانون باید خنثی بوده و صرفاً با پردازش فنی، خودکار و غیرفعال داده‌های ارائه‌شده توسط کاربران خود، خدماتی را ارائه بدهد و نقش فعال به گونه‌ای ایفا نکند که به او آگاهی یا کنترل بر داده‌ها را بدهد (Hornik, 2017: 3-4). هم‌چنین این قانون اصل کشور مبدأ[2] را ایجاد کرده است؛ بدین معنا که یک سکوی رایانه‌ای صرفاً تابع رژیم مسؤولیت کشور عضو اتحادیه اروپا است که در آن تأسیس شده است.

به هر حال منفعل بودن سکو نسبت به فعالیت شخص ثالث در بستر خود و محتوای وی، مفروض مسؤولیت محدود اندیشیده‌شده در دستورالعمل تجارت الکترونیک است. اما این ناظر به زمانی بود که هنوز سکوهای رایانه‌ای تکامل امروزی خود را پیدا نکرده بودند و با افزایش نقش آن‌ها در دنیای دیجیتال کم‌کم چنین مسؤولیتی نیز محدود گشت و نقش منفعل آن‌ها به نقش فعال و کنترلی تغییر کرد. در واقع رشد شتابان فناوری، ظهور سکوهای عظیم و تغییر رفتار کاربران در دو دهه بعد از آن، نیاز به بازنگری جدی در قوانین را نمایان کرد. سرانجام اتحادیه

---

۱. به عنوان مثال، سکوی «فضای من» (MySpace) توسط دادگاه پاریس به علت حذف نکردن ویدیوهای مربوط به یکی از کاربران خود که بدون اجازه او پست شده بود مقصر شناخته شد و استدلال دادگاه این بود که این سکو به جهت ساختار از پیش تعیین شده صفحات شخصی کاربران و همچنین وجود تبلیغات سودآور در وب سایت، واجد شرایط ویرایش محتوای برخط تلقی می‌شود. چنان‌که سکوی میزبانی ویدیو IOL که تحت صلاحیت ایتالیا بود نیز به نحو مشابهی با اعتقاد بر دانش واقعی داشتن از محتوای غیر قانونی مسؤول شناخته شد؛ زیرا اطلاعات بارگذاری‌شده را فهرست‌بندی می‌کرد و به کاربران اجازه می‌داد تا ویدیو ها را از طریق یک سرویس جستجوی مرتبط پیدا کنند. اما در همان زمان، سکوی ویدیو فرانسوی Daily motion به عنوان یک سکوی غیر فعال شناخته شد؛ زیرا درگیری آن با محتوای برخط صرفاً فنی بود.

2. Country of Origin Principle

اروپا در واکنش به این تحولات و با هدف به‌روزرسانی چارچوب حقوقی خود به تدوین نظام جدید در تنظیم‌گری سکوها با ارائه دو قانون خدمات دیجیتال و قانون بازارهای دیجیتال[1] پرداخت.[2]

قانون خدمات دیجیتال قصد دارد دستورالعمل تجارت الکترونیک را بدون تغییر اساسی مدرن نموده و جهت تمایز بین واسطه‌ها، ارائه دهندگان میزبانی، سکوهای برخط و سکوهای برخط بسیار بزرگ[3] مقرراتی را ارائه دهد. در واقع این قانون، دستورالعمل تجارت الکترونیک را نسخ نمی‌کند؛ بلکه صرفا مقررات خاصی را اصلاح و به دنبال هم‌زیستی با سایر قوانین است (Buiten, 2021: 368). ماده ۵ این قانون مقرراتی به مانند ماده ١٤ دستورالعمل تجارت الکترونیک مقرر کرده و خدمات میزبانی را تا زمانی که محتوای غیرقانونی را با اطلاع از آن فوراً حذف می‌کنند، از مسؤولیت معاف می‌سازد. مقرره‌ای که در عمل منجر به فعال‌شدن روش‌های اطلاع‌رسانی و حذف شده تا کاربران به ارائه دهندگان در خصوص غیرقانونی بودن اطلاع دهند و الزامات جدیدی را برای اخطار و حذف تعیین می‌کند. به عبارتی، برخی کاستی‌های دستورالعمل تجارت الکترونیک[4] از جمله ایجاد الزامات شفافیت و ارائه ابزارهای گزارش‌دهی، رویکرد مشخص‌تر به تعریف آگاهی واقعی،[5] الزام زمانی دقیق برای اقدام سریع و تأکید بر سازکارهای نظارت فعال توسط فناوری‌های مدرن را رفع می‌کند. البته این رفع کاستی‌ها به طور مستقیم

---

1. Digital Markets Act 2022)

۲. قانون خدمات دیجیتال (DSA) و قانون بازارهای دیجیتال (DMA) به عنوان دو قانون مکمل برای تنظیم فضای دیجیتال شناخته می‌شوند. این دو قانون، به دلیل طراحی هماهنگ و هدف مشترک در ایجاد یک چارچوب شفاف و عادلانه برای فضای دیجیتال، گاهی به عنوان قوانین دوقلو یاد می‌شوند. با این حال هر یک به حوزه‌های متفاوتی می‌پردازند و تمرکز ویژه‌ای دارند؛ چنان‌که قانون خدمات دیجیتال بر مسائل مرتبط با محتوا و خدمات دیجیتال تمرکز دارد. این قانون به مسؤولیت سکوها در مدیریت محتوا، جلوگیری از انتشار محتوای غیرقانونی، حفاظت از حقوق کاربران و ایجاد شفافیت در شیوه‌های عمل سکوها می‌پردازد، اما قانون بازارهای دیجیتال بر ساختار رقابتی و انحصارگری در بازارهای دیجیتال متمرکز است. این قانون تلاش می‌کند قدرت انحصاری شرکت‌های بزرگ فناوری را محدود کند و رقابت سالم را در بازار دیجیتال تضمین نماید.

3. Very Large Online Platform (VLOP)

٤. ماده ١٤ این دستورالعمل

5. Actual Knowledge

در متن ماده‌ای مشخص نشده و به‌طور خاص از طریق ارتباط مواد این قانون (مانند ماده ۵ با مواد ۱۶، ۱۷، ۲۰ و ۳۴) درک می‌شود؛ چنان‌که ماده ۱۶ وظیفه سکوها در ایجاد یک سازِکار گزارش‌دهی شفاف و کارآمد را تشریح نموده و آگاهی واقعی تحت ماده ۵ را فعال می‌کند.

قانون خدمات دیجیتال همچون دستورالعمل تجارت الکترونیک، کشورهای عضو اتحادیه اروپا را از تحمیل یک تعهد کلی نظارت بر سکوها منع می‌کند؛ با این تفاوت که این قانون اعلام می‌کند که مقامات و دادگاه‌ها می‌توانند دستوراتی را در راستای توقف تخلفات مربوط به محتوای غیرقانونی خاصی صادر کنند (مواد ۷ و ۸ و ۹). این قانون اثر فراسرزمینی دارد؛ بدین معنا که مقررات آن هر زمان که گیرنده خدمات در اتحادیه اروپا باشد، صرف‌نظر از محل استقرار یا اقامت ارائه‌دهنده خدمات اعمال خواهد شد. به علاوه یک ارتباط اساسی بین ارائه‌دهنده خدمات و اتحادیه اروپا را لازم می‌دانند؛ یعنی یک سکو تعداد قابل توجهی کاربر در اتحادیه اروپا داشته باشد یا ارائه‌دهنده هدف فعالیت‌های خود را به سمت یک یا چند کشور عضو قرار دهد (ماده ۲). به همین دلیل، سکوهای رایانه‌ای مستقر در خارج از اتحادیه اروپا که در اروپا فعال هستند موظف به تعیین یک نماینده قانونی در اتحادیه اروپا می‌باشند.

در فصل چهارم قانون خدمات دیجیتال پس از معرفی مکانیسم‌های اجرایی دقیق برخلاف دستورالعمل تجارت الکترونیک و به مانند دستورالعمل جامع حفاظت از داده‌های ۲۰۱۶ اتحادیه اروپا (ماده ۴۱). به‌طور خاص مقامات ملی مسؤول اعمال مقررات را مشخص می‌کند و مرجع نظارت را براساس محل استقرار اصلی خدمات قرار می‌دهد و مقرر می‌دارد به منظور تسریع در اجرا توسط مقامات ملی، هرکشور عضو باید یک ناظر خدمات دیجیتالی را منصوب کند که به عنوان مسؤول نظارت بر خدمات واسطه‌ای در آن کشور ایجاد شده و به عنوان یک مرجع مستقل و شفاف اقدام می‌نماید و به این ناظران خدمات دیجیتال اختیارات قابل توجهی اعطا می‌کند؛ چنان‌که آن‌ها می‌توانند از هرکس که اطلاعات مربوط به تخلفات را دارد درخواست همکاری کنند، از اماکن مورد استفاده سکوها بازرسی نمایند و حتی حق توقیف اطلاعات مربوط به تخلفات مشکوک و قدرت بازجویی از هر کارمندی را دارند

(ماده ٤١). به مانند سند پیش‌گفته، قانون خدمات دیجیتال نیز یک ناظر اروپایی را که به عنوان هیأت اروپایی خدمات دیجیتال[1] شناخته می‌شود تعیین می‌کند (مواد ٤٧ تا ٤٩) (Buiten, 2021: 377).

البته این قانون بین سکوهای رایانه‌ای بسیار بزرگ و سایر سکوها تفاوت قائل شده و به این سکوها تعهدات بیشتری را بار نموده است. به عبارت بهتر، قانون خدمات دیجیتال به دنبال ایجاد نظامی نامتقارن در جهت تنظیم‌گری سکوها برآمده است؛ بدین معنا که بسته به اندازه، اهمیت و ماهیت کارکردی سکوها، مسؤولیت متفاوتی را در نظر گرفته است و سکوهای رایانه‌ای بسیار بزرگ با مسؤولیت‌های بیشتر مواجه گشته‌اند. سکوهای بسیار بزرگ از لحاظ این قانون سکوهایی هستند که میانگین ماهانه حداقل چهل و پنج میلیون کاربر فعال یا ده درصد از جمعیت اتحادیه اروپا را پوشش می‌دهند (ماده ۳۳). این سکوهای بسیار بزرگ به لحاظ مکانیسم‌های اجرایی نیز تابع یک رژیم جداگانه و دقیق‌تر هستند؛ به نحوی که اگر ناظر متوجه رفتار ناقض از سوی هریک از آن‌ها شود، مشمول نظارت بیشتر براساس ماده ۵۰ و تعبیه یک برنامه اقدام[2] و یک کد رفتاری خواهد بود.

هم‌چنین کمیسیون اروپا در خصوص این سکوها اختیارات گسترده‌ای دارد و مشابه نقش کمیسیون در زمینه قانون رقابت اتحادیه اروپا، این قانون اجازه می‌دهد تا تحقیقات، اقدامات موقت، اعمال ضمانت اجراهای خاص هم‌چون جریمه‌های نقدی، جریمه‌های دوره‌ای داشته باشد. به عبارت بهتر، در مقایسه با دستورالعمل تجارت الکترونیک مصوب سال ۲۰۰۰ که صرفاً چارچوبی کلی برای مسؤولیت واسطه‌ها ارائه می‌داد و تعیین ضمانت اجراها را به کشورهای عضو واگذار کرده بود؛ امری که به پراکندگی و ضعف در اجرا منجر می‌شد، قانون خدمات دیجیتال مصوب ۲۰۲۲ با هدف رفع این کاستی‌ها، مجموعه‌ای شفاف، هماهنگ و قدرتمند از ضمانت اجراها پیش‌بینی کرده است. این قانون نه‌تنها الزامات مشخصی در خصوص حذف محتوای غیرقانونی و شفاف‌سازی عملکرد الگوریتمی تعیین کرده، بلکه کمیسیون اروپا را به نهادی ناظر با اختیارات گسترده بدل ساخته است؛ از جمله

1. European Board for Digital Services
2. Action plan

اعمال جریمه‌های مالی تا شـــش درصد از گردش مالـــی جهانی (ماده ۵۲)، صدور دستور توقف فعالیت سکوها در صورت نقض مکرر (ماده ۵۱) و بازرسی حضوری و دسترســـی به داده‌ها و الگوریتم‌ها (مواد ٦٧ تـــا ٧٤). البته در صورت تداوم عدم انطباق، کمیسیون می‌تواند از طریق هماهنگ‌کنندگان ملی نیز از افسر انطباق آن سکو بخواهد همکاری مؤثر داشته باشد (بند ۳ ماده ٤١). در خصوص این سکوها، قانون خدمات دیجیتال یک مدل نظارتی متمرکز را با کمیسیون به عنوان تنظیم‌گر پیش‌بینی می‌کند. به نظر می‌رســـد این انتخاب، پاسخ به شـــکایاتی بود که در اجرای مقررات جامع حفاظـــت از داده‌های اتحادیـــه اروپا به وجود آمد؛ زیرا تجـــربه این قانون نشـــان داد که مقـامات حـــفاظت از داده‌های ایرلند تحت فشار در پاسخ‌گویی به شکایات، کند عـــمل می‌کردنـد. ادغام ناظر خدمات دیجیتال ملی در هیأت اروپایی خدمات دیجیتال، به کمیسیون این امکان را می‌دهـد تا اصل کشور مبدأ را دور بزند و از این که تمام شکایات در مورد سکوهای بسیـــار بزرگ به یک مرجع ملی ختم شـــود، اجتناب نماید (Buiten, 2021: 378). البته باید به این نکته نیز که توجه کرد که انتصاب کمیســـیون به عنوان تنظیم‌گر دال بر آن اســـت سکوها با دو نهاد روبه‌رو خواهنـــد بود. از یک ســـو یک مرجع حفاظت از داده‌ها و از ســـوی دیگر یک نهاد ناظر خدمات دیجیتال که تعامل آن‌ها بســـیار مهم و ضروری است؛ زیرا سکوها باید برای اجرای تکلیف مربوط به مدیریت شـــکایات، حجم زیادی از داده‌ها شخصی را پردازش کنند.

یکی از جامع‌ترین چارچوب‌های قانونی در زمینه حفاظت از حریم خصوصی کاربران در فضای دیجیتال، دســـتورالعمل جامع حفاظـــت از داده‌های اتحادیه اروپا اســـت که بر اساس آن، مســـؤولیت‌های گسترده‌ای برای ســـکوهای رایانه‌ای تعیین شده اســـت. این دســـتورالعمل با تأکید بر اصولی مانند شفافیت، حفاظت از داده‌ها و حق کاربران بر مدیریت اطلاعات شـــخصی خود، سازکارهایی را برای نظارت بر پردازش داده‌ها و مقابله با نقض حریم خصوصی پیش‌بینی کرده اســـت. مطابق این دستورالعمل، برای شمول آن بر یک سکو، سه شرط شخصی بودن اطلاعات، وجود فرایند پردازش داده، کنترل‌کننده بودن سکو باید احراز شود. البته همان‌گونه که سابقاً اشاره شد شرط چهارمی نیز وجود دارد که این دستورالعمل زمانی اعمال می‌شود که

پـــردازش داده‌ها در حوزه اتحادیه اروپا صورت گیرد یا خدمات به کاربران اروپایی ارائه شـــود. سکوهای رایانه‌ای در صورتی که این شرایط را احراز کنند و در اجرای تکالیف خود کوتاهی نمایند مسؤول خواهند بود. طبق این دستورالعمل، سکوها باید تدابیر فنی و ســـازمانی مناســـب برای حفاظت از داده‌های شخصی کاربران را اتخاذ کنند تا از هرگونه تخریب غیرقانونی، تغییر، افشـــا، دسترسی بدون مجوز یا خسارت جلوگیری شود.

از نظر ضـــمانت اجرا و مسوولیت، این دستورالـعمل تأکید دارد که هرگونه فعل یا ترک فعل که منجر به نقض حریم خصوصی و خســـارت به کاربران شـــود، موجب مسؤولیت مدنی و حتی در برخی موارد مسؤولیـــت کیفری سکوها خواهد بود (ماده ۲۳). در همین راســـتا نیز ضمانت اجراهایی بـــرای نقض تعهدات حریم خصوصی پیش‌بینی کرده اســـت؛ از جمله حق افراد برای مطالبه غرامت از ســـکوی ناقض در صورت ورود خســـارت (ماده ۸۲)، اعمـــال جریمه‌های مالی تا ســـقف بیست میلیون یورو یا چهار درصد ازگردش مالی ســالانه جهانی (ماده ۸۳) و اختیار نهادهای نظارتی برای صدور دســـتورات اجرایی نظـــیر توقف پردازش یا اصلاح رویه‌های ناقض مقررات (ماده ۵۸). همـچنین در موارد خاص، امکان محدودسازی برخی از حقوق مندرج در دســـتورالعمل جـــامع حفاظت از داده‌های اتحادیه اروپا برای تأمین منافع عمومی یا امنیت ملی با رعایت اصول ضرورت و تناسب پیش‌بینی شده است (ماده ۲۳). در مواردی که کاربر نیز در نقض حریم خصوصی دخیل باشد، مسؤولیت مشترک میان سکو و کاربر برقرار می‌شود. این بدان معناست که اگر نقض قابل اســـتناد به رفتار یا اقدامات کاربر باشد، هر دو طرف در برابر زیان‌دیده مسؤول خواهنـــد بود. این رویکرد، ضمـــن حفظ تعادل میان حقوق کاربران و مســـؤولیت ســـکوها، به جلوگیری از سوء اســـتفاده احتمالی توســـط کاربران نیز کمک می‌کند (Udrea& Smith,2021: 12).

نمونه این قواعد را در سیســـتم مقررات آلمان می‌توان مشاهده کرد. آلمان در سال ۲۰۱۷ «مصوبه بهبود اجرای قانون در شبکه‌های اجتماعی»[1] را تصویب نمود که

---

۱. NetzDG یا مصوبه بهبود اجرای قانون در شبکه‌های اجتماعی که به‌صورت کامل Netzwerk-durchsetzungsgesetz نامیده می‌شـــود و به انگلیسی به «Network Enforcement Act» ترجمه شده است.

هدف آن مبارزه با محتوای غیرقانونی در شـــبکه‌های اجتماعی بوده و شامل مقرراتی ســـخت‌گیرانه برای سکوها و کاربران می‌باشد. این قانون برای ساماندهی محتواهای مشکل‌ســـاز ابتدا مسؤولیت را بر عـــهده خود ســـکوها می‌گذارد؛ به جای این که مرجعی جدید برای رســـیدگی به چنین موضوعی ایجاد کند؛ زیرا طبق بند ۱۰ قانون تله‌مدیـــا ۲۰۰۷ آلمان[1] ارائه دهندگان خدمات بـــه محض اطلاع از غیر قانونی بودن محتوا باید اقدام به حذف آن کنند و شخصی که فراهم‌کننده خدمات و زیرساخت‌ها بوده و آن را در اختیار اشـــخاص دیگر قرار می‌دهد باید تا حد توان از سوء استفاده از آن جلوگیری نماید و مسؤولیت در برابر چنین سوء استفاده‌هایی ابتدا با خود وی است و در قانـــون مدنی آلمان هیچ قاعده‌گذاری مبنی بر این که مسؤولیت ابتدایی حل و فصل و رســـیدگی به مشـــکلات محتوای غیرقانونی با دادگاه‌ها است، وجود ندارد.[2]

قانون بهبود اجرای قانون در شـــبکه‌های اجـــتماعی بر مبنای اصول بند ۱۰ فوق‌الاشـــاره توسعه داده شد و به‌طور خاص مســـؤولیت بیشتری را برای سکوهای بزرگ تعریف کرد و آن‌هـــا را ملزم به حذف ســـریع محتوای غیرقانونی کرد. این قانون، شبکه‌های اجتماعی با بیـــش از دو میلیون کاربر ثبـــت شـــده در آلمان را موظف می‌کند تا در قبال محتوای غـــیرقانونی حسب وصف آن‌ها به این شـــرح ذیل عمل کنند: الف- محتوای آشـــکارا غیرقانونی: ســـکو تا بیست و چهار ساعت برای تصمـــیم‌گیری فرصت دارد؛ ب- در مواردی استـــثنایی و پیچیده‌تر، این بازه زمانی می‌تـــواند تا هفت روز افزایش یابد؛ به مانند آن که از کاربر بارگزارنده محتوا

1. TelemediaAct (2007)

قانون (TMG) Telemediengesetz که به‌عنوان «قانون خدمات تل‌مدیایی آلمان» شناخته می‌شود، چارچوب حقوقی ارائه خدمات اطلاعاتی و ارتباطی الکترونیکی در این کشور را مشخص می‌کند. بند ۱۰: «ارائه‌دهندگان خدمات برای اطلاعاتی که توســـط دیگران بارگذاری شده و آن‌ها صرفاً آن را ذخیره می‌کنند، مســـؤولیتی ندارند، به شـــرط آن‌که: ۱- از فعالیت یا اطلاعات غیرقانونی آگاهی نداشته باشـــند و در خصوص ادعاهای خسارت از هیچ واقعیت یا شرایطی که نشان‌دهنده فعالیت یا اطلاعات غیرقانونی باشـــد، مطلع نباشـــند یا ۲- به محض اطـــلاع از چنین فعالیت یا اطلاعاتی، بلافاصله اقدام به حذف اطلاعات یا مسدودسازی دسترسی به آن کنند».

2. German Federal Ministry of Justice and Consumer Protection, "Questions and answers: Act to Improve Enforcement of the Law in Social Networks." www.bmjv.de/SharedDocs/FAQ/EN/NetzDG/NetzDG.html

درخواست نظر شود یا تصمیم‌گیری به یک انجمن صـــنفی مشترک معتبر به عنـوان موسســـه خودتنظیمی سپرده شـــود. محتوا به دو حالت مورد بررسی قرار می‌گیرد: یکم، تحت خط‌مشـــی‌ها و دستورالعمل‌های جهانی سکو مثل گوگل که در صورت نقض آن‌ها به طور جهانی حذف می‌شـــود؛ دوم، تحت قانون بهبود اجرای قانون در شـــبکه‌های اجتماعی که در این صورت صرفاً به صورت محلی محدود خواهد شد. برای این که تحت قانون پیش‌گفته واجد شـــرایط حذف شـــود، باید تحت یکی از بیســـت و یک بند قانون کیفری آلمان قرار گیرد. ممکن است محتوا هم ناقض قانون و هم دستورالعمل باشد که حذف جهانی می‌شود. البته قانون بهبود اجرای قانون در شبکه‌های اجتماعی به سکوها این امکان را می‌دهد که در شرایطی که گزارش تخلف مورد بحث اســـت با بارگذارنده تماس بگیرد؛ با این حال دریافت پاسخی قابل قبول از بارگذارنده به شـــکایت دقیق و موجه قانونی ارسال‌کننده که چرا محتوا غیرقانونی اســـت نیاز دارد. در واقع گاه شکایت ناقص است که ابتدا اطلاعات بیشتر و تکمیلی از ارســـال‌کننده درخواست می‌شود و گاه شـــکایت به حدی است که نمی‌توان فوراً تصمیم‌گیری در خصوص غیرقانونی بودن آن داشـــت و نیاز به تعامل با بارگذارنده دارد.[۱]

این قانون تکالیف دیگری را نیز بر سکوها و سایر اشخاص بار نموده است؛ چنان‌که شـــهروندان آلمان در راستای اطلاع‌رســـانی محتواهای غیرقانونی موجود، مســـؤول هستند و ملزم هســـتند آن را به اطلاع مرجع ذی‌صلاح برسانند و همچنین کاربران و شـــهروندان که از وجود محتوای غیرقانونی در ســـکوها که مخل حقوق شخصی آن‌ها شده شاکی هســـتند، می‌توانند قبل از اقدام قضایی به دفاتر نمایندگی آن‌ها مراجعه کنند و حذف این محتوا را درخواست نمایند و سکوها موظف هستند به این درخواســـت‌ها با قید فوریت رسیدگی نمایند (Bülent, 2020: 4)؛ زیرا طبق این قانون، ســـکوها ملزم به تأسیس نمایندگی مجاز در خاک کشور آلمان شده‌اند تا دفتری جهت پاسخ‌گویی به مراجعان وجود داشته باشد؛ چنان‌که فیس‌بوک طبق این قانون صدها نفر آلمانی‌زبان را جهت تأســـیس نمایندگی خود استخدام کرده است.

---

۱. برای مشاهده نمونه گزارش شفافیت گوگل بر اساس مصوبه فوق الاشاره رجوع کنید به:
Https://transparencyreport.google.com/netzdg/googleplus?hl=fa&items_by_submitter=period:2019H1&lu=items_by_submitter

البته فیس‌بوک برخلاف سکوهایی مثل توییتر، نمایندگی مستقل در خاک آلمان ایجاد نکرده و تمامی اقدامات خود را از طریق مقرّ اروپایی خود در دوبلین[1] پیگیری می‌کند (GEDİKLİ, 2020: 234). باید دقت کرد که محتوای غیرقانونی از سوی قانون‌گذار آلمانی، به لحاظ مفهوم و مصداق مشخص گشته و امری سلیقه‌ای و یا کلی و به عهده سکوها گذاشته نشده است. همچنین قانون بهبود اجرای قانون در شبکه‌های اجتماعی سکوها را ملزم می‌کند تا دو بار در سال گزارش شفاف‌سازی درباره شیوه و تعداد و نحوه رسیدگی خود به شکایات در خصوص چنین محتوایی را منتشر کنند. این الزام موجب مبارزه موثر و دائم سکوها با چنین محتواهایی خواهد بود (Sağıroğlu&Alkan, 2018: 337). لازم به ذکر است که عدم رعایت این الزامات می‌تواند منجر به اعمال جریمه‌های سنگین توسط اداره فدرال عدالت آلمان[2] تا سقف پنجاه میلیون یورو شود.

علاوه بر قوانین فوق، برخی مقررات خاص در راستای مبارزه با انواع خاصی از محتوای غیرقانونی در چارچوب سیاست‌گذاری‌های اتحادیه اروپا تصویب شده است. دستورالعمل سوءاستفاده جنسی از کودکان مصوب ۲۰۱۱ [3] کشورهای عضو اتحادیه اروپا را ملزم می‌کند تا اطمینان حاصل کنند که سکوها محتواهایی که حاوی هرزه‌نگاری کودکان هستند را فوراً حذف کنند. دستورالعمل مبارزه با تروریسم مصوب ۲۰۱۷ [4] از کشورهای عضو می‌خواهد از حذف سریع محتوای برخط که یک درخواست عمومی برای یک ارتکاب یک جرم تروریستی است اطمینان حاصل کنند. دستورالعمل بازنگری شده خدمات سمعی و بصری مصوب ۲۰۱۸ [5] سکوهایی را که میزبان محتوایی هستند که در خصوص آن مسؤولیت ویرایشی ندارند، مانند ویدیوهای ارسالی از ناحیه کاربران، ملزم می‌کند تا اقداماتی در خصوص محتوای مضر در حوزه تروریست، موضوعات نژادپرستانه، هرزه‌نگاری[6] کودکان و سخنان

1. Dublin
2. BundesamtfürJustiz
3. Directive on combating the sexual abuse and sexual exploitation of children and child pornography (2011)
4. Regulation on combating terrorism
5. Directive amending the Audiovisual Media Services Directive (AVMSD)
6. Pornography

نفرت‌افکـــن برای عموم مردم انجام دهند. دســـتورالعمل حق نشـــر مربوط به بازار واحد دیجیتال اروپا مصوب ۲۰۱۹ [1] ارائه دهندگان خدمات اشتراک‌گذاری محتوای برخط را ملزم می‌کند تا بهترین تلاش خود در راستای دریافت مجوز برای محتوای ارسال‌شده توسط کاربران خود به کار گیرند و در صورت عدم حذف مطالب پس از اطلاع و آگاهی، آن‌ها را مسؤول نقض حق نشر می‌داند.

۲-۲. هم‌تنظیمی در آمریکا؛ نقش «قانون حسن ارتباطات» در مدیریت سکوها

هرچند طبق بخش ۲۳۰ قانون حســـن ارتباطات آمریکا، ســـکوها مصون از مسؤولیت هستند و می‌توانند بدون پذیرش مسؤولیت قانونی، محتواهای نامناسب یا مضر را حذف یا مدیریت کنند، اما باید توجه داشت که برخی سکوها مثل سکوهای تولید محتوا کاربرمحور، نه تنها وظیفه اتصال اشـــخاص را به عهده دارند و محتوا را میزبانی می‌کنند، بلکه آن را ســـازماندهی نمـــوده و حتی در برخی موارد به صورت الگوریتمـــی، زیرمجموعه‌ای از آن انتخاب می‌کنند تا به عنوان پیشـــنهادات صفحه اول کانال‌های اشـــتراکی اخبار مطرح شوند. در واقع مشارکت‌های صورت‌گرفته در فضای ســـکوها همچون ماده خامی برای آن‌ها عمل می‌کنند تا جریانی هیجان‌انگیز شبیه پخش ایجاد کنند (Gillespie, 2017: 209-211). همین نقطه است که موجب شـــده تا برخی معتقد باشند که ســـکوها در قبال چنین محتواهایی مسؤول هستند و نمی‌توانند به طور تام از بندر امن [2] بخش ۲۳۰ بهره‌مند شـــوند. به عبارت بهتر، وقتی یک ســـکو پیشنهاد می‌کند که شما را به دوستان و فالوورها متصل کند و آنچه را که آن‌ها به شـــما می‌گویند و آنچه را شـــما می‌گویید به آن‌ها ارائه دهند، چنین رفتاری از مصونیت بخش ۲۳۰ برخوردار اســـت، اما وقتی سکو به هدف افزایش ارزش‌ها و افزایش علاقمندی کاربران و و بقای آن‌ها اقدام به انتخاب برخی از محتواها نســـبت به سایرین می‌کند، در قبال چنین محتوای جمع‌آوری‌شده، مسؤول هستند؛ حتی اگر به نحو تام از محتوای کاربران تشـــکیل شده باشـــد و تولید محتوایی از ناحیه خود سکو به عمل نیامده باشد.

---

1. Directive on Copyright in the Digital Single Market
2. Safe harbor

یک اســـتثنای جالب در خصوص اعمال بخـــش ۲۳۰ تصمیم در خصوص ســـکوی هم‌اتاقی[1] در ایالات متحده است. ســـکوی هم‌اتاقی متهم به تسهیل تبعیض براساس نژاد و ترجیحات جنسی بود؛ زیرا نظرسنجی از کاربران داشت تا ترجیحات هم اتاقی آن‌ها را بشناســـد و پس از آن از این اطلاعات برای نشان دادن الگوریتمی برخی از حساب‌های کاربری[2] به برخی از کاربران استفاده می‌نمود. هرچند این سکو به بخش ۲۳۰ و مصونیت آن اســـتناد کرد، اما دادگاه حکم داد که چون ســـکو این جزئیات شـــخصی را خواسته و به صورت الگوریتمی انتخاب کرده که چه چیزی را به چه کسی نشـــان دهد، آن‌قدری در ایجاد و توزیع این اطلاعات شرکت داشته که نمی‌تواند از چنین مصونیتی برخوردار شود (Gillespie, 2017: 211). اما در دعوای ابرهارت[3] علیه آمازون، دادگـــاه منطقه فدرال نیویورک اعلام کرد که آمازون خارج از زنجیره توزیع اســـت و به همین دلیل نمی‌تـــوان آن را به عنوان یک توزیع‌کننده، تحت مسؤولیت سخت‌گیـرانه محصولات ایالتی مسؤول دانست (Sharkey, 2022: 1335-1336).

به هر حال، از یک ســـو این مقرره، ســـپر بزرگی را برای سکوهای رایانه‌ای ایجاد کرده و گزینه‌های قانونی موجود جهت مبارزه با انتشار محتواهای غیر قانونی در چنین بستری را محدود کرده است و از سوی دیگر تصویب هر قانون جهت رفع چنین مصونیتی با واکنش متمم اول قانون اساسی روبه‌رو بوده و باید از سد مستحکم حمایت آن از آزادی بیان بگذرد؛ زیرا با محدود کردن یا لغو آن امکان به خطر افتادن آزادی بیان و محدودیت در آن به شـــدت محتمل اســـت (ناتانیل پرســـیلی، ۱۴۰۰: ٤٤٢). به علاوه چنین اقدامی موجب آســـیب به ســـکوهای کوچک‌تر به جهت عدم توان رقابت و شفافیت و مشارکت‌پذیری کمتر به جهت اتخاذ رویکرد الگوریتمی از سوی سکو برای به حداقل رساندن خطر مسؤولیت و محدود شدن مشارکت مردمی می‌شود (Halfaker et al, 2013: 670).

حـــال اگر بخواهند بدون اصلاح یا حذف بخـــش ۲۳۰ به عنوان راهی میانه تلاش‌های خود جهت تنظیم‌گری در این حوزه را در ســـایه آن صورت دهند، دوراه

1. roommates.com
2. Profile
3. Eberhart

پیشنهاد گشته است: یکم، بر اساس سابقه قانونی تعیین شده در پرونده سکوی هم‌اتاقی دادگاه‌ها را مجاز به ورود در خصوص درجه‌ای که سکوها می‌توانند در محتواهای غیر قانونی دخالت داشته باشند، دانست؛ دوم، قانون‌گذاری در خصوص تغییر محیط اطلاعاتی حاکم بر سکوها بدون ایجاد مسؤولیت برای عملکرد سکوها (ناتانیل پرسیلی، ۱۴۰۰: ۴۱۸)؛ بدین معنا که باید اقدامات قانون‌گذارانه فراتر از اصلاح بخش ۲۳۰ همچون بار کردن الزامات مربوط به شفافیت، آشکارسازی از سوی کاربران سکوها و تغییر در جریان واقعی اطلاعات از طریق اصلاح الگوریتم‌های محتوای زیربنایی صورت داد. همه این‌ها به این دلیل است که بدون همکاری سکوها، شناسایی، پیگیری و مقابله با ناقضین قانون با چالش بزرگی مواجه خواهد شد و بهترین موقعیت را جهت اعمال این سیاست‌ها خود سکوها دارا هستند.

۳. خودتنظیمی به عنوان مکمل

خودتنظیمی به‌عنوان رویکردی انعطاف‌پذیر، سکوها را قادر می‌سازد تا به‌صورت مستقل سیاست‌ها و قواعدی را برای مدیریت محتوا و رفتار کاربران خود ایجاد و اجرا کنند. این مدل در کنار تنظیم‌گری‌های قانونی، نقشی مکمل ایفا می‌کند و امکان انطباق بهتر با نیازهای خاص هر سکو را فراهم می‌آورد (Cusumano et al, 2021: 4). علت آن است که سکوها برای حذف محتوای نامناسب انگیزه دارند؛ زیرا از یک سو محتوای ناقض موجب کاهش کاربران و ترجیح سکوهای رقیب می‌شود و از سوی دیگر با افزایش تأثیر سکوها بر افکار عمومی، احساس مسؤولیت در قبال پرورش جامعه سالم ایجاد می‌شود (Bu-iten et al, 2020: 7). به عبارت بهتر، چگونگی حکم‌رانی سکو بخشی جدایی‌ناپذیر از مراحل طراحی آن است؛ چرا که سکوها ناگزیر هستند میان حفظ منافع خود، تامین مستمر خدمات برای کاربران و رعایت حقوق آن‌ها تعادل برقرار کنند. از این رو، هر اندازه بتوانند ساختاری با کمترین سطح خطر[1] برای خود و کاربران شکل دهند، احتمال جذب اعتماد و رضایت کاربران و در نتیجه، موفقیت آن‌ها بیشتر خواهد بود (طحان‌نظیف و علی‌پور، ۱۴۰۱: ۱۳۳). در این راستا دو محور

1. Risk

اساسی یعنی خطوط راهنمای اجتماع[1] و تمایز میان سکوهای فعال و منفعل، نقشی تعیین‌کننده در اثربخشی خودتنظیمی ایفا می‌کنند و پایه‌های اصلی این رویکرد را تشکیل می‌دهند.

۱-۳. خطوط راهنمای اجتماع

موارد حذف داوطلبانه محتوا از سوی سکوها مستند به مجموعه‌ای از اصول و قواعد هست که سکوها برای حفظ سلامت، امنیت و کارکرد سالم محیط دیجیتال خود و با هدف مشخص‌سازی محتوای مجاز و غیرمجاز، شیوه‌های تعامل کاربران و حفظ حریم خصوصی تدوین و منتشر می‌کنند و به عنوان خطوط راهنمای اجتماع شناخته می‌شوند (Chan et al, 2023: 5). این خطوط ممکن است براساس باورهای اخلاقی سکو یا هنجارهای اجتماعی تدوین شوند. خودتنظیمی سکوها مزایایی چون انعطاف‌پذیری، کاهش مداخلات دولتی و توانایی سریع در پاسخ به چالش‌های جدید را فراهم می‌کند؛ در حالی که قوانین دولتی معمولاً زمان‌بر هستند. سکوها از طریق این رویکرد می‌توانند قوانین داخلی خود را مطابق نیازهای نوظهور و قوانین کشورهای مختلف تنظیم کنند و با عبور از پیچیدگی‌ها و تناقضات بین‌المللی، استانداردهای جهانی طراحی کنند. این امر تسهیل تجارت و تعاملات جهانی را در مواجهه با نظام‌های نظارتی متنوع امکان‌پذیر می‌سازد.

البته مسأله‌ای که وجود دارد دشواری‌های ارزیابی صحت عملکرد سکوها در به کارگیری این قواعد می‌باشد؛ زیرا خود این قواعد به خوبی درک نگشته‌اند و اطلاعات کمی در خصوص محتویات مورد حذف وجود دارد. به همین دلیل برخی معتقدند عملکرد سکوها در راستای هم‌تنظیمی و تحت قوانینی همچون «قانون حق نشر هزاره دیجیتال ایالات متحده» برخلاف قواعد داوطلبانه در دسترس‌تر و شفاف‌تر می‌باشد.[2] البته برای رفع این چالش، اقداماتی در محورهایی چون خودشفافیتی، رژیم‌های شفافیت مبتنی بر قوانین حکومتی (به مانند قانون بهبود اجرای قانون در شبکه‌های اجتماعی)[3] و بازرسی‌ها و تحقیقات

1. Community Guidelines

۲. همان، ص ۳۶۱.

۳. به عنوان مثال، اداره عدالت فدرال آلمان در ۲ جولای ۲۰۱۹، فیس‌بوک را به خاطر این‌که در

اشخاص ثالث نـــمونه در: (Macdonald, 2014: 5) پیشنهاد شده‌اند که می‌توانند زمینه را برای شفافیت بیشتر در عملکرد سکوها فراهم آورده و به تقویت خودتنظیمی کمک کنند.

به عنوان مثال، خودشـــفافیتی و رویکرد داوطلبانـــه، نه‌تنها اعتماد کاربران را افزایـــش می‌دهد، بلکه می‌توانـــد زمینه را برای درک بهتـــر محدودیت‌ها و اهداف خطـــوط راهنما فراهم کند. اعلام معیارهای حذف محتوا، ارائه آمار شـــفاف درباره نوع محتواهای حذف‌شـــده و توضیح دلایل حذف، به کاربران این امکان را می‌دهد که از منطق پشت تصمیمات ســـکو آگاه شوند. در سال ۲۰۰۸ ابتکار شبکه جهانی[1] تاســـیس شد[2] و بسیاری از سکوها برابر اصول ابتکار شـــبکه جهانی اقدام به انتشار گزارش شفافیت نموده‌اند؛ مثلاً گوگل در ســـال ۲۰۱۰ درخواست‌های دولت برای حذف محتوا را منتشر نمود و یا در سال ۲۰۱۲ گزارشی در خصوص محتواهایی که به خاطر قوانینی چون قانون حق نشر هزاره دیجیتال و قوانین دیگر حذف شده بودند را به آن افـــزود (Drummond, 2018). بعد از انتخابات ۲۰۱۶ آمریکا و با افزایش فشـــار عمومی جهت شفافیت بیشـــتر، در آوریل ۲۰۱۸، فیس‌بوک خطوط راهنمای اجتماع خود را منتشر نمود که گامی رو به جلو محسوب می‌گشت؛ زیرا انتشار چنین نسخه مفصلی مشتمل بر اطلاعات مربوط به سیاست‌های این سکو در استانداردهای خود همچون تعریف مفاهیمی چون گفتار نفرت‌افکن و محتوای جنســـی و برهنگی بود. البته در ادامه، فیس‌بوک در ســـال ۲۰۱۹ گزارش خود را مفصل‌تر نمود و حتی اطلاعاتـــی را از محتواهای محـــذوف، موارد اعتراض بـــه آن و اعتراضات منتج به

گزارش‌های خود دقیقاً مشخص نکرده است که کدام شکایت‌ها بر اساس خطوط راهنمای اجتماع است، دو میلیون یورو جریمه کرد. جهت مشاهده رجوع کنید به:
BundesamtfürJustiz. "Facebook fined for lack of transparency." July 2, 2019. https://www.bundesjustizamt.de/SharedDocs/Pressemitteilungen/EN/2019/20190702_facebook.html.

1. Global Network Initiative

۲. ابتکار شـــبکه جهانی (GNI) ماهیتی غیر دولتی، چندذی‌نفعـــی و داوطلبانه دارد؛ بدین معنا که تحت مدیریت یا کنترل هیچ دولت خاصی نیست و یک بستر همکاری بین ذی‌نفعان مختلف است و با مشارکت شرکت‌های فناوری، سازمان‌های جامعه مدنی، دانشگاهیان و سرمایه‌گذاران اجتماعی تاسیس شده است و همچنین به‌طور داوطلبانه عمل می‌کند و شرکت‌ها و سکوها به اختیار خود به آن می‌پیوندند و اصول آن را می‌پذیرند.

بازگشت محتوا منتشر نمود. چنین گزارشی نشان می‌دهد که ممکن است محتواهایی نیز علی‌رغم عدم مخالفت با استانداردهای خطوط راهنمای اجتماع یا قوانین مربوط صرفاً به علت مواردی همچون تشخیص اشتباه یک سامانه خودکار حذف شده باشند (Gorwa et al, 2020: 9).

۲-۳. تمایز سکوهای فعال و منفعل

همان‌گونه که سابقاً بیان شد، طبق دستورالعمل تجارت الکترونیک اروپا، سکوها از مسؤولیتی برخوردار هستند که به آن‌ها اجازه می‌دهد بدون نیاز به نظارت یا کنترل بر تمام محتواهای بارگذاری‌شده، به فعالیت خود ادامه دهند، اما رویه قضایی سکوها را بر اساس میزان دخالت در محتوای کاربران و آگاهی از محتوای غیر قانونی، به دو قسم فعال و منفعل تقسیم می‌کند. حال در دورانی که سکوها با تکیه بر خودتنظیمی، ابزارهایی همچون سیستم‌های رتبه‌بندی،[1] اعلام و حذف،[2] سیستم‌های مبتنی بر هوش مصنوعی و یادگیری ماشینی و حتی استفاده از تیم‌های انسانی را برای مبارزه با محتوای غیرقانونی توسعه داده‌اند، آیا مصونیت قوانینی همچون دستورالعمل تجارت الکترونیک که منوط به ارائه خدمات منفعل و حذف سریع محتوا پس از اطلاع است، همچنان برای سکوهای امروزی مناسب و کارآمد باقی مانده است یا خیر؟ بدین جهت که برخی بر این باور هستند که در چارچوب ماده ۱٤ دستورالعمل تجارت الکترونیک اتحادیه اروپا، سکوها ممکن است از هرگونه نظارت داوطلبانه بر محتوا خودداری کنند؛ زیرا این مداخله می‌تواند آنان را در معرض از دست دادن مصونیت قانونی قرار دهد.

قانون خدمات دیجیتال اتحادیه اروپا تلاش نمود تا نواقص نظام مسؤولیت دستورالعمل تجارت الکترونیک از جمله نامشخص بودن تمایز نقش‌های فعال و منفعل و محدودیت در اقدامات داوطلبانه سکوها را رفع کند. این قانون یک بند سامری نیکوکار[3] را در خود جای داده است که با هدف تشویق

1. Rating system
2. Notice and takedown
3. Good Samaritan

مقصود مواردی است که فرد وظیفه قانونی نداشته و لیکن از روی نیکویی سرشت و اخلاق مبادرت به انجام کاری می‌نماید.

سکوها به نظارت بهتر، بدون نقض اصل ممنوعیت نظارت عمومی، ارائه شد. این بند تصریح می‌کند که اقدامات داوطلبانه برای شناسایی و حذف محتوای غیرقانونی، مصونیت سکوها را از بین نمی‌برد و آن‌ها را به ابتکار عمل بیشتر در مقابله با محتوای غیر قانونی، بدون نگرانی از از دست دادن مصونیت ترغیب می‌کند (Buiten, 2021: 373). این نوآوری حقوقی، سکوها را تشویق می‌کند تا نقش مسؤولانه‌تری در فضای برخط ایفا کنند؛ بدون این که نگران شوند با ورود به این فرایند، وارد محدوده مسؤولیت شوند. البته برخی معتقدند که تمایز فعال و منفعل به عنوان معیاری برای مسؤولیت سکوها با توجه به تعدیل گسترده‌ای که در آن‌ها صورت می‌گیرد مشکوک است؛ در حالی که سکوها برای جذب مخاطب از تعدیلات گسترده‌ای مانند الگوریتم‌های سفارشی‌سازی استفاده می‌کنند، این تصور که آن‌ها نقش خنثی دارند، پذیرفته نیست. از سوی دیگر تشخیص این که چه نوع تعدیلی مجاز است و در چه نقطه‌ای به نقش فعال تبدیل می‌شود دشوار است. راه حل جایگزین، کنار گذاشتن تمایز فعال و منفعل و پیوند معافیت مسؤولیت با رعایت تعهد مراقبت[1] و دقت لازم تحت قانون خدمات دیجیتال است؛ امری که به طور موثر یک استاندارد مراقبت در سطح اتحادیه اروپا برای سکوها ایجاد می‌کند (Buiten, 2021: 371-372). در واقع یک تحول اساسی در سیاست حقوقی اتحادیه اروپا با عبور تدریجی از تمایز کلاسیک فعال و منفعل به سمت یک رویکرد مبتنی بر مسؤولیت‌پذیری رخ داده است. این تحول به معنای پذیرش واقعیت‌های فناوری امروز است؛ جایی که سکوها نمی‌توانند به بهانه منفعل بودن از مسؤولیت اجتماعی و حقوقی شانه خالی کنند.

1. Duty of care

برآمد

۱- رشد سریع سکوها در عصر دیجیتال و تأثیر گسترده آن‌ها بر زندگی افراد، به‌دلیل ویژگی‌هایی چون دسترسی آسان و تسهیل خدمات، موجب استقبال عمومی شـــده و ضرورت تنظیم‌گری دقیق آن‌ها را بیش از پیش نمایان ساخته است. سکوها به‌عنـــوان پدیده‌ای نوظهور، در کنار مزایای چشمگیرشـــان، مخاطراتی نیز به همراه داشته‌اند که در صورت فقدان سیاست کیفری مناسب، می‌تواند آسیب‌های جدی به جامعه وارد کند.

۲- یکی از چالش‌های اساســـی در زمینه تنظیم‌گری سکوها، ضرورت وجود قوانینی به‌روز و متناسب با ماهیت آن‌ها و دشواری اعمال نظارت بیرونی بر محتوای تولیدشده توســـط کاربران اســـت؛ به‌ویژه آن‌که قوانین ســـنتی توان پاسخ‌گویی به پیچیدگی‌ها و اقتضائات این حوزه را ندارند. از سوی دیگر موجودیت سکوها بسته به اقبال کاربرانشـــان اســـت و همین موضوع، آن‌ها را وادار می‌کند فضایی جذاب و مناســـب برای کاربران فراهم آورده و به کاربســـت قواعد مربوط در راستای کاهش بزه‌دیدگی کاربران در بستر خود اقدام نمایند.

۳- این پژوهش با بررســـی نظام‌هـــای حقوقی مختلـــف و روند تحول در دیدگاه‌ها پیرامون مســـؤولیت ســـکوهای محتوایی -اعم از مدنـــی یا اداری و حتی کیفری- و تنظیم‌گری فضای آن‌ها و رهیافت‌های مختلف اندیشیده‌شـــده در راستای آن، به اهمیت گذار از مصونیت مطلق به ســـوی پذیرش معیارهایی برای پاسخ‌گویی پی برده و تنظیم‌گری مشارکتی را که در آن سکوها نه صرفاً تابع مقررات دولتی، بلکه به‌عنوان ذی‌نفعان اصلی در فرایند تنظیم‌گری مشـــارکت دارند، به‌عنوان یک راهکار مؤثر پیشـــنهاد می‌نماید. چنین رویکردی می‌تواند با ایجاد تعادل میان نظارت کارآمد و حفظ نوآوری، به بســـیاری از چالش‌های موجود در این حوزه پاسخ دهد. از این رو قانون‌گذار باید چارچوب‌ها و معیارهای کلی را تعیین کرده و جزئیات اجرایی و تطبیق آن‌ها با شرایط خاص را به عهده سکوها بگذارد.

٤- به رویکرد مذکور در بند پیشـــین، ایرادهایی وارد می‌شود که از یک سو، ســـکو در تعیین دســـتورالعمل و خطوط راهنمای اجتماع خود ممکن است فراتر از حدود قانونی عمل نماید و از ســـوی دیگر در برخورد با محتوای ناقض و بررســـی

مقبولیت درخواست مرتبط با آن نقشی به مانند یک قاضی ایفا می‌کند؛ در حالی که در همان زمان به عنوان یک ذی‌نفع چنین مواردی می‌باشد و با حذف، از مسؤولیت احتمالی مبرا می‌شود. برای رفع این ایرادها، لازم است قانون‌گذار اصول راهنمایی روشن و مشخص را تدوین کند تا سکوها براساس این اصول اقدام به تعیین دستورالعمل‌ها و هم‌چنین محدودسازی یا حذف محتواهای ناقض و نامناسب نمایند.

۵- در حقوق ایران، کارگروه تعیین مصادیق محتوای مجرمانه طبق مواد ۷۴۹ تا ۷۵۱ کتاب پنجم قانون مجازات اسلامی مصوب ۱۳۷۵ با اصلاحات و الحاقات بعدی (مواد ۲۱ تا ۲۳ قانون جرایم رایانه‌ای مصوب ۱۳۸۸) تا حدی این وظیفه را بر عهده دارد، اما این نظام نیز در عمل با کاستی‌هایی روبه‌رو است. از جمله این کاستی‌ها، کلی، زمان‌بر و تفسیرپذیر بودن اصول راهنمای موجود است که می‌تواند دوباره سکوها را در جایگاه قضاوتی نامتناسب قرار دهد. برای حل این معضل، اصول راهنما باید به‌صورت مصداقی و شفاف تنظیم شوند؛ به‌گونه‌ای که سکو بتواند بلافاصله و بدون ابهام تصمیم‌گیری کند. افزون بر موارد فوق، ضرورت دارد امکان اعتراض صاحبان محتوا به تصمیمات حذف یا غیرقابل‌دسترس‌سازی پیش‌بینی شود؛ بنابراین نیاز است در قانون، یک کمیسیون و یا نهاد مشابه آن پیش‌بینی شود که بتواند این محتواهای ابداعی جدید را مورد بررسی قرار داده و ناقض یا غیر ناقض بودن و تحت لوای مواد قانونی مقرر قرار گرفتن یا نگرفتن آن را بر اساس معیارهای کلی مدنظر قانون‌گذار مشخص نماید یا در صورت محدودیت عملی بررسی تمامی محتواهای جدید، در اقل امر نسبت به بررسی موارد مورد استعلام سکوها یا مورد اعتراض کاربران اقدام نماید. بدین‌ترتیب هر چند معیار کلی مدنظر قانون‌گذار تغییر نمی‌کند و به عنوان مثال در حقوق ایران محتوای موجب اشاعه فحشا و منکرات، ناقض و مجرمانه تلقی می‌شود، اما این که یک عکس یا فیلم یا متن به عنوان یک محتوای جدید تولیدی از سوی یک کاربر که آن را در سکو منتشر می‌کند، چنین محتوایی تلقی می‌شود یا خیر، نیازمند تعیین از سوی چنین کمیسیونی دارد تا از سلیقه‌ای شدن تصمیمات در راستای حفظ اصل آزادی بیان و حریم خصوصی اشخاص جلوگیری شود و بتوانیم سکوها را در این زمینه راهنمایی کنیم تا آن‌ها

بدون دغدغه و نگرانی که ممکن اســـت منجر به برخـــورد و حذف‌های حداکثری شـــود، اقدام نماینـــد. در نهایت، در صورت نقض ضوابط از طرف ســـکوها نیاز به ایجاد سازِکار مســـؤولیتی می‌باشد. این سازِکارها چنان‌که در اسناد راهبردی اتحادیه اروپا مشـــاهده شد اغلب به کشورها واگذار شده است و کشورها بر اساس رویکرد اقتصادی، سیاســـی و اجتماعی خود اختیار داشـــته مبادرت به تعیین ضمانت اجرای مدنی و یا انضباطـــی و اداری نمایند؛ با این حال، تعیین ضمانت اجرای کیفری تنها در موارد نادر و ضروری و تنها نسبت به نقض ارزش‌ها یا وظایف بسیار مهم توسط ســـکوها ممکن می‌باشد و اغلب کشورها برای تبادل اطلاعات، این راهکار را نسبت به مســـوولیت هـــای مدنی و انضباطی با احتیاط بیشـــتر و در قلمرو محدودتر مقرر نموده‌اند.

فهرست منابع

الف. فارسی

* امامیان، سید محمدصادق و جمعی از همکاران (۱۳۹۷)، **نظام ملی تنظیم‌گری (۱) مفهوم تنظیم‌گری و ارتباط آن با نظام حکمرانی**، مرکز پژوهش‌های مجلس شورای اسلامی.

* حسنی، حسین (۱۴۰۳)، «**حکمرانی و تنظیم‌گری پلتفرم‌های ویدئویی در ایران: از منازعه بر سر نهاد متولی تا تعدیل محتوا (مورد مطالعه: آپارات)**»، حقوق فناوری‌های نوین، دوره ۵، شماره ۱۰.

* طحان نظیف، هادی و علی‌پور، محمدرضا (۱۴۰۱)، «**جایگاه و آثار حقوقی خودتنظیم‌گری پلتفرم‌های دیجیتال**»، حقوق فناوری‌های نوین، دوره ۳، شماره ۶.

* غلامی، محمد و جمعی از همکاران (۱۳۹۶)، **سنجش اقتصاد دیجیتال**، پژوهشکده آمار.

* قاسمی، مجتبی و عبدالهی نیسیانی، مصطفی (۱۴۰۰)، «**تنظیم‌گری بهینه اقتصادی در خصوص سکو(پلتفرم)های اینترنتی**»، تحقیقات حقوقی، دوره ۲۴، شماره ۹۴.

*ناتانیل پرسیلی، جاشوا.تاکر (۱۴۰۰)، **رسانه‌های اجتماعی و مردم‌سالاری: وضعیت حوزه و چشم‌انداز اصلاح**، برگردان: علیرضا کاظمی و دیگران، تهران، پژوهشگاه فضای مجازی.

ب. انگلیسی

* Boyle, James, and Jennifer Jenkins(2014), **"Intellectual Property: Law & The Information Society**.

* Buiten, Miriam C., Alexandre De Streel, and and Martin Peitz (2020), **"Rethinking liability rules for online hosting platforms."** International Journal of Law and Information Technology 28, no. 2.

* Buiten, Miriam C (2021). "The Digital Services Act From Intermediary Liability to Platform Regulation." J. Intell. Prop. Info. Tech. & Elec. Com. L. 12.

❋ Bülent, KENT(2020). **"Regulation of Social Networks in German Law and the German Social Network Act."** Journal of Information Technology Law 2, no. 1.

❋ Cannon, Bryant, and Hanna Chung (2018). **"Who decides? A framework for fitting the co-regulation of sharing economies to the contours of the market."** The Cambridge handbook of the law of the sharing economy.

❋ Chan, Ngai Keung, Chris Chao Su, and Alexis Shore (2023). **"Shifting platform values in community guidelines: Examining the evolution of TikTok's governance frameworks."** new media & society.

❋ Cusumano, Michael A., Annabelle Gawer, and David B. Yoffie (2021). **"Can self-regulation save digital platforms?."** Industrial and Corporate Change 30, no. 5.

❋ Drummond, David (2010). **"Greater Transparency Around Government Requests."** Official Blog, Google.

❋ Finck, Michèle (2018). **"Digital co-regulation: designing a supranational legal framework for the platform economy."** European law review.

❋ GEDİKLİ, Ahmet Taha (2020). **"Prevention of the Spread of False Information on the Internet in Comparative Law."** Journal of Information Technology Law 2, no. 2.

❋ German Federal Ministry of Justice and Consumer Protection, **"Questions and answers: Act to Improve Enforcement of the Law in Social Networks."** www.bmjv.de/SharedDocs/FAQ/EN/NetzDG/NetzDG.html

❋ Gillespie, Tarleton (2017). **"Platforms are not intermediaries."** Geo. L. Tech. Rev. 2.

❋ Gillespie, Tarleton (2018). **"Regulation of and by platforms."** The SAGE handbook of social media.

❋ Gorwa, Robert, Reuben Binns, and Christian Katzenbach (2020). **"Algorithmic content moderation: Technical and political challenges in the automation of platform governance."** Big Data & Society 7, no. 1.

❋ Halfaker, Aaron, R. Stuart Geiger, Jonathan T. Morgan, and John Riedl (2013). **"The rise and decline of an open collaboration system: How Wikipedia's reaction to popularity is causing its decline."** American behavioral scientist 57, no. 5.

❋ Hornik, Joanna (2017). **"An Economic Analysis of Liability of Hosting Services: Uncertainty and Incentives Online**. Bruges European Economic Research Papers.

❋ Macdonald, Lord Kenneth (2014). **A Human Rights Audit of the Internet Watch Foundation**. Internet Watch Foundation.

❋ MacKinnon, Rebecca, Elonnai Hickok, Allon Bar, and Hae-in Lim (2015). **Fostering freedom online: The role of internet intermediaries**. UNESCO Publishing.

❋ Sağıroğlu, Şeref, and M. Alkan (2018). **Cybersecurity and Defense**. Grafiker Publishing, Ankara.

❋ Sevanian, Andrew M (2014). **"Section 230 of the Communications Decency Act: A" Good Samaritan"Law Without the Requirement of Acting as a" Good Samaritan"**. UCLA Ent. L. Rev. 21.

❋ Sharkey, Catherine M (2022). **"Products Liability in the Digital Age: Online Platforms as" Cheapest Cost Avoiders"**." Hastings LJ 73.

❋ Udrea, Andreea, and David Smith (2021). **"Minority Protection and Kin-State Engagement: Karta Polaka in Comparative Per-**

spective." Ethnopolitics 20, no. 1.

❊ Wyman, Katrina (2018). **"The novelty of TNC regulation."** Nestor Davidson, MichèleFinck and John Infranca, Cambridge Handbook on Law and Regulation of the Sharing Economy (Cambridge University Press 2018)., NYU Law and Economics Research Paper 18-07

A Comparative Study of Co-Regulation in Addressing the Risks Posed by Content Platforms

Mohammad Yekrangi[1], Seyed Mahmoud Ghoroghchian[2]

Abstract

The rapid growth of digital platforms and their profound impact on individuals' lives, coupled with the inability of traditional laws to adequately respond to the complexities of this field, have highlighted the need to reconsider regulatory approaches. Today, many interactions and transactions between individuals take place through digital platforms. Among these, user-centered content platforms have assumed particular significance, as users are able to upload and disseminate virtually any type of content. This raises the question of the platform's liability-whether civil, administrative, or even criminal-for such content. Do platforms bear liability for user-generated content, and is their liability limited to removing harmful and unlawful content and restricting access to it, or does it extend beyond such measures? Employing a descriptive-analytical methodology based on library research, this study

1. Assistant Professor, Department of Criminal Law and Criminology, Faculty of Law and Political Science, University of Tehran, Tehran, Iran
Yekrangi@ut.ac.ir
2. Ph.D of Criminal Law and Criminology, Faculty of Law and Political Science, University of Tehran, Tehran, Iran (Corresponding Author)
ghoroghchian73@ut.ac.ir

comparatively examines three regulatory models governing cyber-space- namely, co-regulation, self-regulation, and state regulation- and analyzes the transition from absolute platform immunity toward the recognition of limited liability and the participation of platforms in the regulatory process. Within this framework, the two key approaches of co-regulation and self-regulation transform the role of platforms from that of mere rule-followers into active participants in the formulation and implementation of regulatory guidelines. Nevertheless, challenges such as discretionary decision-making, over-removal of content, and conflicts of interest further underscore the need to develop clear guiding principles and establish independent oversight commissions. The findings of the study indicate that co-regulation, by striking a balance between effective oversight and the protection of freedom of expression, can provide an appropriate response to the regulatory challenges arising in the digital environment.

Keywords: Civil Liability, Content Platforms, Co-Regulation, Criminal Liability, Self-Regulation; State Oversight

Introduction

The present research aims to conduct a comparative analysis of the principles of civil liability of online trading platform owners within the legal systems of Iran and the European Union. The rapid expansion of e-commerce and the proliferation of trading platforms such as Amazon, eBay, and Digikala have underscored the urgent need to reassess traditional civil liability frameworks, particularly in the face of complex, multi-layered, and technologically mediated relationships in digital spaces. The central research question is whether platform owners can be held liable for damages suffered by users-including both consumers and suppliers-and if so, upon which legal foundations such liability may be established.

The research methodology is descriptive-comparative in nature, involving a thorough examination of legal sources, regulations, judicial precedents, and international instruments within both jurisdictions. In EU law, key documents include the E-Commerce Directive (2000/31/EC), the Digital Services Act (2022), and the Product Liability Directive (85/374/EEC). In Iranian law, the analysis draws upon the Electronic Commerce Act (2003), the Computer Crimes Act (2009), the Consumer Protection Act (2009), general civil liability principles, and Islamic legal maxims such as the rule of "no harm" (lā Zarar), "waste" (itlāf), and"causation" (tasbīb).

Discussion and Findings

The findings of the study indicate that, in both legal systems, traditional foundations of civil liability-such as the theory of customary fault, presumed fault, strict liability, and the risk theory-continue to serve as the primary and general bases for analyzing the liability of platform operators. Nevertheless, the technical and structural complexities of the digital environment have created significant difficulties in establishing fault and causation. Users and injured parties, particularly ordinary consumers, often lack access to critical information and the

evidence necessary to establish the platform operator's technical or organizational fault. This protective gap justifies the adoption of modern approaches to civil liability as complementary mechanisms alongside traditional foundations.

In this regard, novel theories such as "participatory infringement," "legitimate trust," "effective control over economic aspects," "agency," and the "brokerage liability regime" have been introduced and examined as complementary foundations for analyzing the civil liability of operators of online trading platforms. The theory of participatory infringement, which has its roots in the judicial practice of common-law jurisdictions, rests on two elements: "the platform operator's knowledge and awareness of users' unlawful activities" and "effective participation in the breach of duty." It may serve as a basis for liability where a platform, despite being aware of an infringement, fails to take preventive or deterrent measures. The theory of legitimate trust is based on the premise that where a trading platform, through its design, advertising, and provision of services, goes beyond the role of a mere intermediary and thereby induces consumers to rely on the safety and quality of goods, it may be held liable for compensation in the event of harm. This rationale is also reflected in Article 6(3) of the European Union's Digital Services Act. The theory of effective control, inspired by the case law of the Court of Justice of the European Union, maintains that where a platform exercises a decisive role in significant economic aspects of a transaction-including transportation management, warehousing, payment processing, and marketing-it may be treated as the seller or supplier of the goods and may consequently be held liable for harm arising from the acts of a third-party supplier.

A comparative analysis indicates that the European Union legal framework, through the adoption of the Digital Services Act, has taken significant steps toward narrowing the liability exemptions available to online platforms, clarifying their monitoring and due-diligence obli-

gations, and strengthening consumer protection. Accordingly, where platforms have actual or constructive knowledge of illegal activities and fail to respond in a timely manner, they may lose the benefit of the hosting exemption and be treated as "active intermediaries" subject to liability. Nevertheless, the European Union's Product Liability Directive, adopted in 1985, has not undergone a corresponding update to adequately address digital supply chains and continues to present significant ambiguities and regulatory gaps concerning the liability of online platforms for defective goods. The case law of European countries is likewise not uniform in this area, and courts frequently seek to address legislative gaps by resorting to emerging theories such as effective control and legitimate reliance.

In Iranian law, despite the potential afforded by the general principles of civil liability and Islamic jurisprudential foundations, the existing legal framework suffers from significant structural shortcomings. These include the absence of comprehensive and integrated legislation governing the status and liability of online trading platforms; the lack of explicit statutory provisions defining the scope of the platforms' monitoring and information duties; the absence of well-established and coherent judicial practice; and the lack of independent regulatory bodies vested with sufficient powers to ensure compliance with applicable standards. Iran's Electronic Commerce Law focuses predominantly on the formal aspects of electronic transactions. Article 33, which addresses the obligation to provide transparent information, lacks an effective enforcement mechanism. Moreover, although Article 78 of the same Law identifies defects or deficiencies in systems as grounds for liability and compensation for damages, its application to online platforms remains subject to considerable uncertainty, and judicial practice has thus far been unable to effectively remedy this regulatory gap.

Based on the findings of this study, it may be concluded that the civil liability of operators of online trading platforms may be con-

tractual or non-contractual, depending on the platform's role and degree of involvement in the transaction, and that its legal foundations derive from a combination of traditional and modern theories. In the European Union legal framework, the recognition of "constructive knowledge" under the Digital Services Act has, to some extent, alleviated the burden of proof on the injured party in cases of non-contractual liability and shifted the analysis toward a presumption of fault. By contrast, Iranian law continues to emphasize customary fault as the primary basis of liability and has yet to adequately incorporate modern complementary approaches. Furthermore, where a platform operator plays an active role in the supply chain of goods or services-including quality control, warehousing, transportation, or creating an appearance of reliability for consumers-it can no longer be regarded merely as a passive intermediary. In such circumstances, depending on the specific facts of the case, the basis of liability may instead rest on the theory of effective control, legitimate reliance, or product liability.

Conclusion

Finally, by identifying the existing legal gaps in the legal system of Iran, this study puts forward recommendations at three levels. First, at the legislative level, it proposes the enactment of comprehensive and coherent legislation governing the liability of online trading platforms, drawing on the successful experiences of the European Union and integrating modern theories with the traditional principles of civil liability. Second, at the judicial level, it recommends the development and publication of specialized judicial guidelines, together with the establishment of a database of analogous judgments, in order to promote consistency in judicial practice and facilitate the issuance of harmonized decisions. Third, at the institutional level, it proposes the establishment of an independent and effective regulatory body to periodically monitor the performance of online platforms and, through the application of proportionate enforcement measures, safeguard the rights of con-

sumers and suppliers. The implementation of these recommendations could, while addressing existing legal uncertainties, strengthen users' confidence in e-commerce systems and create a more conducive environment for growth and innovation within the digital business sector.